

# Strategy for Strengthening the MIS and Database Management in the Social Protection System

Valery Dmitrushchenkov

Armenia Social Protection Systems Strengthening Project

USAID SO 3.4

USAID Armenia 111-C-00-06-00067-00

AECOM International Development  
November 21, 2007



**USAID**  
FROM THE AMERICAN PEOPLE



USAID ARMENIA, SOCIAL PROTECTION SYSTEMS  
STRENGTHENING PROJECT

ԱՄՆ ՄՁԳ ՀԱՅԱՍՏԱՆ, ՍՈՑԻԱԼԱԿԱՆ ՊԱՇՏՊԱՆՈՒԹՅԱՆ  
ՀԱՄԱԿԱՐԳԵՐԻ ՀՁՈՐԱՑՄԱՆ ԾՐԱԳԻՐ

---

# Strategy for Strengthening the MIS and Database Management in the Social Protection System

---

**21 November 2007**

**Submitted to: USAID/Armenia**

**Submitted by: Valery Dmitrushchenkov,  
IT Expert  
SPSS/ The Services Group, Inc. (TSG)**

This report was made possible with the support of the American People through the U.S. Agency for International Development. The contents of this report are the sole responsibility of TSG and do not necessarily reflect the views of USAID or the US Government

USAID Armenia-The Social Protection Systems Strengthening Project

Implemented by TSG ■ Իրականացվում է TSG-ի կողմից

18 Bagramyan, Zarubyan Street Entrance ■ Yerevan 0009 Armenia ■ T (374 10) 542 608/9/10 ■ F 588 204 ■ [www.tsginc.com](http://www.tsginc.com)

Զառուբյան փողոց ■ Երևան 0009 Հայաստան ■ Հ (374 10) 542 608/9/10 ■ Ֆ 588 204 ■ [www.tsginc.com](http://www.tsginc.com)

## TABLE OF CONTENTS

Abbreviations .....	5
Executive Summary.....	6
Introduction .....	11
Part 1 Current situation .....	15
Analysis of the current situation .....	16
Strengths .....	16
Weaknesses.....	16
Opportunities .....	17
Threats.....	17
Part 2 Information Strategy: goals, challenges and opportunities .....	19
Vision, Principles and Objectives.....	20
Supporting infrastructure.....	26
Information Infrastructure .....	33
Business Solutions .....	34
Implementation and Monitoring.....	35
Part 3 Action Plan.....	41
Goal 1: Well-Coordinated ICT Policies in Social Protection sphere.....	41
Strategic Activities.....	42
Goal 2: Creation of ICT-Supportive Legislative Environment .....	43
Strategic Activities.....	44
Goal 3: Implementing citizen-centered, transparent, efficient services.....	44
Strategic Activities.....	45
Goal 4: ICT solutions for Social Services .....	46

Strategic Activities.....	47
Goal 5: Development of inexpensive, fast and secure ICT infrastructure.....	49
Strategic Activities.....	50
Goal 6: Monitoring of ICT Developments in Regional and European Context.....	51
Strategic Activities.....	51
Financing Options.....	52
References.....	54
Appendix A. LIST OF LEGAL ACTS IN the SOCIAL SPHERE.....	56
A.1 Laws.....	56
A.2 Government Decrees.....	57
A.3. Other legal acts.....	61
Appendix B. Best practices of e-Government.....	63
USA.....	63
Denmark.....	65
United Kingdom.....	66
Norway.....	67
Netherlands.....	67
Belgium.....	67
Estonia.....	68
Malta.....	69
Spain.....	69
France.....	69
Italy.....	69
Appendix C. What is else beyond strategy?.....	71
Maturing IT Infrastructure Management.....	71

Maturing IT Development Management.....	72
Maturing IT Security Management.....	73

## Abbreviations

CIO	Chief Information Officer
SESA	State Employment Services Agency
EU	European Union
GOAM	Government of Armenia
IT	Information Technology
ICT	Information and Communication Technology
IPU	Information Policy Unit
LAN	Local Area Network
WAN	Wide Area Network
LI	Labor Inspectorate
MLSI	Ministry of Labor and Social Issues
MOF	Ministry of Finance
NLSRI	National Labor and Social Research Institute
SSIF	State Social Insurance Fund
CNIF	Corporate Network for Information Flows for Social Protection sector organizations
UN	United Nations
WEF	World Economic Forum
WSIS	World Summit on Information Society

## Executive Summary

The primary aim of the document is to recommend necessary actions to rectify present deficiencies in Management Information Systems and Databases management in The Social Protection System of Armenia and to outline essential frameworks for ensuring the optimal development and utilization of information.

The document is describes the vision, principles and objectives of the Strategy.

## Information in Context

The vision is to introduce of Citizen-friendly e-services in all state agencies of The Social Protection System and to promote the use of self-services by citizens and enterprises.

The principles of the Strategy are to:

- **Safeguard the privacy and confidentiality** of personal information
- **Ensure** that Management Information Systems are **efficient and effective**
- **Promote the optimal use** of information
- **Ensure the high quality** of information.

The objectives of the Strategy are to:

- **Establish a legislative and information governance framework** for safeguarding the confidentiality and privacy of information while optimizing its use
- **Adopt an integrated, national approach** to the development and expansion of information sources and systems to best meet the strategic information needs as well as for operational activities and for monitoring and evaluation tasks
- **Establish processes and structures** that ensure the broader use of information in policy making, service planning and implementation processes, service provision and to inform quality assurance and accountability in the system
- **Improve access** to information for all stakeholder groups
- **Establish information standards** that ensure the quality and comparability of information and enable appropriate sharing of information within the sector
- **Exploit enabling technologies** in the collection, processing, analysis and dissemination of information and its application in the delivery of services.

## Improving Social Protection Information

While overall responsibility for information policy and related legislation rests with the

MLSI, the Information Policy Unit (IPU) will be given a central role in the implementation of the Information Strategy. To promote the quality of information and ensure its relevance to strategic priorities of The Social Protection System, the Information Policy Unit will set standards by which it will assess and advise on the suitability of major developments in the area of Social Protection information and the supporting Information and Communications Technology. The main responsibilities of IPU include the following:

- Review and update the Information Strategy every year and submit it to the MLSI Minister for approval
- Establish monitoring and evaluation system for the Information Strategy implementation
- Human resource development program supporting the delivery of the Information Strategy
- Provide relevant training programs
- Assess and advise on major developments in information and information technology
- Draw up a multi-annual information and ICT action plan.
- Develop and maintain a Social Protection information database inventory
- Develop and maintain a Social Protection services data model
- Assess information databases of all agencies which provide key Social Protection service information on an ongoing basis and enter into service agreements as appropriate for the supply of information
- Publish an annual report

### **Access to Information – the Portal solution**

The Social Protection Information Portal will constitute a single internet-based access point to a range of Social Protection related information sources and online services for all stakeholders. Building upon existing and future Social Protection MIS and databases the Social Protection WEB Portal, which will include provision of Social Protection services information, documents library and data access facilities as well as provision of rapid notification of urgent information to specified stakeholders.

### **Unique Identification**

A system of unique identification will promote the quality and safety of Social Protection data.

The Information Policy Unit in cooperation with MLSI, SIF, and other State agencies, will develop a plan for the implementation of a unique identification system, based upon the SSC Number and its supportive infrastructure, which meets the functional requirements of the Social Protection System. It is recognized that unique identification within the sector must be supported by a robust information governance framework and be provided for in legislation.

### **Supporting Social Protection Information**

## **Information Governance and Legislation**

A legislative framework to authorize the Strategy has to be introduced, together with a framework for information governance. These frameworks will support quality assurance of service delivery processes and comprise 3 levels:

- Laws – created by state lawmakers, affecting how business and government act and usually enforced by civil courts.
- Regulations – issued by state agencies at all levels and usually enforced by the same agencies.
- Policies – created by an organization as internal procedures to enforce accountability in processes not directly covered by laws and regulations.

Existing legislation (Appendix A. LIST OF LEGAL ACTS IN the SOCIAL SPHERE) is not sufficiently supportive of some aspects of information governance.

For example, in 2002 the National Assembly of the Republic of Armenia adopted the Law of the Republic of Armenia “On Personal Data”. In general the law complies with the principles outlined in the Council of Europe Convention No 108.

However, there are some gaps in the Armenian legislation related to specific provisions of the Convention that do not provide adequate guidance on personal data stored in public and private databases. One of these gaps is the absence of “appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection” as required under the Article 10 of the Convention. While the Law of the Republic of Armenia “On Personal Data” formally declares that persons violating the law shall be liable for violating the law, there are no administrative or criminal sanctions for the violation of data protection law.

It is essential to analyze existing legislation (Appendix A. LIST OF LEGAL ACTS IN the SOCIAL SPHERE) and prepare recommendations for necessary amendments or new legal acts. Regulations, Policies and Codes of practice also have to clarify issues of data sharing, and there will be a comprehensive framework enabling information flows, so that information can be used more fully and properly and for promoting demonstrably first class and accountable services.

## **Information Standards and Quality**

The adoption of information standards is necessary for improving the quality, comparability and usefulness of information for all stakeholder groups. The Information Policy Unit will introduce a national information standards framework, develop common sets of indicators and establish a system of quality assurance of information services provided to the public.

## **Information and Communications Technology**

The outcome of under-investment in information and communications technology (ICT) in the past is an inadequate infrastructure to meet the complex information needs of a modern service, including performance management.

To reap the full benefits of investment in ICT, a shared infrastructure and a common approach will be adopted. The introduction of national ICT systems will build upon the infrastructure and wealth of knowledge and experience already in the field and include effective change management and training processes. ICT actions will be developed and included as part of a multi-year information and ICT action plan in order to achieve a consistent, coordinated and common approach across the Social Protection service for all mainstream ICT developments.

## **Implementation**

The implementation of the Strategy requires cooperation and partnership between the key stakeholders. To support this process of cooperation and partnership, ongoing consultation on initiatives and participation in local, regional and national structures are required.

To implement the Strategy, a number of essential requirements must be met, including:

- The development of infrastructures, and especially the empowerment of Information
- The Information Policy Unit, as the central driving force behind the implementation of the Strategy
- The availability of skilled and trained staff, within MLSI, SSIF and Social Protection agencies, with the expertise to exploit available information and to support the roll-out and use of new information systems.
- A clear and supportive legislative and information governance framework that permits appropriate sharing of Social Protection information while protecting privacy and confidentiality
- Major investment in information systems to enable appraisal of effectiveness, efficiency and economy. A range of options including third party provision of ICT services will be considered.

The current low level of investment in Social Protection information in general and ICT in particular is central to the difficulties currently experienced in meeting the complex information requirements of modern Social Protection services. Future investment needs will be determined as part of the process of estimating needs.

## **Implementation Phases**

The Strategy will be implemented on a phased basis and advantage will be taken of the developing information infrastructure. The process is divided into phase 1 (year 2007), phase 2 (year 2008) and phase 3 (years 2009-2011).

Improved access to existing information for planners, Social Protection professionals and the public will be an early objective of the IPU.

During phase 1 emphasis will be placed upon establishing essential infrastructures and processes, with priority given to establishing the IPU.

Actions and processes to attain short term goals:

- Recommendations for **IT Infrastructure improvement** (LAN, WAN), pilot implementation
- **Assessment** of current Information Infrastructure and **recommendations for improvement**
- Recommendations for **data exchange mechanisms**
- Recommendations and action plan for IT systems improvement or development
- The ICT Plan will be completed as part of the information and ICT action plan.
- The service planning process at national and regional level will be strengthened.

In phase 2, emphasis will be placed on the ongoing development of the necessary ICT infrastructure, including a secure communications system and the deployment of the infrastructure and procedures for unique identification. New and enhanced sources of information will be commissioned. In addition it is planned that the ongoing roll-out of key functional systems will be completed during this phase.

Actions and processes to attain short term goals:

- Development and Implementation of automated and flexible data exchange mechanisms
- Development of Social Protection Information Portal
- Implementation of improved IT systems

The ongoing deployment of the electronic Social Protection records will be the dominant undertaking of phase 3. This will build on the primary service ICT developments from phase 1 and the overall electronic Social Protection model addressed in the ICT action plan.

Actions and processes to attain long term goals:

- Implementation of **Nationwide information systems** architecture in compliance with the requirements of data protection and information security.

## Introduction

High-quality information lies at the heart of all good decisions concerning Social Protection. Social Protection information must be relevant and accessible to all those who require it, must be presented in the most useful formats and must utilize the power of Information and Communications Technology (ICT) to the full in its collection and dissemination. Good information empowers us all. This applies equally to consumers, Social Protection professionals, managers and policy makers.

Widespread availability and use of Social Protection information will mean better informed public and citizens, improved service delivery, enhanced quality and efficiency and well-targeted planning.

The purpose of this Strategy is to recommend the framework and actions required to make sure that all those who need Social Protection information get the information they need and are in the position to use it competently, confidently and effectively.

Access to information technologies is one of the targets listed in the Millennium Development Goals (MDGs) and is also considered important by itself for the attainment of all other goals. To promote access to ICTs and bridge the digital divide, the United Nations agencies have set up several initiatives seeking to exploit the potential of new technologies. The WSIS conference held in Geneva in 2003 set global targets for improving connectivity and access and measuring progress towards an information society, which were endorsed by 175 Member States.

The **UN Global E-Government Readiness Report 2005** [1] presents an assessment of the countries according to their state of e-government readiness and the extent of e-participation worldwide. The **UN Global E-government Survey 2005** ranks the 191 Member States of the UN according to a quantitative composite index of e-readiness based on website assessment, telecommunication infrastructure and human resource endowment. The basic message in this Report is that there are huge disparities in the access and use of information technologies, and that these disparities are not likely to be removed in the near future unless concerted action is taken at the national, regional and the international levels.

Another valuable and unique benchmarking tool for determining national ICT strengths and weaknesses is the WEF **Global Information Technology Report** [2]. It also highlights the continuing importance of ICT application and development, regulatory environment, government leadership and vision in leveraging ICT for growth and promoting ICT penetration and usage. This report has become also a valuable tool for country progress evaluation. The Report uses the **Networked Readiness Index (NRI)** [3] to measure the degree of preparation of a nation or community to participate in and benefit from ICT developments.

According to the E-government Readiness rankings in 2005, the United States (0.9062) is the world leader, followed by Denmark (0.9058), Sweden (0.8983) and the United Kingdom (0.8777). As of 2004, the Republic of Korea, Singapore, Estonia, Malta and Chile are also among the top 25 e-ready countries. Armenia with rank 0.3625 was ranked 106, moving down 23 places compared to the previous year.

In May of 2001 the GOAM approved Program for Information and Telecommunication Industry development in Armenia. This program was prepared by the Ministry of Industry and Trade. It is based on the **ICT Master Strategy** [4], which was developed with substantial technical assistance from the World Bank and USAID experts.

The Program and the ICT Master Strategy are the basic guidance documents for both government and donor organizations supporting the ICT development in Armenia. The Program specified priorities of the government and indicates the main directions for the activities of governmental organizations in this field. According to the ICT Master Strategy implementation of targeted e-government initiatives was one of Strategic Direction. It was planned, that ‘The Government of Armenia will establish a comprehensive approach for leveraging ICTs to improve the internal operations of key processes within the Ministries as well as improve the delivery of services to the businesses and citizens of Armenia’.

Current document continues elaboration of this initiative for Social Protection sector, aiming strengthening MIS and Database management, reinforce the centralized coordination of IT and improve collaboration and consistency in the development of an information society.

The term "e-Government" focuses on the use of information and communications technologies by governments as applied to the full range of government functions.

E-Government reorganizes the way governments work, share information, and deliver services to external and internal clients for the benefit of both government and the citizens, and the businesses that they serve. Specifically, e-government harnesses technologies (such as Wide Area Networks, the Internet, and mobile computing) to transform relations with citizens, businesses, and other arms of the government.

These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with businesses and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, and/or cost reductions.

These are main benefits for external and internal users of e-Government applications:

- *Delivering services to citizens.* E-Government can benefit citizens by reducing delays, consolidating multiple services under one roof, eliminating the need for frequent visits to government offices, and containing corruption. In addition, publishing rules and procedures online can increase transparency. Moreover, because poor people bear the largest costs of administrative inefficiency and corruption, delivering services through rural kiosks leads to their economic and social empowerment.
- *Delivering services to businesses.* Businesses often face significant administrative roadblocks when interacting with government. Electronic delivery can shorten the turnaround on license applications from several weeks to a few days. Rules can be made transparent and consistent across departments. Transaction costs for business and government can be reduced. Government can benefit from more efficient revenue collection.

- *Increasing efficiency.* E-Government can lead to higher productivity. Governments can cut staff or redeploy workers in more productive tasks. Data captured by an electronic system often enables more frequent and accurate data sharing across departments, closer monitoring of employee productivity, easier identification of pressure points for delay and corruption, and improved compilation of historical data that can be mined for policy analysis.

The UN Surveys mentioned above include a large amount of useful information for policy makers on choices in their e-government program undertakings. Each Survey offers insights into the different strategies and common themes in e-government development among regions and across them. By studying broad patterns of e-government use, it identifies countries, which have taken a leadership role in promoting e-government readiness and those where the potential of ICT for development has not yet been exploited.

The United States was at leading position and 5 EU countries are in top 10 of UN E-government Readiness Index. Thus, these country information society strategies are a resource of good practices.

US law ‘**E-Government Act of 2002**’ [5] outlined reform ensuring strong leadership of the information technology activities of Federal agencies, a comprehensive framework for information security standards and programs, and uniform safeguards to protect the confidentiality of information provided by the public for statistical purposes. The Act will also assist in expanding the use of the Internet and computer resources in order to deliver Government services for a citizen-centered, results-oriented, and market-based Government.

**eEurope 2005 action plan** [6] followed by the EU **information society initiative strategy i2010** [7] emphasized the EU priority fields in eGovernment: e-services as well as their secure underlying infrastructure. Member States have agreed to a common list of basic public services, 12 for citizens and 8 for businesses, indicating eGovernment developments.

Some of best practices are presented in Appendix B. The Strategy document reflected these best practices and adapted them to the current state of the Social Protection System of Armenia and to existing political and economic realities.

The Strategy implementation requires strong leadership and vision. The key vehicle for achieving the necessary improvements in Social Protection information is establishment of an Information Policy Unit (IPU) at MLSI. The IPU will be given a central role in the development and implementation of the Information Strategy. To promote the quality of information and ensure its relevance to strategic priorities, the Information Policy Unit will set standards by which it will assess and advise on the suitability of major developments in the area of Social Protection information and the supporting Information and Communications Technology.

This document consists of three parts. The first part is assessing current situation with Management Information Systems and Databases management in the Social Protection System.

In the second the high-level vision of an optimal ICT for The Social Protection System is described:

- Where we need to be in 2011, looking at requirements from a user's perspective while considering the vision in the context of current realities and developments, both at national and international level?
- What are goals to achieve and challenges to be addressed?

A last part of the Strategy outlines the roadmap of implementation of the strategic vision:

- How we are going to get there?

## Part 1 Current situation

This part of the Strategy document has to answer at following questions:

- What are the organization and its customers today?
- Have the current situation, processes, functioning, capacity of change, etc been identified and analyzed?

In the 1980s and yearly 1990s, information technology departments mainly designed and developed back-office systems. Accordingly, the number of users/stakeholders involved was relatively small, or at least the variety of users and user needs was relatively contained and somewhat easier to predict. This situation changed in the late 1990s, and more recently the introduction of Internet technology created a new (and far larger) group of stakeholders – the clients of the organization. They are the ones who primarily use the new system(s), and they are not only a much larger body than the traditional concept of users – they also have a much wider range of needs and abilities when it comes to interacting with many modern systems.

Today it is normally necessary to involve all types of stakeholders in more meaningful ways.

Stakeholders can be defined as follows:

- External stakeholders: final users or customers (potentially all citizens, or perhaps limited to insured persons and employers, in the case of social insurance and claimants and other beneficiaries), banks, suppliers (including outsourcers) and partners
- Internal stakeholders: managers, employees and users in general
- Other stakeholders: legislators, journalists and other media contacts, pressure groups, etc.

Internal stakeholders can be identified at the following organizations:

- Ministry of Labor and Social Issues
- State Social Insurance Fund
- National Institute for Labor and Social Research
- State Employment Services Agency
- Labor Inspectorate
- Information Analytical Centre NORK
- State Register of Enterprises
- Police (Passport database)
- State Tax Service (taxpayers DB)
- Property Cadastre
- The National Statistical Services

## ***Analysis of the current situation***

SWOT Analysis is a strategic planning tool used to evaluate:

- **Strengths:** attributes of the organization that is helpful to achieving the objective.
- **Weaknesses:** attributes of the organization that is harmful to achieving the objective.
- **Opportunities:** external conditions that is helpful to achieving the objective.
- **Threats:** external conditions that is harmful to achieving the objective.

### **Strengths**

- During last decade several Information Systems and database were developed and implemented in The Social Protection System of Armenia. Currently the following Information Systems with basic functionality are up and operational:
  - ✓ Social Security Cards
  - ✓ GORTS - Employment Services
  - ✓ PAROS - Poverty family allowance
  - ✓ PYUNIK - Disabled persons
  - ✓ MANOUK - Orphan children
  - ✓ PARNAS - Personal Account Registration, Numbering and Analysis System
  - ✓ PARNAS-E - Employer version of PARNAS
  - ✓ ARAKS - Database of pensioners
- Systems designs have been based on existing Government regulations (see Appendix A)
- Users are trained and familiar with operating of these systems
- ICT expertise in subject area automation is concentrated in 2 local IT organizations: "Mergelyan Institute" (Yerevan Automated Control Systems Scientific Research Institute) and NORK IAC.

### **Weaknesses**

- Lack of top management commitment and awareness of the ICT benefits
- Low service standards
- Lack of systems integration:
  - Lack of customer focus in systems design
  - Isolated subsystems and databases
  - Different versions for central and territorial offices
  - Heterogeneous databases and programming languages,
- Outdated technologies: databases and development tools
- Data quality problems

## **Opportunities**

- There are several donor projects to assist improvements in social area
- New Information Technologies allow improvement of management and quality of services
- Existing and applicable international experience, best models for solutions
- About 2.5 million of citizens have Social Security Cards and SS number exists in all systems and can serve information integration purposes
- Implemented new WEB based Employment Services system GORTS can serve as best practices example

## **Threats**

- Lack of LAN and WAN infrastructure (territorial and central offices connections)
- Multiple entry of the same information
- Business processes are not coordinated
- Security problems of data exchanges
- Lack of standard project life cycle for IT systems development and quality assurance
- Legislation changes
- Lack of financial other resources for new developments

This is just a bird's eye view of the current situation. The Information Policy Unit of MLSI has to take inventory of Social Protection information assets. After determining what it has, IPU must determine the quality of what it has, as well as what it does not have. Then it must write out an Action list of what it needs to make the Strategy happen.

It is important to ask the following questions when taking an inventory.

People and skills:

1. What type of ICT skills do they possess?
2. What is their level of competency?
3. Are there enough of them with the skills necessary to implement the Strategy?

Hardware, software and equipment:

1. What types of ICT hardware/software does each Agency have?
2. How old or how new are the equipment?
3. What does the existing physical infrastructure of government telecommunications look like?
4. How existing MIS and databases satisfy business needs?

Laws and regulations:

1. Are the appropriate policies and regulations in place for the development and implementation of the Strategy?

2. What policies and regulations need to be amended or changed in order to implement the Strategy and facilitate e-government?

## **Part 2 Information Strategy: goals, challenges and opportunities**

### **What is an information strategy?**

An Information strategy is a coherent approach to change. It is focused on the organization's goals and the role information will play in supporting them.

It needs to assess the value of its existing repositories and sources of information, and consider how those sources might change and grow over time. Furthermore, the strategy is not complete unless it is based on the organization's governance policies and frameworks.

Information strategy focuses on the business problem that the organization is trying to solve.

It is necessary to ask questions about its information issues and assess needs:

- Integrate roles and responsibilities for the generation and use of management information with the structure of the Organization and the pattern of its work processes.
- Link management information to business planning.
- Are the supporting platforms capable of providing the required service levels at a reasonable cost as the organization's needs expand?
- Is information stored in a way that enables management to quickly and efficiently retrieve key details? Are there business issues related to the capture and creation of information?
- Are there isolated silos of information?
- Are there conflicts between those data silos?
- Provide a scenario for immediate implementation as well as a medium and long-term strategy for information system consolidation and development.

A key to the success of such a strategy is to ensure that the Organization:

- Accepts and embraces a need for significant change of organization and management culture.
- Makes an overall commitment to the use of management information for strategic and tactical planning as characterizing such a change.
- Integrates the interests of all of those who have (or should have) a role and responsibility for the generation and use of information.
- Identifies a timetable whereby core information will be developed and used within the strategy.

Information Strategy addresses the major information needs and broad interest groups within society. The use of information to support high-quality services and in planning, developing, evaluating and accrediting the quality of the services is a central theme. Special attention is given to establishing processes and infrastructures to underpin future information developments. Furthermore, it is recognized that effective use of information is largely dependent on the skills and knowledge of service staff and the culture of the environment in which they operate.

## ***Vision, Principles and Objectives***

- Main objective - Introduce Citizen-friendly e-services in all state agencies pertaining to the social sphere and promote use of self-services by citizens and enterprises.

The key principles comprising this vision are:

- **Safeguarding privacy and confidentiality.** In providing access, processing and use of personal information, the Social Protection System should comply with legislative and information governance requirements. Special attention should be taken to protect personal and sensitive information.
- **Efficient and effective Social Protection Information Systems.** The development and continuation of Information Systems should be driven by their usefulness to stakeholders. Data that are routinely collected as an intrinsic part of service delivery (i.e. from operational sources) should be the primary source of information and be complemented by other sources as and when required. Data should be gathered once and once only; if data are not going to be transformed into useful information, they should not be collected.
- **Optimal Social Protection information access and use.** Stakeholders need ready access to available Social Protection information that is appropriate to their needs. Available information should be fully exploited and shared in the support of safe and high-quality services, the development and evaluation of Social Protection services and policies and for legitimate research purposes.
- **Quality assurance of Social Protection information.** Social Protection information should be of the highest quality and be demonstrably compliant with information standards.

## **The objectives of the Information Strategy**

Using IT is not an objective itself, but adding value to the main activities as a key driver of productivity and effectiveness. Thus IT objectives have to be in line with main business objectives.

### **Business objectives**

- Accurate and timely pensions and social assistance payments delivery to eligible beneficiaries
- Improved job placement, especially among the disabled and young workers
- Improved citizens' satisfaction regarding service delivery related to pensions, employment services and social assistance

### **ICT objectives**

For achieving its vision and business objectives, the Strategy is centered upon a number of fundamental ICT objectives:

- Establish a legislative and information governance framework for safeguarding the confidentiality and privacy of Social Protection information while optimizing its use
- Adopt an integrated, national approach to the development and expansion of information sources and systems to best meet the strategic Social Protection information needs
- **Establish processes and structures that ensure the fuller use of Social Protection information** in policy making, service planning and implementation processes, service provision and for underpinning quality assurance and accountability arrangements in the Social Protection system
- **Improve access to Social Protection information** for all stakeholder groups
- **Establish Social Protection information standards** that ensure the quality and comparability of Social Protection information and enable appropriate sharing of Social Protection information within the Social Protection system
- **Exploit enabling technologies** in the collection, processing, analysis and dissemination of Social Protection information and its application in the delivery of Social Protection services.  
In particular:
  - Automate major business processes and data exchange procedures
  - Establish efficient communication between agencies headquarters and local offices
  - Implement interagency communications and data exchange

**Principal goal of IT systems and services** is to promote the widest possible use of data, delivering them timely, in proper context and required quality, leveraging information to meet needs of social service professionals and citizens, and appropriately protecting data confidentiality.

To achieve the goal of leveraging corporate information it essential to keep focus on all 4 key components of complete solution:

- Information Strategy
- System Platform
- Information Infrastructure
- Industry Solutions

A central theme throughout this Strategy is the importance of transforming raw data into useful information that can then be applied as knowledge in guiding decisions about the provision of services, the planning and evaluation of services and the formulation of Social Protection policies. In the past resources have tended to focus on the collection of data that sometimes flow into ‘islands of information’ that are not properly exploited on an everyday basis. This Strategy

places greater emphasis on the importance of transforming data into different types of information that is readily available to meet the needs of different stakeholder groups.

While data that are routinely collected as an intrinsic part of service delivery are a primary source of Social Protection information, such ‘activity’ data must be complemented by other types of information (such as surveys) to provide a comprehensive basis for the planning, monitoring and evaluation of services.

The scope of the information required to encompass the needs of the stakeholders is broad and includes:

- Information for the public, beneficiaries and professionals about Social Protection services to empower them to make services-related decisions
- Information to assist Social Protection professionals in decision making and to provide quality services, including access to best practice guidelines, knowledge databases and library services
- Information to support the planning, monitoring and evaluation of Social Protection services, including human resource management and planning, resource allocation and information that demonstrates service quality
- Information to support the development and implementation of policies and the allocation and utilization of resources to promote, guaranty and delivery of the Social Protection services
- Information to support Social Protection research
- Information on Social Protection status and Social Protection determinants.

## **Social Protection information in Context**

Information strategy has to be in line with Enterprise architecture and plans for IT and data governance in dynamic information environments.

Key for the successful implementation of Information strategy is that an organization accepts and embraces the need for significant change of organization management culture.

Modern and effective Social Protection Information Systems have to be based on the best practices and the experiences of other countries. As evidenced elsewhere, the most important high-level requirements are the commitment of politicians and senior managers, adequate resourcing of systems and training, and explicit policies and responsibilities for data standards and data use.

A number of key themes can be identified in modern and effective Social Protection Information Systems:

- **Data usage:** sharing of data, training in its use and effective information governance are essential.

- **Data collection:** data should be entered only once and as close to the point of client contact as possible.
- **Data content:** the most advanced and effective systems utilize a unique identifier throughout the system. Finland provides a good model where linkage between a population register and address registers simplifies geo-coding, shared information arrangements and research applications for Social Protection data.
- **Data collection systems:** systems must meet the purposes for which they were designed, and a single agency/body should have overall responsibility for ensuring data quality, access and reporting.
- **Legal issues:** all countries with effective Social Protection Information Systems have paid full attention to the legislation required to protect confidentiality and facilitate appropriate access and use.
- **Technical issues:** optimization of ICT and application of advances in secure data transmission are features of high-quality Social Protection Information Systems.

## **Improving Social Protection information**

### **Role of the Information Policy Unit**

Significant progress has been made in improving and expanding information systems and functions across the Social Protection System. However, attention here has been drawn to persistent deficiencies and omissions in existing systems, to continuing difficulties in accessing and utilizing information and to the requirement for an integrated, strategic approach to addressing current and future Social Protection information needs.

Many significant Social Protection information deficiencies exist. In some instances, this may be due to the information being relatively inaccessible or not being in a format relevant to the stakeholder groups. In others, it is due to information ‘black-spots’ where the information is limited or very fragmented.

In the process of developing this Strategy a number of key areas requiring development were identified. These include:

### **The information role of the Information Policy Unit**

- A Social Protection services data model
- A national Social Protection services database inventory.

### **Information and the service planning process**

- Value for money and service performance information
- Human resources information
- Client satisfaction.

### **Access to Social Protection information**

- Social Protection information and eServices for the citizens and employers.

### **Electronic Social Protection data records**

- Social Protection information and support systems
- Risk management information to support robust safe-system processes.

While overall responsibility for Social Protection information policy and related legislation rests with the MLSI it will be the job of the IPU, working with the MLSI Departments Executives and other MLSI agencies, to address information deficits. As a matter of priority, the Information Policy Unit will, in partnership with MLSI agencies, identify and specify in detail the deficiencies which must be addressed. This will be done in the light of strategic priorities within the Social Protection System. A broad range of Social Protection information functions to be undertaken by the Information Policy Unit as follows:

- Providing leadership and guidance in the implementation, monitoring and evaluation of the Strategy at the national and regional level
- Supporting and enabling the implementation of the information governance framework
- Undertaking and providing for the analysis of data for policy and planning requirements
- Developing a national Social Protection information database inventory
- Develop and maintain the overall Social Protection Service Data Model and minimum datasets
- Specify information standards, definitions and data dictionaries to be adopted
- Identifying the priority areas for improved Social Protection information and investment
- Demonstrating value for money in information-related investments
- Providing advice on international best practice in the areas of Social Protection information and information and communications technology
- Providing representation for the stakeholder groups in the area of Social Protection information
- Promote a common approach to security, privacy and confidentiality
- Develop and agree guidelines governing access to information held by Social Protection agencies
- Carry out information audits
- Promote education, training and skills development for information staff
- Promote and coordinate national research and development of eSocial Protection
- Advising on updates of the Information and ICT action plans as appropriate
- Assist efficient and effective procurement of Social Protection information technology for the Social Protection System.
- Publication of an annual report.

These functions are partly performed by the NORK Information Analytical Center. This center is the key implementer of ICT projects of MLSI and its staff have substantial knowledge concerning

automation in the Social Protection sphere. But functions of the IPU must be focused on other areas of ICT activities: policy making, planning, monitoring and control. These functions may not be collocated with project implementation or operations.

In order to fulfill its role, the Information Policy Unit will need to have access to all the necessary information and data available within the Social Protection area to enable national policy development and integrated service delivery, while ensuring that confidentiality and privacy are respected fully. The legal framework that will be put in place to ensure this access is set out. Close cooperation and coordination of IPU with MLSI, Agencies and NORK IAC is a key success factor.

### **Access to Information –The Portal solution**

Stakeholders are currently faced with many barriers in gaining straightforward access to the information they need whether in paper or electronic format. The reasons for this include the following:

- The great diversity of systems and sources results in a lack of awareness of the scope and depth of the information available and how it might be accessed.
- Information may not be fully analyzed and interpreted or widely distributed in a relevant format and its quality may be unclear.
- The differing roles, priorities and histories of the agencies involved may contribute to a cultural hesitancy towards the sharing of Social Protection information, together with the general absence of agreed upon mechanisms and guidelines for doing so and uncertainties over issues of privacy and confidentiality.
- There is no effective mechanism at present to draw the myriad strands of information together enabling their fullest use on a national basis.
- Application of IT capacity to facilitate the delivery of information and other eServices to clients and professionals remains underdeveloped.

The development of a Social Protection Information Portal to provide a single point of Internet access to Social Protection information and eServices to all stakeholder groups is necessary.

IPU, given its remit in producing a multi-annual information and ICT action plan, will take the lead role in coordinating the development of the Social Protection Information Portal.

As the capacity of ICT continues to develop, as information sources become more standardized and as the framework for eSocial Protection service delivery is extended, so the range of services made available directly through or linked via the Social Protection Information Portal can be extended and improved.

The Social Protection Information Portal should also facilitate and promote the availability of information and services to people who may not have access to or experience of internet applications. Many people most in need of services will fall into this category, and it is critical

that the benefits provided by the Portal can be extended through telephone facilities, walk-in centers, information leaflets and campaigns and other appropriate media and formats. It will also be essential that information for the public is both timely and accurate.

A key objective of the Social Protection Information Portal will be to facilitate access to statistical data and databases to serve the needs of policy analysts, service planners, researchers, and others with Social Protection data requirements. General access to aggregate statistics will be available online, and restricted/authenticated access to disaggregated data for more in-depth research will be authorized in line with information governance requirements and agreed mechanisms with source agencies.

## **Unique Identification**

Unique identification promotes the quality and safety of services in many ways.

The SSC Number has the potential to meet many of the key requirements of the Social Protection System including:

- A robust means for unique identification
- A robust means of authentication
- A comprehensive core client index through continuous updating by all sectors
- A means for providing linkages to the wider public service for a variety of purposes ranging from determining eligibility for public Social Protection services to banking services
- Provision of a high level of protection and security.

However, initiatives to incorporate the SSC Number as a common key in the process of migrating towards a unique identifier within the public sector has proven to be a challenging task, especially with regard to the incorporation of unique identification within existing databases.

Use of the SSC Number is currently confined to specified agencies within the public sector, and any further extension of its use requires legislative provision.

## ***Supporting infrastructure***

### **Information Governance and Legislation**

Information governance provides the stakeholders with a clear and practical basis for the appropriate use of Social Protection information. Some references to best practices materials of Information governance may be found in Appendix B.

Issues such as information sharing, Social Protection surveillance, quality assurance, confidentiality, privacy, records management, freedom of information and data protection are included.

The Social Protection Information Act will aim to put Social Protection information governance on a sound and robust footing and provide a clear legislative context for supporting Social Protection service processes while recognizing the rights and duties of clients, Social Protection professionals and Social Protection agencies. Above all, the act should foster and support a culture that ensures and safeguards the appropriate and best use of Social Protection information.

The eight principles of data protection are that data should be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection.

#### Code of practice

To assist Social Protection service staff in the everyday collection and management of personal Social Protection information a handbook of good practice will be prepared. The handbook will include developing a Code of Practice supporting shared policy and practice and provide guidance on good practice in the collection, protection, use, disclosure and disposal of personal information in the context of the Social Protection System. It will draw on emerging international practice and it may be that more than one version of the code will be required for different groups, and be updated as required. The Code would put the statutory requirements within a context of good practice and professional ethics, offer practical advice on everyday situations, recognize the range of contexts in which access may be required, and reassure Social Protection professionals that practice within the guidelines would be in accord with requirements.

#### Statistical data

The EU Data Directive applies to the processing of personal data (i.e. relating to a living individual who can be identified directly from the data itself or in conjunction with other data). It does not apply to statistical data processed in a form that does not allow for the identification of individuals. Statistical data can be generated through the use of a number of sophisticated techniques including:

- Anonymization of data by the removal, aggregation, or conversion of information items which would identify the individual
- Pseudonymization of data on transfer to specific parties so as to protect privacy but allow connection back to the individual where such reference becomes necessary

- Restriction of disclosure by aggregation or manipulation of data so that the recipient would be unable to restore the information to an identifiable form.

There is a need for information systems to separate the identifiable from the non-identifiable data and, in response to the Data Directive, to rely where possible on the latter. Social Protection professionals need guidance on the appropriate statistical practices to safeguard privacy and confidentiality together with a common approach to be adopted, for example in relation to record linkage and the avoidance of re-identification of individuals. These issues will be addressed in the business rules and information governance arrangements of Social Protection agencies.

### **Information Standards and Quality**

Information standards are necessary to allow for the sharing of Social Protection data.

The adoption of standards is an essential requirement for improving the quality and usefulness of information for all stakeholder groups.

The bulk of information systems operated by service providers do not conform to the same standards, making inter-operation and information sharing impossible. This clearly has implications for operational efficiency and effectiveness. In the absence of a national mechanism for the selection and adoption of information standards, Social Protection agencies record and process the same data in a great variety of ways.

The successful implementation of this Strategy is heavily dependent upon the general adoption of information standards. Standards will be fully incorporated into the development and enhancement of information systems, building upon the available expertise and progress already made in this area.

#### Data standards

A key requirement for Social Protection information systems is to have consistent coding and classification systems for the data items, ranging from the most objective and quantitative (e.g. sex, date of a visit) to the more subjective and descriptive. It is important that data content, e.g. name and address, is recorded in the same format by different systems.

#### Common indicator sets

Common approaches to the use of information depend on the availability of national data standards. The Social Protection Information Systems are examples of an application that can provide added value and insight by bringing together data from diverse sources in a common indicator-based format.

#### Technical standards

Technical standards are required in a number of areas, including messaging, connectivity and security. Messaging is the process of exchanging specified Social Protection data (agreed

datasets) between individual users or agencies using the same language, conventions and coding system in accordance with strict rules; for example the exchange of test results between primary and secondary service information systems. Connectivity is the ability to connect computers and information systems so that they can exchange data in a transparent way.

Data containing personal and sensitive information are confidential and ensuring their security is of paramount importance. There are a number of approaches to security standards, all of which can be deployed together including:

- **Physical security** which ensures that only authorized personnel can physically access information through PCs, terminals, printouts or other areas where information is stored
- **Authentication** of users, for example through password, PIN numbers or biometrics, required to gain access to information electronically
- **Restriction of access** to information to groups on a 'need to know' basis, e.g. front desk staff cannot access personal information and service staff cannot access financial information
- **Audit trails** of access attempts which help to identify attempts at unauthorized access
- **Encryption**, an added layer of security that is usually used for messages being exchanged between agencies, but is used at a local level if required, including storage media (such as disks).

### Quality standards

The quality of Social Protection information is closely related to the issue of data standards described above.

Data quality includes coverage in terms of the capture of all relevant records, comprehensiveness with respect to the information collected and accuracy of coding and data entry. The concept of quality can be extended to include timeliness of data and well-specified procedures for its use and dissemination.

The important components of quality assurance in information systems include:

- Ensuring use and usefulness of the data to data providers
- Regular audits of data to assess quality with respect to coverage, comprehensiveness, accuracy and adequacy of validation procedures and the timeliness, use and dissemination of information
- Personal involvement of data providers in the system
- Application of internationally recognized quality standards wherever relevant.

### **Information and Communications Technology**

Information and communications technology (ICT) includes hardware and software for the support of Social Protection information.

ICT offers many ways to make the Social Protection service more people-centered improve the quality of services, help staff to make better use of their time and expertise and promote greater efficiency. The range and quality of ICT solutions has vastly improved over time and it can revolutionize the way information is shared between Social Protection service staff.

ICT is a tool to facilitate the collection, analysis, dissemination and use of Social Protection information. It is not an end in itself and it is essential that strategic ICT developments are determined by the information requirements they are designed to serve, not the reverse. Looking to the future, the recommendations under this Strategy will facilitate standardization and enhance the information capabilities arising from ICT.

There have been ICT systems implementations and usage within the Social Protection services for many years and it is important to note that there is considerable knowledge and experience in relation to ICT in the Social Protection services.

However, it is hard to conceive of an operation of such complexity, and involving such a level of commitment, being managed effectively with the current level of funding of information systems. The legacy of under-investment in ICT is an inadequate infrastructure to support the complex information requirements of a modern Social Protection service. However, has been agreed for the 2004 Estimates. This development and underlines a commitment to make the necessary decisions to prioritize

Information is the very foundation of a high quality and responsive The Social Protection System. That is why an increase of funding for Information Systems development and modernization is very important if senior management is committed to significant development The Social Protection System.

In the most of areas ICT provision is very limited and does not provide significant support for complex business processes. There is an urgent need for a mechanism to determine and enforce data standards on a Social Protection services wide basis so as to ensure ICT conformity and connectivity and the availability of Social Protection information across the Social Protection System.

As ICT opens up new horizons for its use in The Social Protection System, such as the Social Protection eServices, it is also becoming increasingly complex, sophisticated and costly to implement and support. At the same time, the need for better information sharing between clients and service providers, and within and between agencies is ever more apparent. It is recognized that ICT is also a powerful enabler and catalyst for organizational change but for the purposes of this Strategy the focus is on information. To ensure value for money, spending on ICT must be complemented by major change management programs and supported by comprehensive business cases.

### National ICT System Platform

There is a need for a national, cohesive and integrated approach to the implementation of modern ICT solutions in response to priority Social Protection information requirements.

Organizations must develop and implement plans for accessing and securing information throughout its lifecycle and delivering it within the required service levels. Servers and storage systems need to be scalable.

Due to explosion in the quantity of data it is critical to find ways to increase productivity, control costs, eliminate downtime, and derive more processing power and speed from the existing platform infrastructure. System platform and infrastructure has to support a dynamic, flexible and resilient information environment.

Virtualization technologies are important to deliver uninterrupted access to data and applications. Virtualization allows multiple servers, storage devices, and other physical infrastructure components to work as one logical unit. It helps organizations to optimize the capabilities of the existing infrastructure and simplify the management of increasingly complex heterogeneous systems.

Tools to manage and monitor security are important to ensure that all system assets utilized to their full potential to support needs for information and enables quick decision making.

Development tools are required to ensure that databases and other information infrastructure components are designed efficiently and accurately.

It is preferable to base system platform on open industry standards.

National ICT developments have to take into account EU eGovernment initiatives such as Reach/eBroker and OASIS. eBroker services enable the appropriate exchange of information within each public service sector, such as access to client databases and the provision of robust user authentication services. As the eBroker for all Government services may not hold information specific to any sector (such as Social Protection, Social Protection, education, local government), a dedicated eBroker function may be required, holding more detailed information relevant to Social Protection, for example pointers to where relevant information might be held or to key Social Protection data held in summary format.

### **Operational Information Systems**

First class ICT support for Operational Information Systems is essential for the delivery of first class Social Protection services. It is also essential for the collection of a very large proportion of the information underpinning this Strategy. Collection of information at the operational level ensures its fullest use and highest quality.

A wide range of Operational Information Systems is required to support the entirety of the Social Protection service.

Work will be started by the Information Policy Unit as soon as possible on developing the scope and specifications for the electronic records of The Social Protection Systems as a frontline operational information system.

The introduction of unique identification is of crucial importance in this regard. It is recognized that introducing the electronic record throughout the Social Protection System will be a vastly more challenging undertaking than any that has occurred in the past.

### **Fast and secure communications infrastructure**

The appropriate sharing of Social Protection information between Social Protection service staff and their clients is a prerequisite for good-quality service. The development and implementation of a fast, robust, reliable, scalable and secure communications infrastructure for carrying all Social Protection service communications traffic within the sector on a national basis is of central importance to this Strategy.

The Corporate Network for information flows for Social Protection sector organizations will provide the basic data communications networking infrastructure for Social Protection and Municipalities. The Social Protection services are actively participating in the CNIF project. The CNIF will facilitate the creation of smaller networks within it (e.g. a region, a Social Protection agency or hospital, a team within primary service) to serve specific groups of authorized users who are given a portfolio of access appropriate to their needs, such as access to specific hospital databases from primary service. The CNIF will provide the underlying technology to enable the real time and secure exchange of information between The Social Protection System organizations and their territorial offices. It is a key requirement for supporting the functionality of the electronic Social Protection records and for providing immediate and secure access to services and the Social Protection information Portal and the knowledge databases through the Internet.

### **ICT action plan**

The multi-year information and ICT action plan will set out national ICT priorities. The Information Policy Unit will undertake this work as a high priority.

The plan will take this Strategy as its framework and, in developing the plan, will review available relevant strategic reports in the area of ICT. It will include a national implementation plan that builds upon the existing ICT infrastructure where appropriate. The plan will ensure that the process of identifying and remedying strategic Social Protection information deficiencies is fully supported.

The plan will also ensure that a standardized approach to systems is taken on a national basis and that value for money is achieved. The process may involve commissioning centers of excellence to pilot developments where there is a commitment to national roll-out following a successful pilot. The Action Plan will be broad-ranging and, in addition to the phased implementation of the electronic Social Protection records and Social Protection eServices, other specific areas to be included are outlined below.

A national data model will be included in the Action Plan which will be at a strategic level and will consider the major elements of Social Protection information and their locations.

It will define the major information flows and the level of integration required between databases.

The model will define the location of major databases, such as the database to support the national unique identifier (SSC number), and who will have responsibility for their maintenance. Additionally, it will define how the model will interact with the public service broker and how these databases will be accessed by the various levels of users. The model will also address how the electronic Social Protection records will assimilate data and how user access will be provided.

The information and ICT action plan will, inter alia, deal with the following:

- A national secure communications infrastructure
- Electronic broker services
- ICT support for primary services
- A national ICT inventory
- Relevant universal access to email/Internet services
- A national waiting list database
- Self-service solutions.

### ***Information Infrastructure***

Data is the most important and underused asset in the Social Protection System. The transformation of data into information that is valued and used is fundamental to delivering better services and making decisions.

Information needs to be delivered in the right business context at the right time. The relevant information must be accurate, consistent and available when and where it is needed. Equally the misuse, copying, theft, loss and abuse of your information can be the cause of litigation and even business failure.

To achieve this goal expertise in the data needs of all stakeholders, both producers and users of data, is required. Through collaboration between business and IT, it is possible to develop and manage sound business processes aligned with its strategic and tactical information needs.

Support of Information Infrastructure, which is flexible and adaptable for changes of business needs, will require from IT to:

- Be aware of existing **data** and associated **data collection mechanisms**,
- Recognize **duplicates of data sources** and stop unnecessary data collections,
- **Identify additional data sources** whenever it is necessary.

The foundational components of a flexible and cost-effective information infrastructure include scalable and high-performing servers for structured data.

Information stored in various formats and locations needs to be analyzed, cleansed and integrated in an accurate and consistent way into data warehousing or master data management, and for multiple other uses across the organization.

Some references to best practices materials of Information Infrastructure may be found in Appendix B.

## ***Business Solutions***

Fundamental goal of IT is to provide solutions (**MIS, Databases, Data warehouses, WEB sites, etc**) for timely delivery of relevant information for solving specific business problems:

- Improving **quality, availability and effectiveness of services** and making them citizen-friendly
- Allocating and making **efficient use of resources**
- Supporting and facilitating **decision making process**
- Development and implementation of **Monitoring and Evaluation policy**

Integration is critical success factor for solving major problems of current solutions and achieving specified above goal.

There are several aspects of integration:

- Regional Centers with Headquarters
- Interagency: Social Insurance, Social Assistance, Employment Services, etc
- WEB portal, integrating access to social services and creating single entry point for self services and information sharing
- Integrated social services centers

IT solutions provide strong foundation for all aspects of integration. In particular they include:

- IT Infrastructure improvement (LAN, WAN)
- Development of automated and flexible data exchange mechanisms
- Development of social sector WEB portal Integrated social services center
- Development of integrated system for social sector, including monitoring and evaluation subsystem

Examples of best practices for eGovernment solutions may be found in Appendix B.

## ***Implementation and Monitoring***

The Strategy implementation will require a complex range of developments and changes in legislation, organization, management and culture. This will present significant challenges throughout the sector, and effective change management processes will be of particular importance.

Strong political leadership is critical to the success of this Strategy because it ensures the long-term commitment of financial resources, personnel and technical expertise in the design, development and implementation of e-government projects.

Strong leadership means garnering support for the projects at all levels, involving the public and meeting their needs and expectations, acting as a catalyst for intergovernmental collaboration, being willing to share the power and credit, establishing and meeting milestones, and maintaining a sense of urgency to complete the e-government projects.

Success of this Strategy is dependent upon the presence of ongoing strategic direction, a strong central driving force and regional and local mechanisms that ensure its consistent, effective and timely implementation. As mentioned below, major investment in human resources, capital projects, new technology and change management is required.

The MLSI Executives will set down the levels of investment required in implementing major Social Protection information systems. There are potential opportunities for use of donor project resources and cooperation with regard to information and ICT.

Another important issue is public-private partnerships. There are many reasons for developing partnerships with the private sector in developing e-government projects. First, there is the possibility of cost-sharing projects, with a possible return on investment for the private sector. Second, the private sector has invaluable expertise that can be tapped by government in the areas of customer satisfaction, work productivity gains, and personnel efficiency. Third is the possibility of technology transfer from the private to the public sector.

### Infrastructural requirements

A number of infrastructural developments are required to support the implementation of this Strategy, as it is essential that a clear mechanism exists for implementing all of its dimensions.

An effective process for monitoring and enabling its progress over time in line with the targets and deliverables as set out in the Action Plan is essential. The Action Plan also specifies the lead responsibility and timeframe for each element.

### Human resource and change management requirements

The availability of appropriately skilled and trained staff to support the potential of information within Social Protection agencies, together with providing the skills-base and training programs

to support the roll-out and full use of major ICT solutions throughout the sector, are critical for the implementation of this Strategy.

Developing the capacity of the Social Protection System to deliver on the actions set out in this Strategy requires significant and sustained investment in human resources.

Using ICT and information effectively requires an understanding of its potential together with imagination, innovation and an appreciation of the way people currently work and how they can be enabled to work differently. This goes far beyond new skills training and requires fundamental changes to the ways in which people interact with each other and use information. The most immediate effect is often felt by those closest to the operational information systems while those in positions of management must modify their management style to exploit the benefits of the newly available information. While using ICT to optimize service delivery requires that technology be designed around the needs of the people using and providing those services, the migration towards a set of common systems for similar functions throughout the Social Protection service and the need for standardized information will force some standardization of procedures. The implications of a transition from a mainly paper-based The Social Protection System to a digital environment should not be underestimated as such a transition will be a significant cultural challenge to Social Protection service staff. Considerable effort will be required to manage the necessary changes in procedures and practices.

With respect to ICT, innovative programs are required in structured project management methodologies, business process reengineering, process mapping, benefits realization and new and emerging technologies and applications. With respect to information management, the same innovative approach is required, with particular emphasis being placed upon developing skills in information science, information management, data quality, business intelligence tools and a broad appreciation and understanding of the complementary role that ICT has in information management. The training requirement, however, extends beyond the traditional information management function. Information authors, information providers, information consumers and those who form part of the knowledge management and information society value chain also need relevant training. The training requirements will be different for the various information constituents and careful consideration is essential for the development of such programs.

#### Information governance requirements

Effective Social Protection service demands close cooperation and teamwork. Better communication and information sharing can be of great benefit to the individual and to the service overall, but there are also risks to privacy and confidentiality. Harnessing the power of modern ICT systems within the Social Protection service increases benefits and risks. There is a need for a cultural change regarding the use and sharing of Social Protection information throughout the Social Protection System if the benefits are to be reaped while the risks are minimized. It is essential that a clear and supportive legislative and information governance framework be established for the appropriate use of Social Protection information throughout the sector, while safeguarding privacy and confidentiality.

### Information system requirements

As already pointed out, major and sustained investment in information systems is required. Otherwise it will not be possible to provide the necessary scope and depth of information that is necessary to meet the complex requirements of the Social Protection System. Major investment in systems is required so as to provide a basis for coherent and consistent appraisal of effectiveness, efficiency and economy, and to determine the value for money being delivered in return for increased levels of investment in the system generally or in its component parts. This Strategy requires investment in the phased adoption of modern enabling technologies of proven value. It will take advantage of the developing Social Protection information infrastructure and the new opportunities that arise in the evolving field of ICT.

### Funding requirements

A The Social Protection System urgently needs greatly improve the availability of high-quality information. Indeed, the achievement of the objectives of these strategies is largely dependent upon the availability and proper use of information.

It is recognized that there is example of good Social Protection information system and that there is a growing body of expertise in using information and in implementing ICT solutions.

However, it is clear that the level of investment in Social Protection information in general and ICT in particular is central to difficulties in meeting the complex information requirements of a modern Social Protection service.

However, the full extent of what is needed across the Social Protection service in terms of properly integrated and comprehensive systems, including at the level of individual clinicians, will be worked through by the Information and ICT Action Plan.

Initially, the vast majority of these costs relate to identified below major ICT programs. A number of options will be explored in funding the investment program in order to maximize its effectiveness in terms of cost, system delivery and performance. These include outsourcing, strategic alliances with the private sector. The benefits of shared services across agencies for common functions and for agencies providing similar types of services will be considered. In some areas it may prove beneficial to outsource elements or all of a particular service. Each option will need to be assessed on its own merits, taking into account the cost effectiveness that can be achieved through economies of scale and critical mass. A major part of the Information and ICT action plan will be the identification of the most cost-effective delivery Implementation.

The implementation of this Strategy is divided into three phases, but in the knowledge that the whole process is closely interdependent and will be influenced by factors outside the Social Protection System itself. In addition to the new initiatives, the cycle of ICT upgrading and replacement will continue, but it will be carried out in the context of the Information and ICT action plan and in light of the policy of a common approach to ICT investment and deployment set down.

It is recognized that there must be ongoing investment in a change management process to accompany the implementation of this Strategy. No matter what decisions are taken on future methods of resourcing and implementing the Strategy, a change management program is essential if we are to grasp the opportunity presented to transform the way the Social Protection System responds to community and individual needs. This will entail a radical analysis of the organization of work throughout the system and a determination to follow through with the necessary changes. An information-based culture amongst all personnel is fundamental to any modern The Social Protection System. The costs of this change, including appropriate facilities, development of new procedures and training staff in their use, should be an integral part of any systems implementation.

#### Develop formal policies on outsourcing

IPU and MLSI must establish clear parameters for working with the private sector. Outsourcing requires government Agencies to use and develop new types of contracts - with clear benchmarks of performance - that will not only ensure the delivery of good services, but also measure the performance of vendors and the quality of services received. More important, the bureaucracy needs to be trained in how to negotiate and draft such contracts.

Empirical evidence recognizes the critical role of the private sector as often a partner vital integral actor in a country's ICT component in the development efforts and progress of ICT in general. In a capital intensive industry like ICT, the government Agencies has found itself a partner in the private sector. This is also true of e-Government.

Having the private sector fully participate in e-government has many advantages. It could mean passing off the costs of design, development, maintenance, and risk to the implementing firm. Moreover, by using private partners, state governments can build e-governance systems at greatly reduced costs, for start-up and ongoing operations. At the same time, more services can be delivered on a fee-for-service basis, with the private partner being paid from the fee revenues. Thus, e-government can be a tool for moving certain government services from tax-based financing to user fees, where only those actually using the service pay for it.

#### **Implementation Phases – Roadmap**

This Strategy will be implemented on an incremental basis, and the overall process is divided into three broad and overlapping phases: phase 1 (year 1), phase 2 (year 2) and phase 3 (following 3 years) following the publication of the Strategy.

Usually evolution of e-Government solutions may be divided into five stages:

1. Planning stage: Setting up task forces, strategy formulation, creating coordination structures.
2. Working pilot projects that demonstrate value of e-government applications.
3. Working pilots demonstrating successful scalable models.
4. Replication/Rollout on a wider scale (Countrywide).
5. Stage of maturity reflecting integrated functioning of e-government applications.

Stage 1 may be implemented during phase 1. Stages 2 and 3 may be merged and implemented during phase 2. Stage 4 fits into phase 3.

Stage 5 goes further than just delivering services through a single channel i.e. via the Internet. Increasingly other forms of ICTs will be used to connect citizens and government agencies including ATMs, mobile phones, community service centers and call centers. An e-government application would be considered more evolved if it offered many alternate channels to a citizen to transact business and a friendlier and convenient interface design. Stage 5 is beyond this Strategy.

At the outset, emphasis is placed on getting the essential building blocks into place at the earliest opportunity. That is why pilots are essential for proof of concept and risk minimization.

Given the scale and scope of the Strategy and the resource requirements, many of which will only be identified over time, a precise timetable is not set forth.

Actions and processes to attain goals	
Short term (present to end of 2007)	<p><u>Planning stage:</u></p> <ul style="list-style-type: none"> <li>• <i>Recommendations for IT Infrastructure improvement (LAN, WAN), pilot implementation</i></li> <li>• <i>Assessment of current Information Infrastructure and recommendations for improvement</i></li> <li>• <i>Recommendations for data exchange mechanisms (eBroker services)</i></li> <li>• <i>Recommendations and action plan for IT systems improvement or development</i></li> </ul>
Medium term (2008)	<p><u>Pilots stage:</u></p> <ul style="list-style-type: none"> <li>• <i>Implementation of improved IT systems</i></li> <li>• <i>Development and Implementation of automated and flexible data exchange mechanisms</i></li> </ul>
Long term (2009-2011)	<p><u>Rollout stage:</u></p> <ul style="list-style-type: none"> <li>• <i>Implementation of Nationwide information systems architecture in compliance with the demands of data protection and information security.</i></li> </ul>

- |  |  |
|--|--|
|  | <ul style="list-style-type: none"><li>• <i>Development of social sector WEB portal</i></li></ul> |
|--|--|

For measuring progress of eGovernment evolution, the following two indicators are the basis for benchmarking:

- Percentage of basic public services available online,
- Use of online public services by the public.

To make these indicators operational, EU member states have agreed to a common list of **20 basic public services** [9], 12 for citizens and 8 for businesses. Progress in bringing these services online will be measured using a four stage framework:

1. **WEB PRESENCE**. Posting of information online: publish rules and procedures and other static information on the Web
2. **LIMITED INTERACTION** (one-way interaction). Allow email contact, access to online databases and downloadable forms;
3. **TRANSACTIONS** (two-way interaction). Electronic Delivery of services with some or all stages automated
4. **TRANSFORMATION**. Full online transactions including delivery and payment. Joined up Government One stop shop for services that cut across many Agencies.

This measuring model may be used as a basis for development of indicators for monitoring of Strategy implementation progress.

## Part 3 Action Plan

"The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency."

Bill Gates - Co-Founder and Chairman - Microsoft

Introduction of ICT is not a goal in itself. Through, the Social Protection Agencies can transform and make more efficient their own operations and the way of interacting with citizens and businesses. The use of ICT, together with applications, supported by a legal and policy infrastructure, is embedded in a process that is being driven by the promotion of good governance goals and public sector reforms. Technology can be catalytic, but the process means a re-orientation of Social Protection services towards serving citizens and businesses, which implies a change of work procedures, and the attitude of officials.

Collaboration with donors and with the private sector will be essential to advance use in ICT in Social Protection sphere throughout the country. Private organizations that participate in achieving these objectives could be supported by special measures of the government.

In the previous part the following strategic areas have been identified:

- Infrastructure development and de-bottlenecking
- Enabling policy and legal framework
- Building human capacity and institutions

To achieve progress in these areas necessary actions have to be taken to achieve the following strategic goals:

- Well-Coordinated ICT Policies in Social Protection sphere
- Creation of ICT-Supportive Legislative Environment
- Implementing citizen-centered, transparent, efficient services
- ICT solutions for Social Services
- Development of inexpensive, fast and secure ICT infrastructure
- Monitoring of ICT Developments in Regional and European Context

### ***Goal 1: Well-Coordinated ICT Policies in Social Protection sphere***

To successfully introduce and deploy ICT in Social Protection sphere, MLSI will have to assume a role as a champion and driver. This role must be institutionalized and embedded in ministry to have a long lasting effect. The nomination of a champion and the creation of proper organizational structures is a fundamental action for the successful implementation of ICT, as demonstrated by examples of other countries. The first goal aims at defining responsibility for ICT for and within the Social Protection sphere by creating an IPU, which will be in charge of the overall coordination of ICT policy within the Social Protection sphere and with other

ministries and state agencies. Follow-up of the strategy and its implementation, coordination and general awareness creation are also defined in this first goal.

## Strategic Activities

- Institutionalizing the role of the Information Policy Unit as ICT champion in Social Protection sphere.

Strategic Direction #5 of ‘ICT Master Strategy for Republic of Armenia’ states that ‘The government will undertake specific actions to assume leadership in ICT development and to expand and improve the quality of public services delivered to citizens and business via the deployment of ICTs.

To achieve leadership in ICT development the following actions were planned:

- Ensure efficient coordination of ICT-related activities being carried out in Armenia
- Appoint or Chief Technology Officer (CTO)

Following the same direction MLSI will have to take the lead in defining and implementing ICT strategy in Social Protection sphere. The Minister will nominate Chief Information Officer (CIO) of the ministry responsible for ICT and will establish under his supervision a permanent Information Policy Unit (IPU), which will be responsible for the coordination and monitoring of the implementation of the national ICT strategy, including those issues pertaining to e-governance based public administration practices and which will co-ordinate ICT standards with other relevant ministries.

This body will assume a horizontal function within the ministry. It will promote and ensure the use of ICT, prepare the planning and implementation of the ICT strategy, coordinating the use of ICT within the whole ministry, and will recommend future actions. IPU may be created in MLSI secretariat.

As part of this organizational measure, a special item on ICT will be created in the ministry budget. It will also be in charge of relations to and coordination with the donors.

This State Body will be supported by a Forum for Information Society, composed of government representatives, civil society, business, and academic community. Wider issues will be covered by Parliament. In setting up these entities, their role and functions will be more precisely defined.

- Action plan for implementing the ICT strategy

An action plan will be derived from the national ICT Strategy and serve as the base for implementing the Strategy. It will be defined as the responsibility of the ministry, in collaboration with all stakeholders, in particular in public-private partnership. It will integrate ICT implementation and deployment within the framework of institution building.

- Coordination and Follow-up of ICT Strategy

Having defined the ICT strategy and the action plan, it will be necessary to coordinate its implementation within the ministry, and together with the other stakeholders.

- Promotion of the information society in the Social Protection sphere

Awareness creation activities have to be planned and executed to inform all civil servants about the information society, and the plans for deploying ICT in the Social Protection sphere. Awareness creation will enable civil servants to better understand the value of these technologies in their work.

## ***Goal 2: Creation of ICT-Supportive Legislative Environment***

The proper legal and regulatory framework will facilitate the use and adoption of ICT, and create trust and confidence in the use of technology. Regulatory mechanisms aim at supporting the application of ICT in Social Protection sphere, and at protecting citizens and businesses. The risk is over-regulation: too much regulation may slow down the efficiency of the further deployment of ICT. Therefore, the interests of the private sector should be considered in defining or adapting legislation.

Private sector should advise on new legislation and it must be actively involved in the process of the preparation of the legislation.

The modernization of legislation and introduction of new laws necessary will follow mainstream of European legislation and directives. Experiences from other countries will be considered.

For example, the Council of Europe has developed Convention No. 108 (1981) “for the protection of individuals with regard to automatic processing of personal data”. Important elements of the Convention are obligation of the Parties to ensure relevant measures of the personal data protection and appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles of the Convention.

Armenia is not a signatory to this important international document which was signed and ratified by a majority of the European countries. In spite of the fact that the Council of Europe Convention No 108 has not been ratified by the Republic of Armenia, in 2002 the National Assembly of the Republic of Armenia adopted the Law of the Republic of Armenia “On Personal Data”. In general the law complies with the principles outlined in the Council of Europe Convention No 108. However, there are some gaps in the Armenian legislation related to specific provisions of the Convention that does not provide adequate protection for personal data stored in public and private databases. One of these gaps is the absence of “appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection” as required under the Article 10 of the Convention.

## Strategic Activities

- Structural measures for ICT legislation

The responsibilities and functioning of the regulatory agencies will be reconsidered, with the objective of compliance of their duties and supervision of the communications and information operations on the basis of EU principles.

Giving concessions to operators and service providers should be subject to investments in the development of information and communication infrastructure for general accessibility, and in compliance with international standards.

- Development of relevant e-legislation

Existing laws will be examined in view of the needs of ICT deployment, such as patent laws or copyright law, and new laws will be developed, in accordance in particular with EU directives.

Such laws are those for e-signature, e-contracts and e-documents, access to public information, data protection and privacy, consumer protection, Intellectual Property Rights legislation for copyright, databases, patents, software and semiconductors, and others.

Relevant banking laws will be amended to accommodate ETF (Electronic Funds Transfer) and payment through credit/debit cards. Minimal technical standards and procedures will be defined.

### ***Goal 3: Implementing citizen-centered, transparent, efficient services***

Implementing e-government implies the reorientation of focus from ministry or agency procedures towards citizens and businesses, as customers. A fully functioning e-government cannot be built in one step; it involves subsequent building of several types of such services going from information provision to a fully-fledged interactive government. Customer orientation, along with the use of ICT tools will then lead to more efficient working and streamlining of work processes.

E-government services must not abruptly replace traditional services. Both the traditional means of communicating with administrations and the electronic means will co-exist for a certain time to assure a smooth transition. There are two reasons for this. First, the users have to accept the new ways of communicating, and to learn how to use them. Second, electronic services require the existence of a network infrastructure, which will be built gradually.

The third goal will plan and establish eServices in Social Protection sphere, in transforming traditional administrations and services. Corresponding actions will deal with information systems and their use in the Social Protection sphere; those systems would be planned and used in an integrative way, and with higher efficiency of services in mind, as well as delivering higher quality services to citizens and businesses.

The Social Protection sector consists of several Agencies and therefore, implementation of ICT would go through a process of coordination to assure the interoperability of independent information systems. The role of the responsible CIO and Information Policy Unit is to assure this interoperability rather than taking direct control over development processes.

## Strategic Activities

- Overview of e-government in other countries and its applicability

Study implementations of e-government in similar countries or examples of the best use of e-government services (Bulgaria, Croatia, Estonia, Ireland, Portugal, UK, EU, Australia, etc.)

- Development of an overall concept and plan of development for information systems and eServices

This will set the main directions and priorities in the area of electronic administration. Based on this, a conceptual model will be developed, which includes networking, models for public data, standardization of hardware components, software, databases, etc., types of information systems, organizational models for using and working with information systems, planning of eServices, feasibility studies, specifications. The result will be a basic specification for services in the electronic administration, and a complete architecture for countrywide integrated information system as the base for eServices.

Existing solutions, databases and information systems will be analyzed, and possibilities for their integration defined.

*Procedures will be developed for monitoring and updating the specifications to the evolution of the use of ICT.*

- Definition and implementation of priority services

Some services will be selected as a priority and implemented throughout the country according to the standards developed in the overall concept.

The implementation will start with pilot projects, which, if successful would be rollout countrywide for general use. Such services could include ESA IT system GORTS, PARNAS, because of their large impact on the total development of eServices.

The Social Security Card system will gradually contain data to be used by eligible state and private users, making possible the direct distribution of information for those institutions that use this information as a key source in statistical, social insurance, education, public order, justice and other fields.

Gradually, companies will be required to use the electronic services in order to work with the government services.

- Development of interactive web -based access to public information

All ministry agencies will develop a web presence, in order to provide information about their services to citizens, and establish a means to interact with the citizen, via email or world wide web forms for certain administrative processes. This will involve the definition of guidelines for preparing the ministry's web presence, and the definition of a policy for making public information available to citizens and businesses, based on the European Union's directive on public access to information.

- Civil Servant Training

All activities will be accompanied by appropriate training of civil servants. Training will not only consist of basic training in computer use, but also aim at the reorientation of government services towards e-services. Civil servants will be trained in new organizational procedures based on ICT, and the use of information in e-services.

#### ***Goal 4: ICT solutions for Social Services***

Information as well as basic services is made available via the information infrastructure, which is a fixed and mobile network connecting computers and databases, practically the Internet. The importance of the infrastructure has been widely recognized. For example, the European Union's strategy "eEurope" considers it as one of the main pillars for the establishment of the Information Society.

This infrastructure is the basis of the functioning of the Information Society, but it is expected to co-exist for a long time with the traditional means of information access, such as print, television and radio, which will remain important to many people. The use of the traditional technologies will only gradually be replaced, which is less a matter of the infrastructure but of the existence of applications, services offered and of user acceptance.

The information infrastructure Social Protection services should be enabled to use ICT as a tool, allowing them to work more efficiently and deliver their services with higher quality, thus contributing to increasing the standard of living in Armenia. However, development of computer infrastructure and applications in the sector should take into consideration future decentralization.

ICT tools would mainly be used by the professionals in this sector, but the benefit would be for the user of such services, and especially for the disadvantaged, handicapped, unemployed or elderly, who depend on others or on government's care.

ICT has to be introduced with those beneficiaries in mind. Orientation at users and at work processes will be indispensable.

## Strategic Activities

- Country-wide Social Protection services infrastructure

Services provided via electronic networks in the Social Protection services sector require interconnection between various organizations and access to many databases in the country.

Such an infrastructure for Social Protection services will be defined and planned. In implementation terms it will rely on a Corporate Network.

Issues like data protection and information security will have a high priority. Definition of the infrastructure will also include services made available as well as definition of the data that is used in the services. For instance, national standards will be defined for the Social Protection services data records, as well as other socially relevant data, taking into account international agreements and standards (ISO, ILO, etc.).

- ICT solutions for the Social Protection services sector

ICT tools will be made available to professionals in the social services sector enabling them to work more efficiently and to increase the quality of their service provided to socially disadvantaged people, to handicapped or elderly people. Services and tools will be defined and deployed to support their work, and according to their needs. These could be tools for administration, or those to assist in approval of request for social aid.

The use of such tools will require a network connection between various departments of government and local services, between requesting and monitoring units or statistical offices.

Development of such tools must be done in compliance with international standards. The definition of such services should take into account the advanced technology such as location based services for the monitoring of unemployed people for example.

Below examples of possible activities for implementation of ICT solutions for different areas of the Social Protection sector are enlisted:

### Social Insurance

#### **Short term.**

- Rollout PARNAS to Regional centers.
- Combine personified reporting database (PARNAS) and pensioner database (ARAKS).
- Recommendation for improvement of MIS for personified reporting (PARNAS) and automating data exchange with social card database.
- Monthly reporting

#### **Mid term.**

- Implementation of improved of MIS for personified reporting.
- Recommendation for integration of personified reporting system with social sector portal.
- Recommendation for MIS of reformed pension system.

**Long term.**

- Implementation of MIS for reformed pension system
- Integration of personified reporting system with social sector portal

Employment Services

**Short term.**

- Link regional offices with the center and upgrade ESA IT system.
- Recommendation for automating data exchange with other MIS and databases of social sector.

**Mid term.**

- Implement electronic archiving reception and system.
- Implement automated data exchange with other MIS and databases of social sector.
- Recommendation for integration of ESA IT system with social sector portal

**Long term.**

- Integration of ESA IT system with social sector portal
- Incorporation ESA IT system into integrated Nationwide information system of social sector

Occupational Safety and Labor Code

**Short term**

- Design MIS for data collection, analysis, and risk based enforcement of Labor Code.
- Link regional offices with the center
- Proposal for automating data exchange.

**Mid term**

- Implement MIS at central and regional offices of LI
- Proposal for integration of IT system with future social sector portal

**Long term**

- Integration of IT system with social sector portal

- Incorporation of IT system into integrated Nationwide information system for the social sector

### Social Assistance

#### **Short term.**

- Link regional offices with the center
- Recommendation for integration of IT Social Assistance systems
- Recommendation for automating data exchange with other MIS and databases of social sector.

#### **Mid term.**

- Implement integration of IT Social Assistance systems
- Implement automated data exchange with other MIS and databases of social sector.
- Recommendation for integration of IT system with social sector portal
- Recommendation for Development of Monitoring, Evaluation and Control Information System

#### **Long term.**

- Integration of IT system with social sector portal
- Incorporation IT system into integrated Nationwide information system of social sector

- |   |
|---|
| <ul style="list-style-type: none"> <li>• Information provision in the Social Protection sector</li> </ul> |
|---|

Public services, local administrations or associations active in the Social Protection sector will establish web information services to inform disadvantaged people and their akin to obtain information about possibilities to improve the situation of disadvantaged people, to obtain social care and support, or provide general advice.

- |   |
|---|
| <ul style="list-style-type: none"> <li>• Training of professionals in the Social Protection services area.</li> </ul> |
|---|

It can be assumed that professionals and service providers in this sector have a basic understanding of ICT, but they need special training in the use of highly complex computer systems in this area. Most computer systems will be adapted to the special need of the users, and therefore training has to be integral part of the delivery of such systems. In particular, it necessary to consider this when developing public tenders for the deployment of information systems for this sector.

### ***Goal 5: Development of inexpensive, fast and secure ICT infrastructure***

It is vital that citizens, businesses, and government administrations have access to modern communications networks, which are the base for the provision of information and related services.

This goal aims at building a country-wide Corporate Network infrastructure providing seamless access to data and services. The Corporate Network for information flows for Social Protection sector organizations will provide the basic data communications networking infrastructure for Social Protection and Municipalities.

The Social Protection services are actively participating in the CNIF project. The CNIF will facilitate the creation of smaller networks within it (e.g. a region, a Social Protection agency or hospital, a team within primary service) to serve specific groups of authorized users who are given a portfolio of access appropriate to their needs, such as access to specific hospital databases from primary service. The CNIF will provide the underlying technology to enable the real time and secure exchange of information between Social Protection sector organizations and their territorial offices. It is a key requirement for supporting the functionality of the electronic Social Protection records and for providing immediate and secure access to services and the Social Protection information Portal and the knowledge databases through the Internet.

### **Strategic Activities**

- Design for a country wide Corporate Network

Within the scope of the World Bank “Social Protection Administration Project” and "Public Sector Modernization Project" it is planned to design and develop Corporate Network for Information Flows (CNIF), which will provide the MLSI, SSIF as well as municipalities with a permanent network connection for data exchange between them and accessibility to various data at all central bases from regional centers.

- Implementation of country wide Corporate Network

Based on concepts developed in previous activity the network infrastructure will be built linking national, regional and local government administrations. Any new infrastructure to be built will have interfaces to existing infrastructure in order to achieve co-existence between new developments and existing networks.

It is supposed that there will be gradual implementation of country wide Corporate Network accordingly to technical specifications and requirements developed during the design phase; Acceptance and piloting of CNIF will take place in all concerned agencies.

Existing Internet Service providers are considered as another alternative to offer services to the communities, and as such will be an important infrastructure component in support of the implementation of the strategy, especially in the remote areas.

- Public Access Points (PAP): Cheap and Reliable Internet Access for All

Home Internet connection is uncommon in Armenia, and practically non-existent in rural areas. Only a very slow growth in the number of PCs and home Internet connections can be expected. On the other hand, Internet cafes are growing in the country and are well frequented.

This phenomenon should be supported and will be the first possibility to reach the whole population with the Internet. Public access points such as Internet cafes, Information kiosks etc. should be built in the whole country and in particular their establishment in remote regions should be supported.

Content and applications, or e-government services will be made available via such public access points; pilot projects for PAP in communes using wireless technology would extend the number of connections.

### ***Goal 6: Monitoring of ICT Developments in Regional and European Context***

The implementation of the strategy and subsequent action plan requires a permanent monitoring of the goals of the strategy in order to ensure that the goals can be achieved, and to observe any obstacles or hindrances during the implementation of the strategy. This in turn necessitates the definition of precise goals, including intermediary goals and their follow up. In other words, a roadmap has to be established, along with indicators that allow permanent monitoring. The monitoring will also depend on the action plan that is to be established as a follow up to this strategy, however, the main goal is not to follow the individual projects of the action plan, but to follow the realization of the strategic goals.

The indicators will also allow international comparison of the situation of the information society in Armenia. A relation to the benchmarking process of eEurope will be established.

The monitoring will start with a planning phase, where possible scenarios for the implementation of the strategy in Armenia will be defined, along with indicators and a timetable or roadmap, which allows the precise monitoring. The monitoring process will be performed regularly during the execution of the action plan.

### **Strategic Activities**

- Possible scenarios for the implementation of the strategy

Several scenarios will be designed, including success criteria, the potential for success, obstacles and dangers to avoid. A SWOT analysis will be carried out and repeated regularly to summarize the developments.

- Definition of indicators for monitoring the evolution of ICT

A set of reasonable indicators, may be in the order of 10 – 15 per sector of the strategy, will be defined, following the objectives of the strategy. The indicators will be modeled after the eEurope indicators.

- Definition of a roadmap for the implementation of the strategy

This is the timetable for the realization of the strategic goals defined in this ICT strategy.

The roadmap should be defined for a reasonable timeframe, for example a period of 5 years.

- Monitoring and Evaluation of the Strategy, its objectives and outputs

Having defined and planned the monitoring process, it has to be executed and measurements taken at regular intervals, as defined in the roadmap. The results of this monitoring process should be made publicly available, for example on the ministry web site.

- Monitoring and Evaluation of general quantitative ICT statistics, observatory and surveys of the evolution of ICT in Armenia

It will be very useful to not only follow the evolution of the realization of the strategy with the predefined indicators, but also to carry out more general surveys of the status of the Social Protection sector of Armenia, and to perform an assessment in regular intervals.

### ***Financing Options***

Any strategy can demonstrate its values if there is sufficient money available to finance the planned actions. Very often, however, the question for funds remains unresolved, and strategies cannot be realized. Because of this, it will be necessary to include financing the strategy in the beginning of its planning.

Four different types of actors participate in the implementation of the strategy, with different financing options.

These are the donors, the government, the private sector and the consumers. All should participate in the formulation of the Strategy and the corresponding action plan, and eventually contribute to its financing.

A financing strategy will have to be developed as part of the ICT action plan. This strategy would include options for financing, and aim at effective use of funds to achieve synergy and avoid duplication of effort.

The government will increase its ICT budget in order to finance high priority projects and to catalyze further actions, which subsequently would be financed by other sources. Coordination between donors will have to be part of this strategy.

Donors will provide seed funding to get the actions rolling. They should also prioritize ICT in their programs. Donor funding would remain catalytic during the whole realization of the strategy. The implementation of the strategy should be based on internal capacity and resources; donor support would only enable sustainable development but could never create a dependence on their funding in continuously providing funds. In particular, donor funding could be aimed at attracting private sector investments such as venture capital, private equity or loans, to support larger and more long-term ICT projects and programs.

Donor and government funding would be used in areas that are not directly attractive to private sector investment, such as the deployment of ICT in remote areas. But also here, government and donor funds would be catalytic, aiming at preparing a market for the private sector.

The other actors are the private sector and the consumers; they will finance and invest according to market laws. The private sector, especially, will invest, where it sees an adequate return. The key to financing options will be the nature and extent of public private partnership (which should include government, private sector and donors). The private sector could also establish foundations that could support the long-term research and development needs of the ICT sector.

There are various business models for funding e-government projects, and the private sector plays a critical role in these. Under partnership arrangements, the private sector builds finances and operates public infrastructure, recovering costs through user charges. Various financing schemes exist - from soft and development assistance loans from donor/multilateral aid agencies to partnerships and outsourcing deals with private third party vendors under special financing schemes (e.g., the Build-Operate-Transfer or BOT scheme) that can minimize the initial cost to government.

BOT and its variants are usually the favored financing models/arrangements for government projects that require large and immediate financing from the private sector. Under BOT, the private sector designs, finances, builds, and operates the facility over the life of the contract. At the end of this period, ownership reverts to the government. A variation of this is the Build-Transfer- Operate (BTO) model, under which title transfers to the government when construction is completed. Finally, with Build-Own-Operate (BOO) arrangements, the private sector retains permanent ownership and operates the facility on contract.

Another way for expenses optimization may be special software license agreements with companies like Microsoft and Oracle.

Some other options of public-private partnership for e-government projects may be found in Appendix B and in E-Government Readiness Report 2005 [1].

## References

- [1] UN Global EGovernment Readiness Report 2005,  
<http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021888.pdf>
- [2] The Global Information Technology Report 2006-2007,  
<http://www.weforum.org/gitr>
- [3] Networked Readiness Index (NRI)  
<http://www.weforum.org/pdf/gitr/rankings2007.pdf>
- [4] ICT Master Strategy for Republic of Armenia
- [5] E-Government Act of 2002,  
<http://csrc.nist.gov/policies/HR2458-final.pdf>
- [6] eEurope 2005 Action Plan  
[http://ec.europa.eu/information\\_society/eeurope/2005/all\\_about/action\\_plan/index\\_en.htm](http://ec.europa.eu/information_society/eeurope/2005/all_about/action_plan/index_en.htm)
- [7] i2010 Information Society strategic policy framework, European Commission's  
[http://ec.europa.eu/information\\_society/eeurope/i2010/index\\_en.htm](http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm)
- [8] EU eGovernment Practice portal  
<http://www.epractice.eu>
- [9] List of 20 basic public services  
[http://ec.europa.eu/information\\_society/eeurope/2002/action\\_plan/pdf/basicpublicservices.pdf](http://ec.europa.eu/information_society/eeurope/2002/action_plan/pdf/basicpublicservices.pdf)
- [10] National Progress Report on eGovernment in the EU27+  
[http://ec.europa.eu/information\\_society/newsroom/cf/document.cfm?action=display&doc\\_id=391](http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=391)

**[11] Report to Congress on the Benefits of the E-Government Initiatives**

[http://www.whitehouse.gov/omb/egov/documents/FY07\\_Benefits\\_Report.pdf](http://www.whitehouse.gov/omb/egov/documents/FY07_Benefits_Report.pdf)

**[12] Estonian Information Society Strategy 2013**

[http://www.riso.ee/en/files/IYA\\_ENGLISH\\_v1.pdf](http://www.riso.ee/en/files/IYA_ENGLISH_v1.pdf)



**USAID ARMENIA, SOCIAL PROTECTION SYSTEMS  
STRENGTHENING PROJECT**

**ԱՄՆ ԱԶԳ ԴԱՅՈՒՍՏԱՆ, ՍՈՑԻԱԼԱԿԱՆ ԴԱՇՏՊԱՆՈՒԹՅԱՆ  
ԴԱՄԱԿԱՐԳԵՐԻ ԴՅՈՐԱՑՄԱՆ ԾՐԱԳԻՐ**

**Appendix A. LIST OF LEGAL ACTS IN the SOCIAL SPHERE**

Prepared by Arsen Manukyan

**A.1 Laws**

<b>N</b>	<b>Title of Law</b>	<b>Number of Law</b>	<b>Adopted by National Assembly</b>	<b>Approved by President</b>	<b>Entered into force</b>	<b>Other remarks</b>
1	On assignment of Pensions for long term service	RA Law-43	5-Mar-96	4-Apr-96	4-Apr-96	
2	On Mandatory Social Contributions	RA Law-179	26-Dec-97	30-Dec-97	31-Dec-97	
3	On Social Security of Military Servants and Members of their Families	RA Law -258	27-Oct-98	25-Nov-98	30-Nov-98	
4	On State Pensions	RA Law -519	19-Nov-02	31-Mar-03	10-Apr-03	
5	On Social Security Cards	RA Law -1	24-Sep-03	8-Oct-03	1-Nov-03	
6	On Personal Data	RA Law -422	8-Oct-02	7-Nov-02	14-Feb-03	
7	On Mandatory Social Security in the events of temporary disability	RA Law -208	24-Oct-05	25-Nov-05	1-Jan-06	
8	On Social Protection of Disable Person		14-Apr-93			Supreme Council of Armenia
9	On Children left without Parental Care	RA Law -411	24-Sep-02	18-Oct-02	31-Oct-02	
10	On Social Assistance	RA Law -207	24-Oct-05	25-Nov-05	1-Jan-06	
11	On State Benefits	RA Law-205	24-Oct-05	25-Nov-05	1-Jan-06	
12	Labor Code	RA Law-124	9-Oct-04	14-Dec-05	21-Jun-05	

USAID Armenia-The Social Protection Systems Strengthening Project  
Implemented by TSG ■ Իրականացվում է TSG-ի կողմից

18 Bagramyan, Zarubyan Street Entrance ■ Yerevan 0009 Armenia ■ T (374 10) 542 608/9/10 ■ F 588 204 ■ www.tsginc.com  
Զառույցան փողոց ■ Երևան 0009 Հայաստան ■ Հ (374 10) 542 608/9/10 ■ Ֆ 588 204 ■ www.tsginc.com

13	On Labor Inspection	RA Law-77	24-Mar-05	19-Apr-05	7-May-05	
14	On Employment and Social Protection of Population in case on Unemployment	RA Law-206	24-Oct-05	25-Nov-05	1-Jan-06	

## ***A.2 Government Decrees***

<b>N</b>	<b>Title of Decree</b>	<b>Number of Decree</b>	<b>Adopted by Government</b>	<b>Approved by President</b>	<b>Entered into force</b>	<b>Other remarks</b>
1	On the Procedure of Formation and Expense of Social Insurance Fund's finances, and on approving SIF's statute on the Procedure of providing citizens with state social insurance benefits from SIF.	Decree N584	18-Nov-92		18-Nov-92	
2	On Establishing "Nemrut" Information-Analytical Center	Decree N664	24-Oct-00	24-Oct-00	24-Oct-00	
3	On Renaming ""Nemrut" Information-Analytical Center to "Nork"	Decree N1005	14-Aug-03	21-Aug-03	22-Aug-03	
4	On Insuring Enforcement of RA Law On "State Pensions"	Decree N793-N	May 29,2003	9-Jul-03	24-May-03	
5	On Defining Amounts for Basic and Main Pensions and Defining the Yearly Value of Insurance Record	Decree N707	13-Jun-03	19-Jun-03	10-Jul-03	
6	On Introduction of the Social Security Card System in Armenia	Decree N1783	24-Dec-03	14-Jan-04	5-Feb-04	
7	On Implementation of the Social Security Cards and Number s of Social Security Cards in Armenia	Decree N963	25-Jun-04	12-Jul-04	31-Jul-04	

8	On Providing Financial and Administrative Statistical Data related to Mandatory Social Insurance Program Implementation to the Public Administration's Body in Authority for the Social Sphere	Decree N350	18-Mar-04	March 29,2004	8-Apr-04	
9	On Approving the Procedure of Issuing and Paying Pension to Prisoners, and Recognizing the Prisoner as Disabled	Decree 1457	7-Oct-04	2-Nov-04	18-Nov-04	
10	On Approving the Procedure of Applying for Pensions, Issuing/Recalculating Pensions, Changing the Pension Type, Paying the Pension and Conducting a Pension Case /Documents/	Decree N 930	12-May-05	13-Jul-05	23-Jul-05	
11	On Activities Insuring Incorporation of Personified (Individual) Recording in the state Pension Social System	Decree N 938	12-May-05	July 13, 2005	8-Jun-05	
12	On Approving the Pension Insurance Reform Concept Paper	Decree N 796	26-May-06	17-Jun-06	29-Jun-06	
13	On Approving the Procedure of Calculating Mandatory Social Insurance Payments in Tax Authorities	Decree N 2094	24-Nov-05	14-Dec-05	1-Feb-06	
14	On Insuring Enforcement of RA Law on "Mandatory Social Security in the events of temporary disability"	Decree N 571	30-Mar-06	13-May-06	3-Jun-06	
15	On Approving Classificators for Social-Medical Examination and Standards for Defining Disability Groups	Decree N780-N	13-Jun-03	7-Jul-03	26-Jul-03	
16	On Approving the List of Child Care and Protection Institutions, Standards of Accommodating Children in those	Decree N381-N	24-Mar-05	9-Apr-05	21-Apr-05	

	Institutions					
17	On approving the Procedure of Defining State Benefit Rates and Allocation of Finances from the State Budget for Paying State Benefits,	Decree N2315-N	29-Dec-05	30-Jan-06	9-Feb-06	
18	On Approving the Procedure of Issuing and Paying Family Benefit and One-time Cash Assistance	Decree N110-N	12-Jan-06	18-Feb-06	22-Apr-06	
19	On Approving the Procedure of Implementing Social-Medical Examination	Decree N276-N	2-Mar-06	15-Mar-06	3-Apr-06	
20	On Recognizing RA Government's Decrees N1986 of September 8, 2005 and N2114 of September 15, 2005 on Approving the Procedure of Issuing Student Stipends and State Pensions in Higher Education Institutions, lapsed.	Decree N1183-N	27-Jul-06	26-Aug-06	16-Sep-06	
21	On Approving the Procedure and Conditions of Providing Temporary Accommodation (Asylum?)	Decree N614-N	April 13,2006	20-May-06	1-Jun-06	
22	On Defining the Procedure of Providing In-Kind Assistance	Decree N 958-N	22-Jun-06	14-Jul-06	5-Aug-06	
23	On Approving the Procedure of Centralized Registration (Record-keeping) of Children Left without Parental Care and Children Considered Left without Parental Care	Decree N962-N	22-Jun-06	19-Jul-06	August 03,2006	
24	On Approving the Procedure of Accommodating Children in Child Care and Protection Institutions (orphanage, boarding school)	Decree N1735-N	9-Nov-06	13-Dec-06	4-Jan-07	

25	On Approving the Procedure of Providing Care to Elderly and Disabled People and on Approving the List of Illnesses that Serve as a Ground for Declining Care to the Elderly and Disabled	Decree N1874-N	7-Dec-06	9-Jan-07	3-Feb-07	
26	On Approving the Procedure of Providing Day Care to Children	Decree N1874-N	7-Dec-06	9-Jan-07	25-Jan-07	
27	On Approving the Procedure of Licensing Organization and Provision of Care to the Elderly and Disabled, and approving the License Form	Decree N 143-N	18-Jan-07	18-Feb-07	10-Mar-07	
28	On Providing Information to the State Labor Inspectorate	Decree N 1893-N	6-Oct-05	19-Nov-05	10-Dec-05	
29	On Approving the Procedure of Presenting Quarterly Reports by Employers to the State Labor Inspectorate	Decree N 2301-N	6-Oct-05	19-Jan-06	18-Feb-06	
30	On Approving the List of Documents to be presented to State Employment Services for getting employed, getting information on vacancies, consultation of profession orientation, professional trainings, as well as for getting a status of unemployed. Also on approving the Procedure of Registering those people and taking them out of Register.	Decree N 472-N	23-Mar-06	19-Apr-06	13-May-06	
31	On Approving the Procedure of Organizing Professional Training of Unemployed People, Uncompetitive Groups in the Labor Market, as well as People who Get Pension for Long Service and with Privileges but who are employed and are looking for a job.	Decree N 533-N	30-Mar-06	3-May-06	27-May-06	

32	On Approving the Criteria for Defining the Level of Professional Ability Lost Due to Injury at Workplace, Professional Illness or other Health Damage.	Decree N 619	11-May-06	20-May-06	10-Jun-06	
33	On Defining the Procedure of Paying Burial Benefit in the Event of Death of an Unemployed Person.	Decree 798	8-Jun-06	17-Jun-06	8-Jul-06	
34	On Defining the Procedure of Registering the Employment Contract, the Form of the Register-Book, and Register-Book Keeping.	Decree N 875-N	16-Jun-06	28-Jun-06	22-Jul-06	
35	On Defining the Service Record Book Form, how to Keep this Book and Provide a Copy.	Decree N 876-N	16-Jun-06	28-Jun-06	13-Jul-06	

### ***A.3. Other legal acts***

<b>N</b>	<b>Title of Legal act</b>	<b>Number of Legal act</b>	<b>Adopted by...</b>	<b>When...</b>	<b>Entered into force</b>	
1	On Approving the Charter of the State Social Insurance Fund	Decree N497	Prime Minister of Armenia	2-Aug-04	3-Aug-04	
2	On Approving SIF's head administration's structure	Decree N902	Prime Minister of Armenia	30-Dec-04	31-Dec-04	

3	On Approving the Procedures of Applying for Individual Accounts and Filling in the Individual Reports, as well as forming and Using the database of Individual/personified Record-keeping for individuals involved in the state pension insurance system, on approving the required documents (decision on opening an individual account, decision on declining registration, inquiries for checking information, document on insurance service, application from the insured person on getting extract reports from the individual account, extract report from the individual account, cover page, check-list)	State Registration Number 11505381	Minister of Labor and Social Issues SIF President	8-Sep-05	7-Oct-05	
4	Order on “Approving the Procedure of Providing State Budget Funds to NGOs as Grants”	NK-87	RA President	13-May-05	28-May-05	
5	Precept on “Recognizing an NGO as a Partner”	NK-5	RA President	10-Jan-07	11-Jan-07	Since 2005, “Social Dialogue and Trends Center” NGO is recognized a partner NGO which is entitled to conduct tenders for grants.
6	On Approving the List of Activities Ensuring Enforcement of the RA Law on Social Protection in the case of Population’s employment and unemployment	Decree N 26	Prime Minister of Armenia	17-Jun-06	18-Jan-06	



**USAID**  
FROM THE AMERICAN PEOPLE

## USAID ARMENIA, SOCIAL PROTECTION SYSTEMS STRENGTHENING PROJECT

ԱՄՆ ՄՁԳ ՀԱՅԱՍՏԱՆ, ՍՈՑԻԱԼԱԿԱՆ ՊԱՇՏՊԱՆՈՒԹՅԱՆ  
ՀԱՄԱԿԱՐԳԵՐԻ ՀՁՈՐԱՑՄԱՆ ԾՐԱԳԻՐ

### Appendix B. Best practices of e-Government

The four types of e-government services are Government-to-Citizen (G2C), Government-to-Business (G2B), Government-to-Employee (G2E), and Government-to-Government (G2G).

**G2C** includes information dissemination to the public, basic citizen services such as license renewals, ordering of birth/death/marriage certificates and filing of income taxes, as well as citizen assistance for such basic services as education, health care, hospital information, libraries, and the like.

**G2B** transactions include various services exchanged between government and the business community, including dissemination of policies, memos, rules and regulations. Business services offered include obtaining current business information, downloading application forms, renewing licenses, registering businesses, obtaining permits, and payment of taxes.

**G2E** services encompass G2C services as well as specialized services that cover only government employees, such as the provision of human resource training and development that improve the bureaucracy's day-to-day functions and dealings with citizens.

**G2G** services take place at two levels: at the local or domestic level and at the international level. G2G services are transactions between the central/national and local governments, and between department-level and attached agencies and bureaus. At the same time, G2G services are transactions between governments, and can be used as an instrument of international relations and diplomacy.

There are a lot of excellent sources of information about best practices of e-Government.

#### USA

According to the UN E-government Readiness rankings in 2005 [1], the United States is the world leader in e-government readiness as well as in the web measure index.

The Official Web Site of the President's E-Government Initiative is:

<http://www.whitehouse.gov/omb/egov/index.html>.

The strength of America's online presence is essentially twofold. First, it provides the enormously useful web portal <http://www.firstgov.gov>, which provides enormous amounts of information in one place. The second strength and the cornerstone of the United States' approach to e-government is the reliance on integrated portals, which collect and consolidate information in one place thereby increasing the effectiveness of finding topic-specific information for citizens in an efficient manner.

Noteworthy examples include the portal for federal government forms, <http://www.forms.gov>, payments to the government, <http://www.pay.gov>, and commenting on federal regulations, <http://www.regulations.gov>. The FirstGov site provides

a convenient listing of cross-agency portals “that bring together federal information and services from multiple agencies about a particular topic or for a particular customer group” at [http://www.firstgov.gov/Topics/Cross\\_Agency\\_Portals.shtml](http://www.firstgov.gov/Topics/Cross_Agency_Portals.shtml). Added to all this is the incredible amount of information available all of which lends itself to making United States the undisputed world leader in e-government.

US Office of Electronic Government and Technology develops, coordinates, and defines ways that electronic and information technology business strategies can assist Federal agencies to enhance access and delivery of information and services to citizens, business partners, employees, agencies, and government entities. Their WEB site <http://www.estrategy.gov> contains plenty of valuable information and good practices. In particular, it states main principles for E-Government:

- E-government enables everyone in Government to strive to: Deliver customer-centric services rather than stove-piped Agency-centric processes
- Demand interoperability across government and with industry partners.
- Provide common access to Government services and information via government-wide portals that are organized around the needs of communities of customers.
- Build strong privacy protection, confidentiality, and trust.
- Adopt commercial products, practices, and standards.
- Foster strong interagency, inter-organizational, and cross sector leadership to promote the sharing of information and leading practices.
- Re-engineer paper-based processes to produce results that will dramatically improve service and responsiveness while reducing costs.

In February 2007, the Office of Management and Budget submitted to Congress the second annual “Report to Congress on the Benefits of the E-Government Initiatives” [11]. The report outlines the purpose of these Initiatives and highlights the benefits agencies receive from the initiatives to which they provide funding contributions. Also included are details regarding initiative funding by agency/bureau.

Selected examples of how citizens and Federal employees are benefiting through the use of the Presidential E-Government Initiatives include:

- **GovBenefits.gov** - Currently, GovBenefits.gov is receiving approximately 300,000 visits per month by citizens and, and to date has provided nearly 1 million citizen referrals to benefit programs. GovBenefits.gov provides a single point of access for citizens to locate information and determine potential eligibility for government benefits and services.
- **Grants.gov** - Grants.gov has seen a substantial increase in the number of grant application packages posted on Grants.gov since the beginning of fiscal year 2005 (FY05). In the first quarter of FY05, 252 packages were posted on Grants.gov. By the last quarter of fiscal year 2006 (FY06), 4,523 packages were posted on Grants.gov, almost 17 times the number at the beginning of FY05.
- **Recruitment One-Stop** - Each month, over 100,000 resumes are created on USAJobs.gov, the Federal online recruitment service. USAJobs.gov receives over

240,000 visits daily from job seekers looking for information regarding career opportunities with the Federal government.

Another valuable source of good practices is EU eGovernment Practice portal (<http://www.epractice.eu>) provides access to information and practice exchange on eGovernment throughout Europe. It maintains a series of Factsheets presenting the situation and progress of eGovernment in 32 European countries: EU-27, Croatia, Turkey, Iceland, Liechtenstein and Norway, providing for each one of them a wide and consistent range of information:

- Country Profile (basic data and Information Society indicators);
- History (major past eGovernment developments and milestones);
- Strategy (vision, objectives and principles supporting the eGovernment drive);
- Legal Framework (main legal texts impacting on the development of eGovernment);
- Actors (key organizations involved in the eGovernment drive);
- 'Who's Who' (main decision-makers and executives steering and shaping the move to eGovernment);
- Infrastructure (key components of the nationwide eGovernment infrastructure);
- eServices for citizens and for businesses (online availability and sophistication of services for citizens and businesses, based on the eEurope common list of basic public services).

A "**National Progress Report on eGovernment in the EU27+**" [10], was presented at the Ministerial eGovernment Conference on September 19, 2007 in Lisbon. A meeting attended by 22 eGovernment Ministers reviewed progress made on implementing eGovernment Services since the launch of the European Commission's i2010 initiative for Growth and Jobs (2005), the Manchester Ministerial Declaration (2005) and the i2010 eGovernment Action Plan agreed by Council in June 2006.

The most inspiring recent good practices have received the **2007 European eGovernment Award** (<http://www.epractice.eu/document/3596>).

Some information about these European good practices is presented below.

## **Denmark**

One of the most useful sites in the Danish online presence is the "**net-citizen**" portal, <http://www.netborger.dk>, which is a shortcut guide to public self-services at all levels of government involving everything from school and family to work, pensions and taxes. It is also a model for how a public-private partnership can combine its services to the benefit of citizens. A list of partners as well as more information can be found starting at <http://www.netborger.dk/linkpartnere.asp>.

Like other leading e-government countries, Denmark has established an office for cooperation and standardization for using IT in the public sector. The OIO - Offentlig Information Online (public information online) portal, <http://www.oio.dk>, offers information, knowledge and access to tools while primarily targeting public sector employees who deal with e-government and the implementation of IT in the public sector. Of related interest is

“the public” search site, <http://www.detoffentlige.dk>, which claims to search all three million government web pages.

**CSD - Compensation for Sickness in Denmark.** The stated objective of the CSD is to relieve Danish companies from administrative burdens and to provide them better services. According to law Danish companies can apply for economic compensation when an employee of the companies is absent from work due to illness or childbirth. The paper-based compensation workflow is very time-consuming for both the companies and the local authorities. Therefore the Danish governmental and local authorities decided to provide an ICT solution that would permit effective online applications in a secure and legally binding way and provide at better service for the companies. As a result the companies have experienced significant reductions of their administrative burdens through time savings of 30 - 40 percent. The digital solution is based on advanced ITC-technology using standardized OIO-XML schemas, which increases the interoperability and facilitates re-use of data among authorities and private organizations. A more efficient administration result in savings of an estimated 13 to 25 million Euros.

## ***United Kingdom***

Overall, much like the United States, the United Kingdom’s individual sites consolidate enormous amounts of information and are incredibly useful. The new look entry portal, <http://www.direct.gov.uk>, illustrates this strength. Readily accessible, the national site enables users to browse its offerings by audience, topic, or jump right into the “Do it online” section. Equally impressive are the numerous portals, such as the Government Gateway, <http://www.gateway.gov.uk>, which is the central registration service for e-government services in the United Kingdom.

**DirectGov** is the British Government's flagship digital service project. Its complete implementation will amalgamate all online public services by 2011. It entails closing more than 550 government sites and resurfacing the information they currently offer in just one digital platform. That platform offers a point of entry for citizens to all key government services, information, tools and transactions through Digital TV, Mobile and Web. Its implementation costs exceed five million Euros a year.

Another cutting-edge collaborative initiative is the info4local project, <http://www.info4local.gov.uk>, which, as the header clearly notes, provides “information for local government from central government.” Specifically, six departments, with the Office of the Deputy Prime Minister in the lead, provide local authorities with quick and easy access to useful information from more than 65 government departments, agencies and public bodies.

The Transforming Access to Services in Local Government (**TATS**) project enables citizens and businesses to access Newport City Council's services through a multi-channel and integrated technology platform. TATS has been set up on the basis of sophisticated IT systems that enable integration of front and back office services. 137,000 citizens and 4,000 businesses benefit from an initiative based on telephone, face to face online interaction. Its implementation has been estimated at five million Euros.

**ePetitions** enables citizens to create and sign petitions on the Prime Minister's own site and expect to receive a response direct from government addressing those specific issues and spelling out what action the government intends to take. To date over 8,000 petitions have

been launched and four million signatures have been collected thanks to this initiative. The project has been developed with a 300,000 Euros budget.

**e@ SY** provides citizen and business interactive services via different cost-effective channels, such as digital television, mobile telephones, kiosks, gaming stations and the Internet. The initiative works on the basis of a new generic replicable interface used not only the UK but also in other EU member states. The project is meant to reduce the demand on providers of the service, a partnership of public, private and voluntary sector providers. Its cost is around 300,000 Euros.

### **Norway**

**Mypage** is a user-defined and secured citizen's portal where users can carry out personalized public electronic services in one place. The citizens can also control the information held by various public administrations, improving transparency, data quality, and service. The goal is that all relevant services from all level of the administration will be available through Mypage by end 2009. Its implementation has been estimated at five million Euros.

### **Netherlands**

**DigiD** is a system used by 220 local, regional and national administrations in Netherlands. It permits the digital authentication of citizens and business applying for electronic services. Over 5.7 million people have the DigiD login code, a single number that can be used to access to several electronic applications. The Tax Administration was the first to use the DigiD.

### **Belgium**

The Crossroads Bank for Social Security and the National Office for Social Security launched a joint project to improve collaboration and digital data exchange between more than 2000 social security institutions in Belgium<sup>47</sup>. The network encompasses private companies and public administrations which can consult their databases and exchange up to 190 different types of electronic messages securely. The aim of the project was to effectively combine back office integration and an ePortal solution to provide improved services to citizens, companies and public institutions. The Belgian Social Security case has a strong and visible impact. The service clearly meets social and economic needs and provides benefits to a significant portion of businesses and citizens. It also has a pan-European dimension. It has cross-border scope and could easily be transferred easily to other countries or service domains.

The **LoG-IN** Generic Information Infrastructure (GII) is a powerful infrastructure owned by 35 local authorities from the UK, Germany and Belgium. It allows the local governments to make their information available to several digital channels: online services, mobile, Google Maps, Google Explorer, etc. The GII led to a saving of over 1.5 million Euros.

**My File.** Belgium citizens can check online all data related to the National Register, such as the birth certificate, family composition, civic state, etc. This instrument permits not only to consult information but also to download or transmit documents. This way, the National Register documents can be used for official business without using any paper support. To

access to My File contents, the user must have an eID card, with an authentication certificate and a pin code.

## ***Estonia***

The 'Estonian Information Society Strategy 2013' [12] became effective on 1 January 2007. The strategy is conceived as a sectorial development plan, setting out the general framework, objectives and respective action fields for the broad use of ICT in the development of knowledge-based society and economy in Estonia for the period 2007-2013. The plan focuses on the use of IT to improve quality of life and increase citizen involvement in public life. The new proposal is a continuation of the two previous Information Society Development Plans adopted in 1998 and 2004.

A significant result of Estonia's Information Society development policy is the achievement of the largest functioning public key infrastructure in Europe, based on the use of electronic certificates maintained on the national ID card and allowing to considerably improve the security and functionality of IT solutions. Up to 90 % of the population possesses the ID card that enables both electronic authentication and digital signing. Relevant legislation is in place, giving the digital signature equal power with the handwritten one, and imposing a responsibility on public authorities to accept digitally signed documents.

Moreover, the eagerness of Estonians to use innovative solutions (wide take-up of IT solutions provided by the Tax and Customs Board, Internet banking, m-parking, eVoting etc) highly contributed to such result.

**ID CARD.** The purpose of Estonian ID-program is to use nation-wide electronic identity and develop a new personal identification card that would be a generally acceptable identification document and contain both visually and electronically accessible information. On 28 January 2002 the first ID-cards were issued to Estonian citizens. By October 2006 the number of ID cards issued in Estonia has exceeded 1 million. Nearly 90 % of the Estonian population between ages 15 and 74 now has a valid ID card.

In general, people have accepted the card very well and it is being used on a daily basis. The convenient format of the card and the fact that the electronic chip included in the ID also enables a number of additional functions, have definitely played a role.

The implementation of ID-card actually means establishing new nation-wide infrastructure in Estonia. The structure includes certification service provider (certification centre and its subunits), who issues certificates, and catalogue service provider, who takes care of making these certificates available for everyone. In addition, other services and their providers are needed which would provide the opportunity to use certificates. Pursuant to the Estonian Digital Signatures Act, the structure must include also time stamp service provider who would issue time stamps for digital signatures.

The **e-Citizen** project is a nation-wide project that focuses on developing cooperation between Estonian citizens and the public sector through the Internet. In the course of the project the e-citizen environment is created, which enables the citizen to conveniently obtain information about services provided by the state and the citizen's rights and obligations. It enables people to participate more actively in the public life at national, regional and local

level and to communicate with all national information systems through their personal information system.

**X-Road** is the modernization program of national databases with the aim to change national databases into a common public, service-rendering resource, which would enable agencies, legal and natural persons to search data from national databases over the Internet, provided they are entitled to do so. At the same time, the system will ensure sufficient security for the treatment of inquiries made to databases and responses received.

The aim of the X-road program is to develop software, hardware and organizational methods for standardized usage of national databases.

**iVote** allows Estonians to cast their vote in elections and referendums through the Internet. Its main aim is to widen accessibility and increase participation. According to its promoters, the uniqueness of the case lies, partially at least, in a technical solution: using a nationwide remote authentication system based on digital signatures and electronic ID cards. iVote implementation costs have been valued at 300,000 Euros.

## ***Malta***

In Malta, citizens can access their personal social security records and payments via the internet, and may also opt to be notified about their social security payments via SMS rather than receiving printed payment advice by post. However, the most salient initiative is the introduction of eGovernment Agents that act as intermediaries to those without access.

## ***Spain***

In Spain, **060** is the magic code providing a single access point. Many services provided by different administrations can be accessed via the 060 network, whether they are office-, internet-, or phone-based. Citizens can access these points in the street or their office on the web ([www.060.es](http://www.060.es)), by the phone (060) or SMS. The network is available 24/7 and coordinates the services offered by national, regional and local administrations. The goal of 060 is to offer these services without moving from one office to another and not needing to know

## ***France***

Online Forms. The [www.administration24h24.gouv.fr](http://www.administration24h24.gouv.fr) website was designed to enable French citizens easy access to as many public services as possible at any time, from wherever they wish, and via a single entry point. This portal is complemented by the Online Forms website, which provides an Internet version of forms approved by the authorities, accessible via Internet. The forms can be filled in and sent online to the processing services. Its implementation costs are five million Euros.

## ***Italy***

**VASSI** is an interactive system that the Italian National Social Security Institute has put in place on its web portal to extend its efforts for a more effective way of communicating with citizens regarding pension schemes, social allowances and indemnities for citizens and

immigrants living in Italy. To date it offers multi-channel services via web and mobile phone; in future it will be also available on television. Its implementation costs are five million Euros.

## Appendix C. What is else beyond strategy?

There are a lot of other important issues to consider for Information and ICT policy development. The most critical are the following ICT management pillars:

### Maturing IT Infrastructure Management

- SLA, ITIL

### Maturing IT Development Management:

- ISO/IEC 12207 - Software life cycle processes
- SEI CMM, CMMI
- BSI TickIT

### Maturing IT Security Management

- ISO/IEC 27002 (17799)

## ***Maturing IT Infrastructure Management***

First step is to move up IT management to Service level agreements (SLAs). For example, basic SLA for email infrastructure may include the following agreements:

- Local network logon time: 5 seconds or less
- Availability of email during business hours: 99.999% (approx 1 hour of downtime during business hours per month)
- Minimum notice for schedule maintenance: 5 business days
- Recoverability: No more than 6 hours' data loss in the event of total failure
- Time for new mailboxes to be added (once requested): 1 business day or less
- Response time to user notification of mail system failure: 1 hour or less

How can you meet these promises? Monitoring, planning, and forecasting.

As a basis for development of IT Management Policies, due to lack of International standards, it is recommended to use ITIL (Information Technology Infrastructure Library), collection of IT-related best practices developed and maintained by the UK OGC (Office of Government and Commerce).

### Example of top 10 IT Manageability Policies

The following list highlights the top 10 policy directives:

- Ensure that the health of all critical systems is monitored constantly.
- Where possible, provide automated corrective actions for common problems.
- Ensure that security auditing is automated and includes alerts for problem conditions.
- Provide monthly capacity reports for all critical systems.
- Where possible, consolidate underutilized systems to improve efficiency.
- Extend systems capability when existing systems reach 90 percent utilization or more.

- Maintain a 10 to 15 percent level of general underutilization to provide extra capacity to react to new business opportunities.
- Reduce administrative time spent on handling unexpected problems and conditions by 50 percent or more.
- Define and meet SLAs for general system availability for all critical systems.
- Define and meet SLAs for system response times for all critical systems and applications.

## ***Maturing IT Development Management***

**Information Systems/Software remains the most inefficient and unpredictable area within IT.**



*Figure 1: Common Problems in Software Development*

To overcome these problems International standards for **Software life cycle processes** were developed: **ISO/IEC 12207** that provides a complete set of processes for acquiring and supplying software products and services.

This standard is a solid base for corporate standards and includes a set of processes:

**PRIMARY:** Acquisition, Supply, Development, Operation, and Maintenance Processes.

**SUPPORTING:** Documentation, Configuration Management, Quality Assurance, Verification, Validation, Joint Review, Audit, and Problem Resolution Processes.

**ORGANIZATIONAL:** Management, Infrastructure, Improvement, and Training Processes.

In particular, the **development process** consists of the following activities along with their specific tasks: Process implementation; **System requirements analysis**; **System design**; Software requirements analysis; Software architectural design; Software detailed design; Software coding and testing; Software integration; Software qualification testing; **System integration**; **System qualification testing**; **Software installation**; and **Software acceptance** and support.

**TAILORING PROCESS.** Tailoring is deletion of non-applicable or in-effective processes, activities, and tasks. A process, an activity, or a task, that is not contained in the standard but is pertinent to a project, may be included in the agreement or contract. The standard requires that all the parties that will be affected by the application of the standard be included in the tailoring decisions. It should be noted that this process itself, however, cannot be tailored.

## ***Maturing IT Security Management***

### ***Information and IT Security - Data Protection***

**ISO/IEC 27002:2005 (17799)** Information technology. Security techniques.  
Code of practice for information security management.

A complete set of guidelines and principles for an effective **MIS and information security policy**.

Recognized and adopted by industry professionals worldwide, this universal code of practice provides a complete set of **guidelines and principles** for an effective information security management system (ISMS) and information security policy.

This standard takes into account changes in technology, **working practices and security techniques** which will enable organizations to develop, implement and measure effective security management practice.