

**Achievement of Market-Friendly Initiatives and Results Program
(AMIR 2.0 Program)**

Funded By U.S. Agency for International Development

E-Government Legal and Regulatory Review

Final Report

**Deliverable for ICTI Component, Task No. 431.8
Contract No. 278-C-00-02-00210-00**

December 2002

This report was prepared by International Business Legal Associates (IBLAW) in collaboration with Chemonics International Inc., prime contractor to the U.S. Agency for International Development for the AMIR Program in Jordan.

Table of Content

Preface	4
Executive Summary	5
Part I: SGN Security Related Legal Aspects	6
Matrix (1): Assessment of ISP Legal Requirements	8
Part II : Legal Aspects of SGN Messaging and Directory Services	24
Part III : SGN and Legal Aspects of Data-Sharing	30
Matrix (2): Legal Assessment of Data-Sharing Provisions in Jordanian Legislation	31
Matrix(3) Data Sharing and Disclosure: Status in Specific Laws	42

Preface

The Government of Jordan is seeking to implement a Government wide network infrastructure, to be known as the Secure Government Network (SGN) , and which will eventually link all government institutions. The SGN will enable secure Department-to-Department interoperability and interconnectivity, support secure connectivity to the Internet and provide the mechanism for introducing Government wide shared services accessible by all Departmental users.

This report examines the salient legal issues pertaining to the following aspects and uses of SGN: (1) security (2) data-sharing and (3) messaging and directory service.

With respect to entity specific issues, the report focuses on the six entities targeted by the first phase of the plan namely. There are, the Ministry of Industry and Trade, Ministry of Planning, Ministry of Information and Communications Technology, Ministry of Finance, Greater Amman Municipality, and the Prime Ministry. However, most of the general findings of the report are readily applicable to a full scale SGN initiative.

In preparing this report, account has been taken of the general policy and technical framework within which the SGN will be implemented, as reflected in key related documents, mainly, the Jordan e-Government Information Security Plan, the Jordan e-Government Messaging and Directory Services Statement of Needs, the Jordan E-Government Project SGN Statement of Needs, and the Jordan e-Government Interoperability Framework.

This report was prepared by International Business Legal Associates (IBLAW) and delivered to Chemonics International-AMIR Program, under Task No. Task No. 431.8, ICTI Component, as part of the E-Government Legal and Regulatory Review: E-Gov. Legal Consultation.

Executive Summary

The main conclusions and recommendations of the legal review presented in this report may be summarized as follows:

- (1) *With respect to security aspects of SGN***
 - *Current legislation does not clearly ascribe responsibility for deployment and maintenance of security features of SGN network. There is a need to assign clearly authority for such, as part of the overall task of defining and allocating responsibilities and authorities for implementation and maintenance of e-Government*
 - *Current legislation does not adequately provide a basis for effective implementation of information asset security principles. There is an immanent need for enacting legislation that set, or pursuant to which can be set, government wide security measures and standards. Such legislation would also clearly assign roles and responsibilities for information asset security, and attach effective legal consequences for non-compliance with mandated standards.*
- (2) *With respect to use of messaging and directory services***
 - *It is highly recommended to enact legislation regulating specifically use of e-mail for administrative communication within a closed secure network. Unlike, the current E-transactions law, such a legislation would address the unique features and requirements of administrative communication within a closed and secure government network.*
 - *The use of common e-mail directory service across government is legally unproblematic.*
- (3) *With respect to data sharing***
 - *There is need to enact legislation that would eliminate legal risks entailed in inter-departmental data sharing and regulate all aspects of such. The proposed legislation would provide general criteria for data sharing and mandate government entities to characterize status of data maintained by them with respect to availability and disclosure. As well, it would regulate various aspects of data sharing, define attendant responsibilities upon data providers and recipients, and attach consequence upon non compliance. In addition, there is also a need to enact general legislative provisions mandating data sharing and cooperation in the absence of legislative provisions to the contrary. This would be necessary in order to eliminate unjustified customary resistance to data sharing that may decelerate the pace of e-government.*

Part I

SGN Security Related Legal Aspects

A-Introduction

SGN is intended to enable *secure* department to department interoperability and interconnectivity, support *secure* connectivity to the internet and provide the mechanism for introducing the government wide shared services accessible by all departmental users.

Effective maintenance of SGN security raises legal issues at the level of (1) Infrastructure deployment and expansion, (2) overall maintenance and operation and (3) on going security, governance and maintenance.

(I) SGN Infrastructure deployment and expansion requirements:

Deployment (including future expansion) of an SGN across government is a challenging and ongoing task (expansions and upgrades). It would require considerable coordination between different government entities, and compliance with requisite security (as well as other) standards by all subscribing entities to ensure *secure* connectivity and interoperability. This dictates the need for a leading entity to set such security standards, coordinate procurements and deployment in conformity therewith, monitor ongoing compliance, and “accredit” “secure” subscribing entities. This need for managed deployment is recognized in e-Government SGN Statement of Needs, and e-Government Information Interoperability Framework.

The foregoing raises the question: Does MOICT or any other government entity enjoy currently the requisite legal authority to exercise the above mandate? If not- and this seems to be the case- who should assume such a task? What should the role of MOICT as the supposed custodian of e-government be in respect of *insuring implementation of network security standards*? What legal amendments would be required to stipulate such authorities? Such questions are not within the scope of this assignment and will not be addressed in this report. ***However, they are of principle importance and should be addressed in a separate scope dealing generally with the allocation of authorities and responsibilities for overall e-government implementation and maintenance.***

SGN overall maintenance and operation requirements:

As stated in SGN statement of needs, ensuring proper operation of SGN and the availability of *secure*, managed connectivity requires the establishment of a fully functional e-Government Operations Center. **The e-government operations center will have prime responsibility for the overall management, configuration and support of the Departments connectivity, to the SGN physical network.** This raises legal issues about the role and responsibility of the operations center in security maintenance vis-à-vis other authorities who may be involved in security at deployment level and otherwise. ***This issue must be addressed in the exercise of assigning clear legal mandates and responsibilities for various aspects of e-government implementation and maintenance,***

and with the purpose of defining accountabilities and avoiding unnecessary overlap of authorities.

(III) Information assets security governance:

SGN security governance involves more than deployment and upgrade of network technical security features. It is a complex, ongoing and dynamic affair which depends ultimately upon compliant behavior of all network users. Effective governance of information asset security also involves regulating user behavior, setting security measures, spelling out roles, rights and responsibilities and assigning consequence to non-compliance.

The general guidelines for government information assets security government are spelled out in the e-Government Information Security Plan (ISP). The plan envisions broad and encompassing security principles with respect to, assignment of roles and responsibilities, organizational security, asset classification and control, personnel security, physical and environmental security, communication and operations management, access control, systems development and maintenance, and business continuity management and compliance.

This report presents a detailed assessment of the legal requirements and implications of ISP. Taking into account international practice in governance of information asset security, it identifies current gaps in Jordanian legislation, and recommends measures to address them. The detailed findings of this assessment are presented in ***Matrix (1): Assessment of ISP Legal Requirements***. The salient conclusion and recommendation however can be summarized as follows:

Current legislation does not adequately provide a basis for effective implementation of information asset security principles. There is an immanent need for enacting legislation that set, or pursuant to which can be set, government wide security measures and standards. Such legislation would also clearly assign roles and responsibility for information asset security and attach effective legal consequences for non-compliance with mandated standards.

Matrix (1): Assessment of ISP Legal Requirements

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
Information Security Plan: Essential Principles and Requirements			
E-government and its employees must comply with all statutory, regulatory and contractual requirements which relate directly or indirectly to information security.	There is no current Jordanian legislation pursuant to which legally binding and authoritative ISP directives may be issued, as elaborated hereunder.	Security directives in countries with Information Security Plans are typically issued within or pursuant to IT security Master legislation or in derivative legislation issued pursuant thereto. (see below).	To render ISP requirements mandatory, and legally binding and consequential such requirements must be pursuant to an authoritative legal instrument as elaborated hereunder.
<p><u>Roles and Responsibilities</u> The ISP and subsequent security standards are owned by the e-Gov. Executive and are defined and maintained by e-Gov. Information Security Forum (who reports directly to the Deputy Director General for MOICT).</p> <p>It is for the E—Gov Executive to devolve the maintenance and development of Information Security Plan (ISP) to the Government Information Security Manager (GISM). To direct, lead, challenge and coordinate information security within the e-Gov. The e-Gov Executive should empower the GISM to establish an Information Security Forum (ISF).</p> <p>The ISF membership to comprise a senior manager from each Ministry, e.g. Deputy Director General who has responsibility for</p>	<p>Regardless of the mechanism adopted for developing ISP mandates and guidelines, there is no legal basis in current legislation for issuance of such binding mandates and guideline. Nor is there an entity that is currently authorized to issue such binding standards.</p> <p>Neither the Ministry of Information and Communication Technology nor the Telecommunication Regulatory Commission have a clear mandate to issue “requirements “ that are binding on other ministries.</p> <p>Much less would GISM (presumably an entity, unit within MOICT or TRC) or a forum established – or summoned by such enjoy such authority. This is the case, especially given the “binding” nature of such “requirements”, the responsibility and accountability attached to their implementation and the supposed implications of their</p>	<p>A review of key countries which have mandated Security Plans and standard indicates that such schemes are mandated and regulated pursuant to high level legislative instruments.</p> <p><u>US Example</u> The Office of Management and Budget (OMB) has overall responsibility for computer security policy. Pursuant to legislative amendments issued for this purpose.</p> <p><i>The Government Information Security Reform Act of 2000 (Security Act)</i> gives the OMB information security duties to enhance government wide oversight of Federal agencies.</p> <p>The <i>Security Act</i> requires annual agency program reviews, annual Inspector General security evaluations, agency reporting to</p>	<p>Enact a Master Information Security Legislation to govern security standards, assign authorities roles and responsibilities and define consequences for non-compliance. Such legislation may authorize an entity within MOICT, or otherwise if appropriate, to issue security standards in coordination with an inter-agency forum, summon a forum, develop directives in coordination therewith, and monitor implementation, etc. The directives issued pursuant to such legislation and the authorities vested therein would provide as appropriate for all aspects of Information Security, including management, physical security, network security, asset classification, training, employee responsibility, security planning etc.</p> <p>Such an instrument would define roles and responsibilities, and if need be stipulate “penalties” for violations (see below for applicable penalties and disciplinary measures under current legislation).</p>

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
<p>information security within their Ministry.</p> <p>Information Security Forum will be:</p> <p>Reviewing and approving ISP and overall responsibilities; Monitoring significant changes in the risk profile; Monitoring and reviewing information security incidents; Approving major initiatives for all security related activities.</p> <p>The responsibility for ensuring that the ISP and related security standards are implemented ultimately lies with the Deputy Director General of each Ministry participating in e-Gov. and should be reported as part of an annual self certification compliance program.</p> <p>All employees are responsible for maintaining the required level of security within the scope of their role.</p>	<p>violation.</p> <p>The mandate to issue ISP directives which are binding across government ministries does not fall (either directly or by implication) within the functions and responsibilities of the Ministry of Information and Communication Technology (MOICT) as defined in article (3) of the Telecommunication Law No. 13 for the year 1995. ⁽ⁱ⁾</p> <p>As well, The authorities and functions of the Telecommunication Regulatory Commission also do not authorize the Commission clearly to issue inter-ministerial “security mandates” of the nature envisioned in the ISP. ⁱⁱ</p> <p>Given the extensive, dynamic and ongoing character of the ISP imperatives, and the consequences of non compliance, it would not be legally plausible to mandate them by voluntary self imposed agreement of ministry officials.</p>	<p>OMB, and an annual OMB report to Congress.</p> <p><u>OMB Responsibilities:</u> The <i>Security Act</i> codifies existing OMB policy, OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources", and reiterates the requirements of the Computer Security Act of 1987, the Paper Reduction Act, and the Clinger-Cohen Act.</p> <p>Under the <i>Security Act</i>, agency-wide security programs are subject to OMB "approval." The Director of OMB has the authority to direct agencies to identify, use, and share best security practices; develop an agency-wide information security plan; incorporate information security principles and practices throughout the life cycles of the agency's information systems; and ensure that the agency's information security plan is practiced throughout the life cycles of the agency's information systems. In addition, the Director shall establish government-wide policies for the management of programs that support cost-effective security of Federal information systems by promoting</p>	<p>It is recommended that such an instrument be a Law which establishes general legal framework, and whereby specific aspects would be provided for by regulations or instructions issued pursuant thereto.</p> <p>The legislation would also define the specific roles and degree of responsibilities and accountability of different employees.</p>

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
		<p>security as an integral component of each agency's business operations and include information technology architectures as defined under the Clinger-Cohen Act.</p> <p><u>Agencies Responsibilities:</u> The <i>Security Act</i> names specific authorities, responsibilities, and functions for the agency, the head of the agency, agency program officials, and the CIO of the agency.</p> <p>The Act improves federal agency performance in protecting information by making agencies accountable for their security programs. It requires agencies to have an annual independent audit of their information security programs and plans. All agency programs shall include procedures for detecting, reporting and responding to security incidents.</p> <p>The Act defines responsibilities of programs officials who shall assess the risk to the operations and assets over which they have control. In addition, the Act defines responsibilities of agencies' heads and Chief Information Officers.</p> <p>Furthermore, it defines responsibilities of</p>	

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
		<p>certain agencies such as Department of Commerce through the National Institute of Standards and Technology which shall develop uniform guidelines for Federal computer systems relating to security control.</p> <p>Likewise see the Indian Example, Information Technology Act of 2000, and the Rules issued pursuant thereto, which deal with security.</p>	
<p>The above has outlined the main gap in current legislation and identified a general need for a legislative instrument that provides the foundation for E-Security legal Governance. The following will further provide detailed analysis of the legal requirements of specific aspects and components of SGN security, and the extent of coverage under current legislation.</p>			
<p>Information Technology Security</p>			
<p>Information asset ownership and custodianship.</p> <p>Each asset must have a single nominated owner. The information Asset Owner (IAO) will be held accountable for ensuring the security of their assets.</p> <p>The Information Asset Custodian will be held accountable for implementing the security controls specified by IAO. Individuals must be uniquely identifiable. The method of authentication to information processing facilities must reflect the classification of, and risk</p>	<p>No applicable legislation. See below for scope and nature of responsibility for official documents.</p>	<p>This and other specific requirements are governed pursuant to Security Acts.</p>	<p>Legislation must include provisions mandating ownership and specifying individual responsibility for assets and actions performed thereupon.</p>

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
<p>to the subsequently accessible assets Individuals will be held personally accountable for all actions performed under their unique identify regardless of whether they actually performed the actions or not.</p>			
<p>Information management/ Information classification</p> <p>Assets to be formally identified (by IAO), to be ensured appropriate level of protection commensurate with the risk of their unauthorized disclosure, modification or unavailability.</p> <p>Information assets to be classified to determine level of protection required.</p> <p>Procedures to be defined to ensure IA are correctly labeled. For each of the four classification levels (low, medium, high and extreme) and for each of the classification components (confidentiality, integrity and availability).</p> <p>IAO must formally manage the risk to their assets by commissioning security controls to preserve appropriate levels of confidentiality, integrity and availability.</p>	<p>There is no requirements much less systematic criteria s for information classification under Jordanian legislation. Various laws stipulate specific rules relating to information with respect to level of disclosure allowed. The criteria of classification is typically related to the extent of disclosure and public accessibility.ⁱⁱⁱ (see part II: SGN and Data Sharing and Annex) More comprehensive criteria for classification is required that takes into account each of the security relevant components criteria: namely, confidentiality, integrity and availability.</p> <p>As well- there is no legislative provision under current law mandating the classification of all information generally or for purposes of protection thereof. Nor is there any provision stipulating risk assessment for purposes of determining required level of protection.</p>	<p>Approach of classification of Information varies according to countries.</p> <p>US Example The <i>Computer Security Act of 1987</i> requires that each agency consistent with standards, guidelines, policies and regulations shall establish a plan for the security and privacy of each Federal computer system identified by that agency that is commensurate with the risk and magnitude or the harm modification resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. The measures used for protecting sensitive information shall be cost-effective and commensurate with the risk and magnitude of harm.</p> <p>INDIAN Example Information assets shall be classified according to their sensitivity and their importance to the organization. Classification of information is defined</p>	<p>The proposed Security Legislation shall include provisions mandating information classification, information risk assessment and risk management and shall assign clear responsibilities for such. Without such it would be difficult to gage the level of protection required.</p>

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
		<p>in Rules for IT Act 2000 under Schedule III entitled “<i>Information Technology Security Guidelines</i>”</p> <p><u>NEW ZEALAND</u> <u>Example</u> Information is classified as <i>sensitive</i> or <i>in confidence</i>. Sensitive: Compromise of information would likely to damage the interests of New Zealand government or endanger the safety of citizens. <i>In confidence</i>: Compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect the privacy of its citizens.</p>	
<p>Access to information assets:</p> <p>-Access to information assets to be based on the least privilege and need-to-know so as to ensure their appropriate use. (Likewise with respect to access to facilities).</p>	<p>Jordanian law includes various general as well as specific provisions governing disclosure of information (See Annex). However, there are no provisions regulating access (see recommendation for difference between access and disclosure issues).</p> <p>Moreover, Jordanian information addresses issue of access with respect to disclosure/confidentiality and not security generally.</p> <p>Moreover, there are many instances where the law does not specifically provide for issue of</p>	<p><u>INDIAN Example</u></p> <p>-According to the Rules for IT Act 2000 under Schedule III “<i>Information Technology Security Guidelines</i>” : The “System Administrator” managing and controlling the protective security measures of the computer system shall authorize privileged access to users only on a need-to-know and need-to-do basis and also only after the authorization is documented.</p>	<p>The proposed Master legislation relating to IT Security must clearly regulate access on a needs-to- know or needs to do basis by government employees. This is a distinct issue then the issue of public access which is specifically handled by several Jordanian legislations. Such provisions would regulate access not only to particular pieces of information, but to Information Asset Systems and Public Record Systems, for purposes of preserving not only confidentiality but also integrity and availability. (E.G: Some information may be publicly accessible (full disclosure criteria) even while access to the information system and records are regulated (to preserve integrity and availability from security standpoint).</p>

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
	<p>access to information or documents, and where there is such a provision, it is not sufficiently clear to establish access of a need to know basis only.</p> <p>Perhaps, Article 10 of the Law protecting State Secrets and Documents No.50 of 1971 is the closest general provision approximating the requirements for restricting access on needs to know basis, as it states “Notwithstanding the provisions of any other law, all other official documents not included in this law shall be considered Ordinary Documents. Officials shall protect these Ordinary Documents against tampering or loss. The contents of these documents may not be revealed to persons other than those concerned, unless the publication thereof is authorized.”</p>		
<p>Access across ministries and government agencies^{iv}.</p>	<p>No provision addressing cross agency responsibilities, other than general provision mandating responsibility for safeguarding official documents cited above .</p>	<p><u>US Example</u></p> <p><i>Paper Work Reduction Act</i></p> <p>Cooperation of agencies in making information available: The Director of OMB may direct an agency to make available to another agency, or an agency may make available to another agency, information obtained by a collection of information if the disclosure is not inconsistent with</p>	<p>The Master IT security legislation should transfer to the receiving/ accessing agency same security requirements and responsibilities applicable to the sending agency.</p>

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
		<p>applicable law. If information obtained by an agency is released by that agency to another agency all the provisions of law (including penalties) that relate to the unlawful disclosure of information apply to the officers and employees of the agency to which information is released to the same extent and in the same manner as the provisions apply to the officers and employees of the agency which originally obtained the information. The officers and employees of the agency to which the information is released, in addition, shall be subject to the same provisions of law, including penalties, relating to the unlawful disclosure of information as if the information had been collected directly by that agency.</p> <p><u>INDIAN Example</u></p> <p>According to the Rules for IT Act 2000 under Schedule III “<i>Information Technology Security Guidelines</i>”: Access to the computer systems by other organizations shall be subject to a similar level of security protection and controls as in “<i>IT Security Guidelines</i>”.</p>	

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
Third party access: To be monitored, controlled and contractually bound with ISP.	Not specifically addressed by Jordanian Legislation	<p><u>INDIAN Example</u></p> <p>According to the Rules for IT Act 2000 under Schedule III “<i>Information Technology Security Guidelines</i>”: Access to the computer systems by other organizations shall be subject to a similar level of security protection and controls as in “<i>IT Security Guidelines</i>”.</p> <p><u>US Example</u></p> <p>Computer Security Act: The term Federal "federal computer system" is used to delineate the reach of the Act to include federal agencies, contractors of federal agencies, and other organizations that process information using a computer system on behalf of the federal government to accomplish a federal government function.</p>	The Master IT Security legislation would include provisions mandating contractual arrangements with third parties which stipulate contract obligations regarding access and disclosure and would specify minimum indemnities or penal conditions for non-compliance. In addition third party obligations and penalties for non-compliance therewith can be stipulated within Master legislation.
Assets and information processing facilities should only be used to meet the legitimate business needs of e-government.			
Physical and Environmental Security -Equipment Security.	<p>There is no provision in the Jordanian law banning the transfer of the equipment from one site to another, even the equipment which contains confidential information which should not be disclosed.</p> <p>Moreover, Jordanian law does not clearly provide</p>	<p><u>INDIAN Example</u></p> <p>-Rules for IT Act 2000 under Schedule III “<i>Information Technology Security Guidelines</i>” include “Physical and operational security” under which topics such as site design, fire protection and</p>	The Master IT legislation would include provisions governing all aspects of IT security, including Physical and Environmental Security, the applications of General controls, Network management, Change control, Media management, and System Audit Considerations. This would include provisions such as :

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
<p>-Secure area.</p> <p>-General controls.</p> <p>-Network management: Network servicing e-Gov to have clear defined boundaries and managerial responsibilities.</p>	<p>for the protection of the places which host confidential or sensitive information or for banning entry to the places thereto except in the case of the places which contain confidential documents or information pertaining to the security of the State. This is stipulated by Article (14) of the Law on the Protection of the Secrets and Documents of the State, which provides: Any person entering or trying to enter a prohibited place for the places of obtaining secrets or protected documents or information that should remain confidential by reason of the protection of the security of the State should be punished by temporary imprisonment with hard labor. If the attempt is made for the benefit of a foreign country, penalty shall be life imprisonment with hard labor for life. If the foreign country concerned is an enemy state, death penalty applies.</p> <p>The above provision cannot be applied to all government places which have documents or information, even if they were confidential, if such are unrelated to the internal or external security of the State.</p> <p>Other than the above, Jordanian law does not specifically provide for e-Gov. specific issues related to the applications</p>	<p>environmental protection, physical access are addressed.</p> <p>-Notions such as Security Zone and High Security Zone are envisaged in Schedule V of Rules for IT Act 2000.</p> <p>-“IT Security Guidelines” include “System integrity and security measures” concerning the use of security systems or facilities, system access control, password management etc.</p> <p>US Example <i>Government Information Security Reform Act</i> aims at providing a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets.</p> <p>INDIAN Example “IT Security Guidelines” envisages “Network Communications Security” issue to ensure that all sensitive information on the network shall be</p>	<p>1-Provisions banning unauthorized transfer of the equipment from their place to another place for any reason, and providing penalties for violations.</p> <p>2- Provisions restricting access not only to information but to Network areas with attendant penalties thereupon.</p> <p>3- Legal provision mandating practices and levels of protection proportionate to sensitivity of information.</p> <p>4- Provision mandating clear boundaries for networks servicing e-Gov to have clear defined boundaries and managerial responsibilities in order to be applied to the critical classification of Network management.</p> <p>5- Provision setting mandatory procedures to secure media, input/output data and documentation for information processing facilities from damage, theft and unauthorized access. Media must be securely decommissioned at the end of its lifecycle.</p> <p>6- Provisions regulating and restricting access to Audit tools to be controlled, and kept isolated from development and operational information processing facilities to prevent unauthorized access.</p>

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
	<p>of General controls, Network management, Change control, Media management, and System Audit Considerations which were explicitly addressed by ISP & international IT related security legislation.</p>	<p>protected by using appropriate techniques. Physical access to communications and network sites shall be controlled and restricted to authorized individuals. Each organization shall have a Network Administrator who will be responsible for operation, monitoring security and functioning of the network.</p> <p><u>US Example</u> The <i>Computer Security Enhancement Act of 1997</i> updates the <i>Computer Security Act</i> by including references to computer networking which has become an increasingly important component of the Federal Government information technology system. The Act “recognizes the highly networked nature of the Federal computing environment including the need for Federal Government interoperability and, in the implementation of improved security management measures, assure that opportunities and interoperability are not adversely affected.”</p> <p><u>INDIAN Example</u> “<i>IT Security Guidelines</i>” Change control: Procedures for tracking and managing changes in applications software, system software, hardware and data in the production</p>	

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
<p>-Change control: A formal process for control over the implementation of change to be established.</p> <p>-Media management: Procedures to be developed to secure media, input/output data and documentation for information processing facilities from damage, theft and unauthorized access.</p> <p>-System Audit Considerations.</p>		<p>system shall be established.</p> <p>Organizations responsibilities for the change management process shall be defined and assigned.</p> <p>-Media management: The “<i>IT Security Guidelines</i>” include the Media management issue. Responsibilities for media library management and protection shall be clearly defined and assigned. Access to media shall be restricted to the authorized persons only.</p> <p>”<i>IT Security Guidelines</i>” envisages Audit trails and verification issues. Procedure used to validate that controls are in place and adequate for their purposes. The audit includes recording and analyzing activities to detect intrusions or abuses into an information system. Inadequacies found by an audit are reported to appropriate management personnel.</p>	
Training and Awareness			
Employees to receive training and awareness commensurate with their roles and responsibilities.	No provision mandating such.	<p>US Example</p> <p><i>Computer Security Act of 1987</i></p> <p>Requires federal agencies to provide for the mandatory periodic</p>	IT Security master legislation would provide as appropriate for mandatory training for employees managing or operating Information systems requiring certain skill levels.

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
		<p>training in computer security awareness and accepted computer security practice of all employees who are involved with management, use or operation of a federal computer system within or under the supervision of the federal agency.</p> <p><i>Computer Security Enhancement Act of 1997</i> amends the <i>Computer Security Act of 1987</i> to revise requirements regarding Federal computer system security training to require such training to include emphasis on protecting sensitive information in Federal databases and Federal computer sites.</p> <p><i>Paperwork Reduction Act of 1995</i>: With respect to general information resources management policy, development and implementation of best practices in information resources management, including training.</p> <p><i>Government Information Security Reform Act</i> highlights the importance of information technology training of government workers.</p> <p><i>Appendix III to Office of Management Budget Circular No.A-130- Security of Automated Information Resources</i>: Ensures that all individuals are appropriately trained in</p>	<p>Legislation would also authorize specialized certifying body (ies) to conduct and approve training.</p>

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
		<p>how to fulfill their security responsibilities before allowing them access to the system.</p> <p><u>INDIAN Example</u> A Certifying Authority shall ensure that all personnel performing duties with respect to its operation shall receive comprehensive training.</p>	
Disciplinary measures	<p>Jordanian law distinguishes between employee violations which are viewed as administrative violations subject only to disciplinary measures and violations and misdemeanors that are subject to criminal penalties provided for by law as follows:</p> <p>1- Unless otherwise specified, violations of the provisions of the laws in force at the department in which the employees are working, or of the administrative decisions issued thereto by the higher administrative authority are subject to disciplinary administrative measures which range from reprimand through termination and dismissal from the job^Y.</p> <p>Specific laws may stipulate specific disciplinary measures, as we mentioned earlier in Article 47 of the Income</p>	<p><u>INDIAN Example</u> <i>Criminal offences stipulated by IT Act 2000</i> Chapter XI (Sections 65 to 75) of the IT Act prescribes the civil offences which covers:</p> <ul style="list-style-type: none"> • Tampering with computer source documents (i.e. listing of programs) • Hacking with computer system • Electronic forgery I.e. affixing of false digital signature, making false electronic record • Electronic forgery for the purpose of cheating • Electronic forgery for the purpose of harming reputation • Using as genuine a forged electronic record • Publication of digital signature certificate for fraudulent purpose • Unauthorized access to protected system • Confiscation of computer, network, etc. • Misrepresentation or suppressing of material face for obtaining 	<p>There is a need to assess the extent to which criminal penalties (w may range from fines to imprisonment) are required for serious violations of security provisions. If need is identified, then the penal violations and consequences thereof shall be provided for by law</p>

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
	<p>Tax law No. (57) for the year 1985 .</p> <p>2- Violations are subject to criminal penalties only if such violations and applicable penalties are specifically provided by law, and in which case, violations are referred to public prosecutor or court. Article 150 of the Civil Service Regulations states:^{vi}</p> <p>The penal code only criminalizes certain actions which may be pertinent to IT security.</p> <p>Article 355 of the Penal Code provides: Each of the following shall be sentenced to a prison term of no more than three years:</p> <p>1- A person who by virtue of his job or official position obtained official secrets and disclosed them to those who are not empowered to have access thereto, or to those whose nature of work does not require access thereto, as dictated by the public interest.</p> <p>2- A person who in the progress of performing an official duty or government service kept in his possession secret documents, drawings, sketches, models or copies thereof without having the right to do so or without the nature of his job requiring so.</p> <p>3- A person who by</p>	<ul style="list-style-type: none"> • Breach of confidentiality and Privacy • Publishing false Digital Signature Certificate <p><u>US Example</u></p> <p>United States has carried out elaborate amendment classifying the following as computer crimes :</p> <ul style="list-style-type: none"> • Knowingly access of computer without authorization related to national defense or foreign relation • Intentional access of computer without authorization to obtain financial information • Unauthorized access of computer of a Government Department. or agency • Unauthorized access of computer of federal interest with intent to defraud • Knowingly causing transmission of data/program to damage a computer network, data or program or withhold or deny use of computer, network etc. • Knowingly causing transmission of data/program with risk that transmission will damage a computer network, data or program or withhold or deny use of computer, network etc, an unauthorized access of computer with intent to defraud. 	

Background	Jordanian Legislation	International Practices	Assessments & Recommendations
	virtue of his profession knew of a secret and disclosed it without any legitimate reason.		

Part II

Legal Aspects of SGN Messaging and Directory Services

A-Background and Introduction

As part of the e-government initiative, plans are already underway to implement a government-wide service, for messaging and directory services (MDS) that can be utilized to support all Departments. The said service is intended to enable reliable department-to-department communication and workflow, and provide an enterprise directory of Government employee information. (MDS) will integrate closely within the infrastructure deployed as part of the SGN project, which provides secure managed connectivity between the government network, the Departments network and the internet.

As reported by AMIR program technical advisor,¹ in practice, the security of e-mail messages within SGN will draw significantly upon the secure features of the SGN network as well as proper use of multilevel user/account password schemes. This is deemed to provide a high level of reliability for most messages within a secure *closed intranet*. Although the MDS system employed will be supported with the option of digital certified signatures, (PKI technology; authentication certificates), this option will be generally disabled and will be available to select users only, and on a limited basis. Indeed, a pay-per-use model may be employed to ration uses of this facility, and therefore limit excessive administrative costs associated therewith. In other words, the preference is to curb use of digital signature in routine cases, and limit such to cases dictated by concerns such as confidentiality, and communications of significant legal import.

In light of the foregoing, the report examines the legal issues pertaining to the use of e-mail messages in internal administrative communications (henceforth public administration). In conducting the legal assessment, it has been considered that use of MDS will not be limited to generic, routine, or legally inconsequential communications. Rather, it has been presumed that MDS would eventually serve a potential substitute platform for all written administrative. This includes any communications exercised in the discharge of an administrative duty or authority, whatever the legal import, nature, sensitivity or confidentiality of the subject matter. Viewed in this perspective, use of MDS raises important legal concerns and warrants the following extensive discussion.

B- Legal components of effective administrative communications

In order to promote effective and widespread use MDS facility across government, it is imperative to reduce to a tolerable level the legal uncertainties associated therewith.

Such uncertainties may arise with respect to the following aspects of e-mail messages:

- (1) Validity: i.e. do e-mail messages fulfill the legal requirements of written communication and generate the same legal effect. (For example, is a warning notice that is served electronically deemed to meet the requirement of a written notice, or would such be considered invalid, and as such ineffective)

¹ Interview with Abed Shamlawi, Technical Adviser, AMIR Program, ICTI Component.

(2) **Authoritativeness:** Is the recipient of electronic messages entitled to/ obliged to act upon the knowledge generated by content of such message? Is an instruction, notice, warning, decision received electronically binding upon the recipient? To what extent can it be repudiated by recipient on the principle ground of lack of intrinsic authority of such messages? On grounds of lack of reliability or authentication?

(3) **Evidentiary Weight:** Do e-mail messages constitute admissible evidence in court, and what are their documentary/ evidentiary strength.

In order to reduce regulatory barriers to use of MDS, legal uncertainties about issues of validity, authoritativeness, and evidentiary strength of e-mail messages within SGN context must be eliminated. Moreover, the technical conditions for authenticity and authoritativeness must not also be reliable also be also feasible and cost-effective

C- Legal aspects of writing in administrative communication:

It is important to take into account the following legal aspects of the use of writing in administrative communication in evaluating any legal requirements pertaining to e-mail.

- Although writing is customarily used in most legally consequential administrative documentations, use of writing is often not mandated specifically by law, but rather by customary practice.
- Most signed/ stamped written administrative communications enjoy the evidential weight of ordinary documents. This means that the contents of such documents constitute admissible evidence about consent/intent of signatory, unless, the latter disproves attribution thereto.
- The authoritativeness of written documents in administrative communication does not derive so much from their intrinsic reliability. Rather, it derives from their legal recognition, customary practice, and their stipulated evidentiary strength as ordinary documents. Such features combined lead recipients to act upon contents of written administrative communication, without verifying or actively seeking further assurances about authenticity, even if they may be unfamiliar with the sender's signature, and unless they have reason to believe otherwise. This must be kept in mind in assessing the plausibility of any technical reliability standards proposed for electronic messages.

D- MDS and current legislation

I-Unlike what may be presumed, it is not evident that Jordan's recently enacted E-transactions Law No. 85 of 2001 (E-transactions law) is applicable to use of e-mail in discharge of administrative duties and responsibilities(henceforth public administration) as the following indicates:

Article (3) of the e-Transactions law provides:

- (a)The objective of this Law is to facilitate use of electronic means in conducting **transactions** subject to the provisions of any other laws and without prejudice thereto.

- (b) In applying the provisions of this Law, account shall be taken of *international commercial customs* pertinent to electronic transactions and degree of progress in methods thereof.

Article (4) states:

The provisions of this law shall apply to:

- (a) Electronic *transactions*, electronic records, electronic signatures, and any electronic message
- (b) **Transactions** adopted by any government department or public body in part or in whole.

Article (5) provides:

- (a) The provisions of this law shall apply to transactions in which *parties agree* to conduct their transactions in electronic means, unless otherwise provided.
- (b) For the purposes of this article, the consent of parties to conduct a specific transaction by electronic means does not bind them to conduct other transactions by such means.

Whereby article (2) defines *transactions* as:

“A procedure or procedures conducted between two or more parties with the purpose of creating obligations upon one or mutual obligations between more than one party and pertaining to a commercial activity, or a civil obligation or to a *relationship with any government* department.

Accordingly, the e-transaction law applies to government transaction only in so far as the government is party to a commercial transaction (procurement, buying), or is “transacting” with the public, as a service provider, regulator, licensor, etc. The definition of transaction does not include internal administrative communications. Such communications are legally consequential in so far as they pertain to exercise of legally stipulated rights and authorities. However, they do not give rise or pertain to “obligations” in the sense referred to by the Law.

Moreover, as article 5 indicates, the law does not mandate or impose use of electronic means and transaction. Rather, it applies strictly where parties agree to conduct their transactions by electronic means, and on a case by case basis. This consensual model is appropriate in commercial context where parties have the option means of communication and standards of reliability appropriate for their circumstance. Such an approach is not plausible in context of public administration where uniformly applicable rules are expected and required. The authoritativeness and validity of e-messages in context of public administration context must be grounded in generally and universally applicable rules that are binding on senders and recipients.

Last but not least, the e-transactions law draws almost exclusively on the UNCITRAL model laws on e-commerce and draft model law on electronic signatures. Such laws are explicitly intended to resolve issues of legal uncertainty associated with the use of

electronic means in private commercial transactions conducted in context of open networks. In respect of this, it is stated:

“Focused on the private-law aspects of commercial transactions, the Uniform Rules do no attempt to solve all the questions that may arise in the context of the increased use of electronic signatures. In particular, the Uniform Rules do not deal with aspects of public policy, *administrative law*, [emphasis added] consumer law or criminal law that may need to be taken into account by national legislators when establishing a comprehensive legal framework for electronic signatures.^{2z}

Non-withstanding the foregoing, it may be argued that article (4) (b) is sufficient to extend scope of law to all electronic messages, regardless of context. Thus, the law would serve at least to lend legal validity to e-messages in general. This article however does not stand alone, but should be read together with other articles above pertaining to scope.

In any case, the above highlights that the applicability of the e-transactions law to administrative communication is at best inconclusive, at worse, and unlikely. To eliminate such uncertainty, ***it is recommended to solicit a binding opinion about the applicability of e-transactions law to internal administrative communications.***

2- The provisions of the e-transactions law regarding the authoritativeness and evidentiary value of uncertified electronic messages are inconclusive. Further, the more plausible interpretation of such provisions would impose excessive and costly authentication standards that are not justified within a closed secure network:

Article (32) of the e-Transactions law states:

Unless otherwise proven, the following presumptions prevail:

1-A certified electronic record has not been changed or altered as of date of certification procedures

2- A certified electronic signature is issued to the person to whom it is attributed, and is used thereby to indicate consent of the documents content.

B- If an electronic record or signature is not certified it has no [authoritativeness/evidentiary weight/probative value--translation depends on interpretation of term حجية as used in this context.

The wording of subparagraph (B) above stipulates that that non-certified electronic messages and signature carry no evidentiary weight or authoritative value. This would imply that a recipient of such document could not and should not act upon them. Further, such documents would not even constitute admissible evidence in court.

The above interpretation would preclude on legal grounds use of non-certified messages for any legally consequential communication. This provision which may be warranted in

² UNCITRAL a/CN.9/WG.IV/WP.84 8 December 1999; United Nations Commission on International Trade Law: Working Group on Electronic Commerce; Thirty sixth session; New York 14-25 February 2000

context of open private networks, is entirely unjustified in context of SGN. As stated above, in context of SGN messages signed electronically would have a reasonable degree of reliability, equivalent to, if not higher than reliability of paper based written and signed document. The universal requirement of certification for authoritative would be costly, ineffective and inconsistent with government policy.

The foregoing interpretation of the law is arguably inconsistent with overall spirit and thrust of the law. Article 7, 10, and 15 all imply that electronic messages have evidentiary weight (admissible in court). Moreover, Article (13) of the Evidence Law No. 30 of 1952 (as amended) assigns to e-mail messages the evidentiary weight of ordinary documents, which is equivalent to the evidentiary strength to ordinarily signed written documents (This means that the content of such documents is admissible evidence about their author's consent unless the latter disproves their) In this respect, it may be argued that article should be interpreted to mean that non-certified e-mail messages have no *probative value*, i.e. that no prima facie presumption may be made about their authenticity. However, it should not be construed to mean that they have no evidential weight.

The fact remains however, that the language of article (32) is very categorical in denying evidentiary weight to uncertified messages. The less restrictive interpretation is desirable and perhaps partly plausible, but is risky. The validity and authoritative of SGN needs to be grounded in higher level of certainty.

It is highly recommended to adduce a binding definitive interpretation of Article (32) . If the more restrictive interpretation prevails, there may be a need to amend the law to take into account specific features and needs of administrative communications in context of SGN.

3- The e-Transactions does not eliminate major uncertainties with respect to the authoritative of e-mail in administrative communications.

The e-transactions law validates but does not give mandatory authoritative to communications through electronic means. The principle acceptance of validity and authoritative of such communications rests upon mutual consent of “transacting parties.” This model which is appropriate in context of commercial contractual transactions does not provide adequate basis for regulating e-messages in government. To eliminate legal uncertainty about use of e-mail for administrative duties and responsibilities, the law must validate such messages as well as mandate their authoritative.

4- In light of the foregoing It is therefore highly recommended to enact specific legislation regulating use of electronic communication in public administration and within a closed secure network. Unlike, the current E-transactions law, the proposed legislation would address the unique features and requirements of administrative communication within a closed and secure government network. As it supports efficient back-office communications in government , it constitutes a fundamental legal requirement of e-government.

The proposed legislation would regulate among other things the following:

- **Validity of e-messages in fulfillment of writing requirements**
- **Authoritativeness of e-messages**
- **Rules and requirements governing attribution in SGN closed network context**
- **Rules governing deemed dates and place of dispatch and receipt.**
- **Special standards and requirements for e-mail dispatch of confidential and sensitive material or as appropriate for messages of high legal import**
- **Signature and attribution.**
- **Use and abuses of network e-mail facility.**
- **Mandatory use of e-mail for purposes of paper use reduction**

Part III

SGN and Legal Aspects of Data-Sharing

A key objective of e-government and SGN would be to facilitate and perhaps further promote intra-department data sharing and data exchange, whether through file transfer or through authorized access to common databases. This raises issues with respect to legal permissibility of intra-government data sharing.

This part of the report assesses the implications of Jordanian Legislation with respect to inter-departmental sharing of data maintained by government. It examines the provisions of applicable legislation in this regard, identifies the level of data sharing currently permitted, as well the degree of legal uncertainty/ risk involved in such exchanges. Further, taking into account international practice, it provides legal recommendation for more effective governance of this issue, which is inevitably bound to gain legal prominence due to the possibilities and opportunities unleashed by technology. The detailed findings of this review are presented and documented in details in **Matrix (2): Legal Assessment of Data-Sharing Provisions in Jordanian Legislation and Matrix (3) Data Sharing and Disclosure: Status in Specific Laws.**

The salient findings and recommendations of this assessment may be summarized as follows:

- Jordanian legislation does not provide elaborate and clear guidance regarding the legal permissibility of data sharing much less regulate the various aspects of such, and the responsibilities attendant thereupon.
- *There is need to enact legislation that would eliminate legal risks entailed in inter-departmental data sharing and regulate all aspects of such. The proposed legislation would provide general criteria for data sharing and mandate government entities to characterize status of data with respect to availability and disclosure. As well, it would regulate various aspects of data sharing, define attendant responsibilities upon data providers and recipients, and attach consequence upon non compliance. As well, there is a need for legislative provisions mandating data sharing and cooperation in a manner consistent with applicable laws. This is necessary in order to eliminate unjustified customary resistance to data sharing that may decelerate the pace of e-government.*
Although the need for the aforementioned legislation may not be an immanent prerequisite of launching e-government, it is ultimately inevitable for its sustainable growth .

Matrix (2): Legal Assessment of Data-Sharing Provisions in Jordanian Legislation

SUBJECT	JORDANIAN LEGISLATION	RELEVANT RECOMMENDATIONS FROM INTERNATIONAL PRACTICES	RECOMMENDATIONS
Formal barriers to electronic Data sharing ^{vii}	<p>There are restrictions in the law applying specifically to electronic access and data sharing, where information access and data sharing would otherwise be permitted.</p> <p>As list of laws in Annex I indicates, the language pertaining to data and information sharing and disclosure is not medium specific.</p> <p>This feature is further corroborated by the E-transactions law which recognizes the validity of e-records and duly authenticated electronically transferred files and documents (See Part III: SGN and e-mail communication.)</p>		NA
General Provisions governing inter-agency information sharing	Jordanian legislation does not provide elaborate and clear guidance regarding legal permissibility of data sharing between government entities, much less	Data Sharing is dealt with generally in the context of Privacy Laws, Information Cooperation Laws, Information Security Laws, etc.	To eliminate legal risks entailed in data sharing and clearly regulate all aspects of such , clear legislation should be enacted addressing

SUBJECT	JORDANIAN LEGISLATION	RELEVANT RECOMMENDATIONS FROM INTERNATIONAL PRACTICES	RECOMMENDATIONS
	<p>regulate fully the various aspects of such exchange and responsibilities attendant thereupon.</p> <p>The main general legal provisions which pertain to this are:</p> <p>-Article 7 of the Jordanian constitution which provides that “Personal Freedom” is a right upheld. A survey of scholarly juristic literature indicates that such rights have been interpreted to include the right to preserve privacy of information^{viii}. Thus, it may be argued that Jordanian Constitution protects individuals rights to privacy in relation to personal information, and that such a right may be qualified or subject to exceptions only as specified by Law.</p> <p>-Article 10 of the Provisional Law on the Protection of the Secrets and Documents of the State No.50 of 1971</p>	<p>The laws government issues starting with what data may be solicited as well as issues related to disposal therewith.</p> <p><u>US Example:</u> <i>Privacy Act:</i> Agency requirements: Each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute...” (NB: The term “maintain” includes maintain, collect, use, or disseminate)</p> <p>-In transferring data between government bodies, these bodies shall ensure the integrity of the transferred data. Thus, the data protected by a given body shall also be granted an</p>	<p>generally various aspects of data sharing. Such would include clear criteria on how data is to be handled in absence of specific legal provisions thereabout , the responsibilities attendant upon data sharing on sender/provider and recipient, etc, the consequences for non-compliance, as well as and inevitably issues of what data may be collected or maintained.</p> <p>Although such legislation may not be an immediate prerequisite for SGN, they must be addressed sooner rather than later. As SGN stimulates the need and tendency towards greater data exchange, it would be essential to have clear guidance on all aspects of such, especially as they pertain to privacy. Such laws are becoming a critical foundation of any solid e-government system.</p>

SUBJECT	JORDANIAN LEGISLATION	RELEVANT RECOMMENDATIONS FROM INTERNATIONAL PRACTICES	RECOMMENDATIONS
	<p>provides:</p> <p>Notwithstanding the provisions of any other law, all other official documents not included in this law shall be considered Ordinary Documents. Officials shall protect these Ordinary Documents against tampering or loss. The contents of these documents may not be revealed to persons other than those concerned, unless the publication thereof is authorized.</p> <p>This article may be construed to provide general provision against disclosing even regular documents to other than “interested parties”, unless publicizing thereof is explicitly permitted. Whether government entities are considered “interested” parties is not clear.</p> <p>The general guidance in constitution and other legislation on matters of sharing</p>	<p>equivalent level of protection in the transfer process to another body. In other terms, shared information shall be equally protected from one body to the next.</p> <p>In the US, data sharing issues –inter alia- are handled in various legislation among which:</p> <ul style="list-style-type: none"> • Privacy Act/Computer Matching and Privacy Protection Act • Freedom of Information Act • Homeland Security Act • Paper Work Reduction Act of 1995 • Government Information Security Act 2000 • E-government Act 2002 <p>It is generally agreed that obtaining consent is required prior to collecting, using or disclosing personal information. Consent is particularly important when collecting, using or</p>	

SUBJECT	JORDANIAN LEGISLATION	RELEVANT RECOMMENDATIONS FROM INTERNATIONAL PRACTICES	RECOMMENDATIONS
	<p>and disclosure is not definitive. In the absence of criteria as to what constitutes personal information, and who qualifies as an interested party, the legal validity of inter-government data- sharing of information, in cases where such is not explicitly permitted by law could always be in question.</p> <p>This overall feature of the law is favorable if viewed from vantage points of guarantees for privacy. (Although not sufficient as a clear guidance). However, it can be unnecessarily restrictive, and may lead to excessive and unjustified conservatism in data sharing in cases where no explicit restrictions apply.</p> <p>In summary, there is a gap under current legislation with respect to detailed guidelines on data sharing, which take into account concerns for privacy</p>	<p>disclosing sensitive personal information.</p> <p><u>OECD Guidelines</u> on the Protection of Privacy and Transborder Flows of Personal Data: There should be limits to the collection of personal data by lawful means and, where appropriate, with the knowledge or consent of the data subject. Furthermore, personal data should not be disclosed, made available or otherwise used for purposes other than those specified (related to the “purpose specification principle”) except with the consent of the data subject; or by the authority of law.</p> <p>Legislation allows personal data disclosure except with the consent of the individual to whom it relates.</p> <p><u>US Example:</u> Privacy Act: “Conditions of</p>	

SUBJECT	JORDANIAN LEGISLATION	RELEVANT RECOMMENDATIONS FROM INTERNATIONAL PRACTICES	RECOMMENDATIONS
	<p>as well as e-government and SGN needs for facilitating a certain level of data sharing.</p> <p>See annex for detailed survey of disclosure provisions in Jordanian laws.</p>	<p>Disclosure: No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be -</p> <p>(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;</p> <p>(2) required under section 552 of this title...”</p>	
Specific provisions about Data Sharing.	Most laws surveyed include provision regarding the extent of accessibility/ disclosure of related data and records and the conditions for	Many legislation mandate by law a clarification to the person submitting it and upon submission of the status of Data and	There is a need for general criteria regarding data sharing as well as a mandate for government entities to characterize

SUBJECT	JORDANIAN LEGISLATION	RELEVANT RECOMMENDATIONS FROM INTERNATIONAL PRACTICES	RECOMMENDATIONS
	<p>such. Typically the validity of inter-government sharing is not specifically addressed. Rather, if data and records are characterized regarding disclosure, this is in relation to the public generally. In this respect, data in Jordanian legislation is either confidential and not subject to disclosure, confidential and subject to disclosure only upon order of court or competent authority, accessible to interested parties only, or publicly accessible subject to certain fees, or procedures or even unconditionally. However, there are many cases where data is not specifically characterized. The implications of such provisions for inter-government data sharing may be obvious in cases where information is confidential or publicly accessible. However, the legal status of inter-government data sharing in cases</p>	<p>the extent of accessibility thereto.</p>	<p>status of all data collected and maintained thereby.</p>

SUBJECT	JORDANIAN LEGISLATION	RELEVANT RECOMMENDATIONS FROM INTERNATIONAL PRACTICES	RECOMMENDATIONS
	<p>where interest is a condition for disclosure. Indeed some government officials suggested that they would avail such data while other expressed reservation.</p> <p>The status of inter-government data sharing where data is not specifically characterized is also unclear.</p> <p>Note for example, for example Article 34 The Investment Promotion Law No. 16 for the year 1995 provides: “It shall be permitted to register mortgages on equipment and machinery that are part of the Fixed Assets of any project; as security for extended credit facilities. For the purposes of implementing the provisions of this Article, the Corporation shall, pursuant to instructions issued for this purpose by the Board and published in the Official Gazette, maintain an</p>		

SUBJECT	JORDANIAN LEGISLATION	RELEVANT RECOMMENDATIONS FROM INTERNATIONAL PRACTICES	RECOMMENDATIONS
	<p>industrial register listing the equipment and machinery for every project.” However, no statement is provided as to disclosure status of the register. It cannot be presumed that all the data contained in such register is capable of being disclosed.</p>		
<p>Provisions mandating cooperation and sharing of data where no legal restrictions apply.</p>	<p>There are no general provisions mandating cooperation and data sharing in cases of information that is subject to no legal restrictions and does not involve violation of privacy. Some laws authorize officials to share data upon discretion. For example, Article 6 of Companies Law provides: C- Any data or information in the possession of the Department could be revealed upon instructions issued by the Minister, provided that the data or information are unrelated to the accounts or financial data of the company.</p>	<p>To enhance and facilitate seem less government, and take advantage of IT developments to increase service efficiency, reduce paper use, some countries –most notably the US- have enacted provisions mandating a certain level of data sharing, provided consistent with applicable legislation.</p> <p>Countries typically provide indication in legislation as to status of data collected with respect to disclosure, use, etc</p> <p><u>US Example:</u> <i>Freedom of Information Act</i></p>	<p>Include legislative provisions that mandate data sharing and cooperation in a manner consistent with legislation. Such a mandate would eliminate unjustified resistance to data sharing that may decelerate SGN pace.</p>

SUBJECT	JORDANIAN LEGISLATION	RELEVANT RECOMMENDATIONS FROM INTERNATIONAL PRACTICES	RECOMMENDATIONS
	<p>However some Jordanian laws specifically mandate data cooperation in limited areas and for specific purposes as for example.</p> <p>Article 22 of the Income Tax law No. (57) for the year 1985 provides: <u>A.</u> The Director or any employee designated by him in writing may require any person or authority to furnish him with the information, which may be necessary for the purposes of effecting this law, provided that Government, Public Institutions and Local Authorities employees do not disclose any particulars or details which, under the provision of this law, they are obliged not to disclose. It is also stipulated that secrecy of banking operations is not to be divulged. Any person refuses to furnish such information is deemed to have</p>	<p>The Freedom of Information Act (FOIA) provides access to all federal agency records, or portions of those records, except for those records that are protected from disclosure by nine exemptions and three exclusions (reasons for which an agency may withhold records from a requestor). For example, records that cannot be disclosed: Classified records, internal personnel rules, confidential by law, trade secrets or confidential financial information, personal information about living people, or records of investigations.</p> <p><u>OECD Guidelines</u> on the Protection of Privacy and Transborder flows of Personal Data represent an international consensus on how best to balance privacy protection and the free flow of information. They provide basic</p>	

SUBJECT	JORDANIAN LEGISLATION	RELEVANT RECOMMENDATIONS FROM INTERNATIONAL PRACTICES	RECOMMENDATIONS
	<p>committed an offence punished in accordance with article 42 lo this law.</p>	<p>principles for a general policy of openness related to policies and practices regarding personal data. This openness principle should provide a transparent setting concerning what information can be collected, how it will be used and to what entities it may disclose.</p> <p>In general, many agree that best practices of openness principle require to namely:</p> <ul style="list-style-type: none"> • Develop privacy protection policies and practices that require personal information to be handled in an open and accountable manner. <p>Accountability shall be ensured complying with stated privacy principle.</p> <ul style="list-style-type: none"> • Be open and informative about policies and practices involving personal information. • Inform individuals of any records maintained that contain their personal information. 	

SUBJECT	JORDANIAN LEGISLATION	RELEVANT RECOMMENDATIONS FROM INTERNATIONAL PRACTICES	RECOMMENDATIONS
		<p>The EU Directive <u>95/46/EC</u> known as the EU Privacy Directive gives the citizens the rights concerning their data: Right to know where the data originated; right to have inaccurate data corrected; right to recourse in the event of unlawful processing; right to withhold permission to use data.</p>	

Matrix (3) Data Sharing and Disclosure: Status in Specific Laws

Specific Provisions pertaining to Data Access and Availability	Implication for Inter-agency Data sharing
<u>MINISTRY OF INDUSTRY AND TRADE</u>	
<p>Article 22.1 of The commercial Law No. (12) for the year 1966 provides:</p> <p>The Trade Register shall enable the public to obtain the sufficient information on each of the traders and Trade establishment in the Kingdom.</p>	Permitted
<p>Article 3 of the Trademarks Law No. (33) for the year 1953 provides:</p> <p>1. A Register known as “The Trademarks Register” shall be established at the Ministry, under the supervision of the Registrar, in which records shall be maintained all information related to trademarks, names of owners thereof, their addresses, and whatever occurred on such trademarks of the following:</p> <p>A- Any assignment, transfer of ownership, or license to use the trademark granted by the trademark owner to others. The provisions of confidentiality in the licensing contract shall be excluded from registration.</p> <p>B- The hypothecation or attachment placed upon a trademark or any restriction on its use.</p> <p>2. The Register shall be made available to the public in accordance with Instructions issued by the Minister for this purpose, which shall be published in the Official Gazette.</p> <p>3. The Ministry may maintain computerized records for the registration of trademarks and related data thereto; such documents and data retrieved there from and certified by the Registrar shall be valid proof against others.</p>	Permitted
<p>Article (18) of the Trade Names Law number (30) of 1953 provides:</p> <p>1- Any person is entitled to view the documents submitted to the Registrar at the payment of the due fees, provided that the fees are not more than 50 Fils for each time. Any person is entitled to request the certificate of the registration of any commercial enterprise or person or</p>	Permitted conditionally.

Specific Provisions pertaining to Data Access and Availability	Implication for Inter-agency Data sharing
<p>copy or summary of any registered statement certified by the Registrar provided that the due fees are charged for this registered certificate or certified copy or summary. The fees should not be more than 100 Fils for the certificate of registration and 25 Fils for each page consisting of 72 words of the registry, copy or summary.</p> <p>Article 6 of Companies Law provides:</p> <p>C- Any data or information in the possession of the Department could be revealed upon instructions issued by the Minister, provided that the data or information are unrelated to the accounts or financial data of the company.</p> <p>Article 12 of Companies Law provides:</p> <p>The Controller shall keep a special register in which all General Partnerships are registered in serial numbers and in chronological order according to their registration dates. The alterations or amendments that may occur to any of the said Partnerships shall be recorded therein. Any individual may, upon payment of the required fees, review the said register after obtaining the prior approval of the Controller if the latter is convinced that such individual has a special interest in the register.</p> <p>Article (9) of the Industry and Trade Law Number (18) of 1998 provides:</p> <p>All the data submitted by the industrial enterprises in accordance with this law and the regulations issued accordingly or at the request of the competent authority at the Ministry shall be treated as confidential. They may not be revealed without an order from the competent court unless the public is allowed to view.</p> <p>Article 34 The Investment Promotion Law No. 16 for the year 1995 provides:</p> <p>It shall be permitted to register mortgages on equipment and machinery that are part of the Fixed Assets of any project; as security for extended credit facilities. For the purposes of implementing the provisions of this Article, the Corporation shall, pursuant to instructions issued for this purpose by the Board and published in the Official Gazette, maintain an industrial register listing the equipment and machinery for every project.</p>	<p>Permitted conditionally.</p> <p>Clearly disallowed.</p> <p>Clearly disallowed.</p> <p>Not clear.</p> <p>Permitted</p>

Specific Provisions pertaining to Data Access and Availability	Implication for Inter-agency Data sharing
<p>Article 3 of the Industrial Designs and Models Law No. (14) For The Year 2000 provides:</p> <p>A-A Register known as “ The Industrial Designs and Models Register” shall be established at the Ministry, under the supervision of the Registrar, in which records shall be maintained of all information related to industrial designs and models, names and addresses of their owners, and any changes thereto resulting from procedures and legal acts thereof, including the following:</p> <p>B- The Register shall be available for the public in accordance with the Instructions issued by the Minister for this purpose, which shall be published in the Official Gazette.</p> <p>C- The Ministry may maintain computerized records for the registration of industrial designs or models and data related thereto. The data and documents retrieved there from and certified by the Registrar shall be valid proof against others.</p>	<p>Permitted.</p>
<p>Article 7.b of the Patent Law No. (32) For The Year 1999 provides:</p> <p>B - The Register shall be available for the public in accordance with Instructions issued by the Minister for this purpose, which shall be published in the Official Gazette.</p>	<p>Permitted</p>
<p>Article 3.b of the Integrated Circuits Law No.10 of 2000 provides:</p> <p>The Register shall be available for the public, in accordance with Instructions issued by the Minister for this purpose, which shall be published in the Official Gazette.</p>	<p>Not clear</p>
<p>Article 4 of the Commercial Agents and Mediators Law No.14 of 2000 provides:</p> <p>A register shall be organized at the Ministry under the supervision of the registrar for recording the names of the commercial agents in the Kingdom, and the main information relating to their agencies, in addition to another register for recording the names of the commercial mediators.</p>	<p>Not clear.</p>

Specific Provisions pertaining to Data Access and Availability	Implication for Inter-agency Data sharing
<p>Article 4 .c & d of the Financial Leasing Law No,16 of 2002 provides:</p> <p>The Public shall be entitled to access the data recorded in the Registry.</p> <p>A- All matters and Provisions pertaining to the Registry shall be organized pursuant to instructions issued by the Minister and published in the Official Gazette, provided that they include the following:</p> <ol style="list-style-type: none"> 1-Procedures for public access to the Registry. 2- Services fee collected by the Ministry in return for recording data in the Registry and for public access thereto. <p>Article 4 of the Protection of New Plants Variety Law No. (22) for the year 2000 provides:</p> <p>The Public may be acquainted with the new plant variety register, the documents relevant to the rights granted to the inventor and the tests that are conducted or growth or any other necessary tests stipulated by this law in accordance with the instructions which the Minister issues for this purpose, provided that the instructions are published in the Official Gazette.</p>	<p>Not clear.</p>
<p style="text-align: center;"><u>MINISTRY OF FINANCE</u></p> <p>Article 68 of Custom Law No. (20) for the year 1998 provides: People other than the declarants or their representatives shall not be allowed to examine the declaration with the exemption of competent judicial and official authorities.</p> <p>Article 47 of the Income Tax law No. (57) for the year 1985 provides:</p> <p><u>A.</u> Every person required to carry out any official duties to implement the provisions of this law shall</p> <ol style="list-style-type: none"> <u>1.</u> Consider all documents, information, statements, assessments, decisions and copies which he has access to and which relate to the income or details relating to the income of any person, as 	<p>Not permitted</p> <p>Not permitted</p>

Specific Provisions pertaining to Data Access and Availability	Implication for Inter-agency Data sharing
<p>strictly private and confidential and deal with them on that basis.</p> <p><u>2.</u> Submit and sign a declaration, the text of which shall be determined by the Minister, to maintain secrecy of official documents.</p> <p><u>B.</u> The person appointed under this law or who is required to enforce its provisions shall not be entitled to produce , in any court other than the Income Tax Court of Appeal, any documents or statements or assessment, decisions or copies thereof nor to divulge to any court or give it any information or any matter or thing which may have come to his knowledge in the course of performing his duties under this law except as may be decided by the Director under this paragraph to be necessary in each case arising from the enforcement of the provisions of this law or for the prosecution of any offence relating to income tax in the course of investigation of such an offence.</p> <p><u>C.</u> Any person having possession of, or control over any documents , information or assessment decisions or copies thereof to any person</p> <p><u>1.</u> Other than the person to whom he is authorised by law to disclose</p> <p><u>2.</u> For any purpose other than those provided for in this law.</p> <p>shall be considered to have committed an offence under this law and shall be liable upon conviction to a fine not exceeding 200 Dinars or to imprisonment for a period not exceeding one- year or to both penalties.</p>	<p>Not permitted</p>
<p>Article 29 of the General Sales Tax Law provides:</p> <p>a. Anyone who formally assumes responsibility to implement the provisions of this Law shall be required to consider the document, information, reports, manufacturing means and techniques and any other data relevant to this Law or to the application of its provisions and the copies he examines as secret and confidential and deals with them accordingly.</p> <p>b. The Department may exchange information with Ministries, governmental departments and public institutions and demand documents for the purposes of enforcing the provisions of this Law.</p> <p>Article 5 of the Public Debt Management Law No. 26 for the year 2001 provides:</p> <p>register called "The Government Securities Register"</p>	<p>Mandates data sharing in specific context.</p> <p>Not clear</p>

Specific Provisions pertaining to Data Access and Availability	Implication for Inter-agency Data sharing
<p>shall be established at the Central Bank and shall in particular contain the following:</p> <ol style="list-style-type: none"> 1-The name of the owner of The Government security. 2-Any change in the ownership, mortgage or attachment of the security. 3- The Register may be maintained electronically and the data issued and signed by the officer in charge of the Register shall be considered equivalent to official securities. <p>Article 22 of the Land Registration Fees Law provides:</p> <p>Information shall be given from the page of the Land register to individuals at the request of regular courts or government department after the payment of the due fees.</p>	<p>Permitted conditionally</p>
<p><u>THE MINISTRY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY</u></p> <p>Article 3 of the Telecommunication Law provides:</p> <p>The Ministry shall undertake the following duties:</p> <ol style="list-style-type: none"> 1. To collect relevant information from the Commission and other government departments or private entities for the purpose of accomplishing the Ministry's duties. m. To work towards the elimination of impediments in the information technology and telecommunications sectors through cooperating with the Commission and other parties, so that the Ministry can discharge its duties. 	<p>May be construed to mandate data cooperation relevant to MoICT's work.</p>

Specific Provisions pertaining to Data Access and Availability	Implication for Inter-agency Data sharing
<u>THE PRIME MINISTRY</u> No specific Provisions on data sharing.	
<u>MINISTRY OF PLANNING</u> No specific provisions identified.	
<u>GREATER AMMAN MUNICIPALITY</u> No specific provisions identified.	

Footnotes

ⁱ) Article 3 of the Telecommunications Law provides: The Ministry shall under take the following duties:

- a. To prepare the general policy of the telecommunications and information technology sectors in the Kingdom, coordinating with stakeholders in these sectors as circumstances require, to submit such policy to the Council of Ministers for approval, and to set a biennial national strategic plan for these sectors in accordance with this policy.
- b. To propose the policy related to the provision of Universal Service and to submit the same to the Council of Ministers for approval; and to follow up the development of this policy for the purpose of expanding the scope of coverage of telecommunications and information technology services, both horizontally and vertically, in such a way as to meet the requirements of economic and social development in the Kingdom.
- c. To draw up plans that encourage investment, on a competitive basis, in the telecommunications and information technology sectors in the Kingdom, creating an atmosphere for the provision of services to users at just, reasonable and affordable prices, in accordance with the latest technological developments in these sectors.
- d. To strengthen the competitive position of the Kingdom internationally in the areas of information and communications technology.
- e. To follow up the implementation of the Kingdom's commitments in international treaties in the telecommunications and information technology sectors.
- f. To safeguard the Kingdom's interests with states, regional and international organizations, unions, and commissions concerned with telecommunications and information technology; and, in cooperation with the Commission, the ministries, and concerned parties, to oversee the representation of the Kingdom before those official bodies.
- g. To promote the advancement of research and development in the areas of telecommunications and information technology.
- h. To encourage the setting of advanced education and training programs in telecommunications and information technology, including the use of the Internet, electronic commerce, and electronic transactions.
- i. To spread public awareness of the importance of the role of telecommunications and information technology to the overall economic and social development and advancement of the Kingdom.
- j. To provide the necessary facilities to allow the Commission and designated members of the armed forces and security services to prepare the National Plan for Frequency Assignment and the National Register of Frequencies; to maintain these in the Ministry and prepare procedures for the coordination among these parties so as to ensure the optimal use of the radio frequencies and to prevent harmful interference between frequencies assigned for civilian and military uses.
- k. In consultation with the Commission, to prepare draft laws in the areas of telecommunications and information technology, and to present them to the Council of Ministers.
- l. To collect relevant information from the Commission and other government departments or private entities for the purpose of accomplishing The Ministry's duties.
- m. To work towards the elimination of impediments in the information technology and telecommunications sectors through cooperating with the Commission and other parties, so that the Ministry can discharge its duties.

ⁱⁱ Article (6) of the Telecommunications Law states: The Commission shall undertake the following duties and responsibilities:

a) To regulate telecommunications and information technology services in the Kingdom in accordance with the established general policy so as to ensure the provision of high quality telecommunications and information technology services to users at just, reasonable and affordable prices; and, by so doing, to make possible the optimal performance of the telecommunications and information technology sectors.

b) To establish the basis for regulation of the telecommunications and information technology sectors, in accordance with the approved general policy, in such a way that services meet the comprehensive developmental needs of the Kingdom; in accordance with rules and instructions issued by the Board for this purpose. [most pertinent provision]

c) To specify the minimum level of service quality which must be offered by licensees to meet the needs of Users; this shall be done in consultation with Licensees and shall be without the imposition of any specific technology.

d) To protect the interests of users and oversee the actions of persons and Licensees to ensure that the conditions of Licenses are observed, including specified service standards, service quality, and prices; and to take the necessary steps in this regard to provide for the punishment of those who violate these conditions.

e)...

f)

ⁱⁱⁱ Some legislation provides a high level of protection whereby the information shall not be disclosed at all. (e.g.: Article 22 of the Income Tax Law). Other legislation provides a lower level of protection whereby the information could be disclosed to the court. (Article 9 of the Industry and Trade law) and there is still a lower level of protection whereby the public can have access to this information in accordance with specific conditions (Article 3/b of Industrial Designs and Models law). However, in many cases information is not classified. Furthermore, information is usually classified with respect to disclosure only which is only one of many criteria relevant to assessment of sensitivity and importance.

^{iv} Not addressed by ISP but standard issue in international practice

^v A - Article 142 of the Civil Service Regulations provides: "If the employee commits a violation of the laws, regulations, instructions and decisions in force at the Civil Service Commission or in the application thereof, or carries out any action or activity that is in violation of the responsibilities and powers vested therein or in obstruction thereof, or violates the ethics of the job and the duties and proper attitude of the employee, he shall be subject to one of the following disciplinary penalties:

1- Reprimand.

2- Deduction of no more than half of the monthly salary.

3- Delay of the annual increment for a period of no more than three years.

4- Full or partial reduction of the allowances for a period of no more than one year. Personal or family allowances shall be excluded from this penalty.

5- Lowering the salary.

6- Lowering the grade.

7- Termination of service.

8- Dismissal.

B - An employee may not be subject to more than one penalty of those stipulated in Paragraph (A) of this article for each attitudinal violation he commits."

^{vi} A- Article 150 of the Civil Service Regulations states : "If an authority empowered with disciplinary action against the employees in accordance with the provisions of these regulations, including the Disciplinary Council, comes to the knowledge that the violation justifying the referral of the employee thereto implies criminal action, it should stop the disciplinary procedures and refer the employees and the minutes of the investigation that has been conducted along with the other documents and papers relevant to the violation to the competent public prosecutor or to the competent court to proceed with the case in accordance with the provisions of the law. In this case, no disciplinary action shall be taken against the

employee and no other action taken against him may be continued until a final court ruling is issued on the complaint or the criminal lawsuit filed against him. The employee shall be referred in this case to the public prosecutor or the competent court by the decision of the Minister or the Disciplinary Council if the employee was referred thereto, to start with.”

^{vii} Requirements in the law that pose a legal obstacle to electronic data sharing, because they are formally met only in a paper based exchange.

^{viii} However we have not been able to identify any court decision on this matter.