

# **CAMBODIA DIGITAL SOCIAL PROTECTION PLATFORM VERSION 1.0 AND SOCIAL PROTECTION REGISTRY**

Including: User Experiences, ID Ecosystem  
Overview & Technical Assessment

Assessment of the Early Rollout



**WORLD BANK GROUP**



## Acknowledgements

This assessment was prepared by Darlin Nay, Claire Casher, and Robert Palacios of the World Bank, with biometric technical analysis by Chris Allgrove and legal analysis by Prakhar Bhardwaj and Nay Constantine, also of the World Bank. The authors are grateful to H.E. Samedy Yok, Mr. Lay Veasna Chhut, Mr. Pichponreay Ly, and their team at the General Secretariat of the National Social Protection Council (GS-NSPC) for their collaboration on this evaluation and their facilitation of in-depth field visits. The authors are also grateful to all the individuals who shared their perspectives in interviews, focus group discussions, and the consultation workshop—they are too numerous to name, but their organizations are listed in Appendix 1.

This assessment was made possible by the World Bank's Identification for Development (ID4D) Initiative and Multi-Donor Trust Fund, which is supported by the Gates Foundation, the UK Government, the French Government, the Australian Government, the Norwegian Agency for Development Cooperation, and the Omidyar Network. To find out more about ID4D, visit [id4d.worldbank.org](https://id4d.worldbank.org).

The authors are not qualified to practice law in Cambodia. Accordingly, nothing in these comments constitutes legal advice and no inference should be drawn as to the completeness, adequacy, accuracy or suitability of these comments from the perspective of the laws of or legal practice in Cambodia.

## Contents

<b>Acknowledgements.....</b>	<b>2</b>
<b>Abbreviations.....</b>	<b>5</b>
<b>Introduction.....</b>	<b>6</b>
Harmonization Initiatives .....	10
Harmonization Progress.....	12
<b>About this Assessment.....</b>	<b>14</b>
Objectives .....	14
Methodology .....	15
Analysis .....	17
<b>Part 1: User Experiences with DSPP &amp; SR.....</b>	<b>18</b>
Beneficiary Enrolment (DSPP) .....	18
Field Visit Findings .....	18
Responses from Beneficiaries .....	27
Key Informant Interview Findings.....	28
Beneficiary Management (SR).....	30
Key Informant Interview Findings.....	30
Part 1 Recommendations.....	33
<b>Part 2: Cambodia’s ID Ecosystem: Overview &amp; Technical Assessment.....</b>	<b>37</b>
Introduction .....	37
Cambodia’s Foundational IDs .....	37
Civil Registration and Vital Statistics .....	37
The Khmer ID .....	38
Functional IDs for Social Protection Programs.....	40
The IDPoor based Equity Card .....	40
National Social Security Fund Member Card.....	42
Cambodia’s Person with Disability (PWD) Card .....	43
The Social Protection ID Initiative .....	44
Objectives of the New System.....	44
NSPC system architecture.....	46
Biometric capture process and use .....	47
The NSPC Biometric System .....	49
Biometric Performance.....	52

Part 2 Recommendations .....	53
<b>Part 3: Legal &amp; Regulatory Framework Assessment .....</b>	<b>60</b>
I. Introduction .....	60
II. Overview of Best Practices for Regulation of Digital IDs .....	60
III. Analysis of Legal and Regulatory Safeguards in Cambodia’s Digital ID Systems .....	63
IV. Analysis of Legal and Regulatory Safeguards in the Harmonization Sub-Decree .....	65
V. Part 3 Recommendations .....	68
<b>References .....</b>	<b>70</b>
<b>Appendix 1: Sampling Details .....</b>	<b>74</b>
<b>Appendix 2: Survey Data .....</b>	<b>76</b>
<b>Appendix 3: Note on Impact Evaluation .....</b>	<b>78</b>
<b>Appendix 4: Consolidated Recommendations (Parts 1-3) .....</b>	<b>80</b>
Part 1: User Experience with DSPP & SR .....	80
Part 2: Cambodia’s ID Ecosystem .....	80
Part 3: Legal & Regulatory Framework .....	81

## Abbreviations

API	Application Programming Interface
CamDX	Cambodia Data Exchange
CRM	Customer Relationship Management
CRVS	Civil Registration and Vital Statistics
DGC	Digital Government Committee
DMIS	Disability Management Information System
DPI	Digital Public Infrastructure
DPIA	Data Protection Impact Assessment
DSPP	Digital Social Protection Platform
FGD	Focus Group Discussion
GDI	General Department of Identification
GS-NSPC	General Secretariat of the National Social Protection Council
H-SPIS	Health-Social Protection Information System
IPIS	Integrated Population Identification System
IDEEA	ID Enabling Environment Assessment
IDPoor	Ministry of Planning's Identification of Poor Household Mechanism
KII	Key Informant Interview
MOI	Ministry of Interior
MOP	Ministry of Planning
MOSVY	Ministry of Social Affairs, Veterans and Youth Rehabilitation
MPTC	Ministry of Post and Telecommunications
NPCA	National Payment Certification Agency
NSAF	National Social Assistance Fund
NSCI	National Steering Committee on Civil Registration, Vital Statistics and Identification
NSPC	National Social Protection Council
NSPI	National Strategic Plan on Identification 2017-2026
NSSF	National Social Security Fund
OS	Operating System
PMRS	Patient Management and Registration System
PWD	Person With Disabilities
PW-CTP	Cash Transfer Program for Pregnant Women
RCT	Randomized Controlled Trial
SOP	Standard Operating Procedure
SPID	Social Protection Identifier
SR	Social Registry
SRSP	Shock Responsive Social Protection
UID	Unique Identifier

# Introduction

**Social protection in Cambodia is recognized as a critical mechanism for reducing poverty, enhancing human capital, and promoting social inclusion.** National social protection in Cambodia is structured around two core pillars: social assistance programs and social security schemes. Social assistance programs, funded directly by the national budget, primarily target low-income households identified by the Ministry of Planning's Identification of Poor Household Mechanism (IDPoor) and other vulnerable populations who hold an Equity Card.<sup>1</sup> Social security schemes operate as social insurance mechanisms funded by mandatory and voluntary contributions from formal and informal sector participants, providing essential income security and protection against life-cycle risks.

**Cambodia's commitment to enhancing social protection has been notably evident during recent crises.** The COVID-19 pandemic posed severe socioeconomic challenges, prompting the Royal Government to introduce targeted interventions, such as the Cash Transfer Program for Poor and Vulnerable Households during COVID-19 and the Post-Lockdown Cash Transfer Program. Building upon this experience, the government recognized the critical need for enhancing preparedness and responsiveness to future shocks—including those related to climate change, natural disasters, macroeconomic instability, and public health emergencies. Consequently, the Guideline on Shock Responsive Social Protection (SRSP) was established, providing a structured, predictable, and timely mechanism to assist vulnerable groups both during and after crisis periods.

**Parallel to this, Cambodia has prioritized building a comprehensive and integrated social protection system, particularly through its National Social Assistance Programs within the Family Package.** Administered by the National Social Assistance Fund (NSAF), the Family Package integrates multiple cash transfer programs into a single social assistance framework. The initiative currently provides base benefits to Equity Card holders, as well as financial support under the social assistance programs it consolidated, including the Cash Transfer Program for Pregnant Women and Children Under 2 Years of Age, the Scholarship Program for Primary and Secondary School Students, the Cash Transfer Program for Persons with Disabilities, and the Cash Transfer Program for the Elderly (60 years and above), along with incentives for individuals living with HIV/AIDS.

**Cambodia has demonstrated growing interest in digitalizing its social protection system, underpinned by strong political commitment from the Royal Government to accelerate both digital transformation and the expansion of social protection.** This momentum builds on earlier successes, particularly the digital transformation of the IDPoor system, which introduced an Application Programming Interface (API) layer that enabled interoperability and data exchange between the IDPoor database and other stakeholders within Cambodia's social protection ecosystem. The transition from rounds-based to an on-demand, digital system for identifying poor

---

<sup>1</sup> The Equity Card is a credential issued by IDPoor that outlines a household's composition and economic status details. It is used as proof of eligibility for various social programs.

households marked a significant milestone, embedding digital solutions into social protection processes and contributing to a substantial increase in IDPoor registrations<sup>2</sup>.

**This progress has been accompanied by substantial infrastructure investments.** While social protection programs are often managed on a national level, the enrolment processes are decentralized to the commune/sangkat level. For over four years, commune/sangkat offices have Android tablets to use for social program enrolment (a total of 3,500 tablets were distributed nationally in 2019, with extensive training delivered on their use). A device management system enables remote instantaneous updates to all of the tablets. Also, an interministerial agreement ensures that internet connection is included in commune/sangkat budgets. In under 10% of communes/sangkats nationally there is no internet coverage available, but for the rest where connectivity does exist a connection is available at minimum in the commune/sangkat office. With the availability of internet connection and devices (both the provided tablets and the increasing prevalence of personally-owned smartphones), more social programs have developed digital solutions and provided extensive training programs to their commune/sangkat focal points.<sup>3</sup>



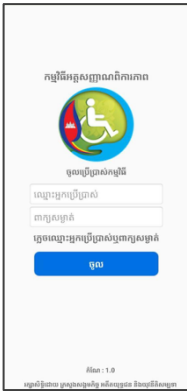
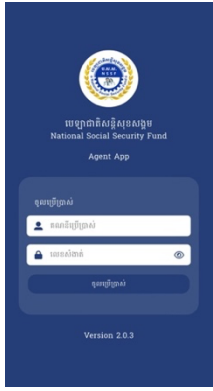
**Nonetheless, Cambodia's social protection system continues to face persistent challenges, with fragmentation and a lack of interoperability standing out in the context of this evaluation.** Social assistance programs often operate in isolation, with each program relying on its own registration platform or application, separate sets of questions, distinct data formats, and program-specific standard operating procedures. These approaches have resulted in disjointed databases that are unable to communicate with one another, limiting potential for deduplication and beneficiary tracking across programs. Other contributing factors include a lack of coordination among development partners that generally support the development of stand-alone systems with differing architectures, as well as weak familiarity with national IT policies and the tendency to favor self-developed applications among the IT personnels of relevant ministries and operators. With multiple programs now being integrated under the Family Package umbrella, the continued use of separate registration systems is not only inefficient but fundamentally contradicts efforts to consolidate social assistance programs. Figure 1 shows the range of social protection applications currently in use for beneficiary enrolment and management.

**Figure 1: Status Quo beneficiary enrolment and management processes**

System	IDPoor	Family Package	Disability Services	Social Security
<b>Beneficiary Enrolment</b>				
<b>Administrator</b>	Commune/Sangkat Working Group (SCWG) for IDPoor (+Commune Sangkat Council Meeting/Chief for approval step)	Commune/Sangkat Focal Point (FP) for Family Package (+Chief for approval step)	Commune/Sangkat Focal Point (FP) for persons with disabilities (PWD)	NSSF officer

<sup>2</sup> For more details on the progress of Cambodia's efforts in digitalizing its social protection, see GiZ 2024.

<sup>3</sup> Each program has a focal point in each commune/sangkat office; one official may be the focal point for multiple programs or the duties may be divided amongst multiple officials.

<b>User Interface</b>				
<b>Enrolment Procedure</b>	<p>Households self-identify or are identified through assistance by local authority/other stakeholders (in-person or via public IDPoor app). CSWG conducts an interview with them and enters the data into the app live during the interview.</p> <p>Enrolment final after Commune/ Sangkat Council validation.</p>	<p>FP identifies an eligible beneficiary OR beneficiary self-identifies. FP enrolls them by entering their data into the app.</p> <p>May be done at Commune/ Sangkat office or household.</p> <p>Enrolment final after Chief approval, data verification by central team.</p>	<p>FP identifies a PWD, conducts an interview with them and enters the data into the app live during the interview.</p> <p>May be done at Commune/ Sangkat office or household.</p> <p>Enrolment final when data is verified by central team.</p>	<p>Employers/Owner of Establishments/ Contractors must register their regular and casual workers with the NSSF. Once the NSSF verify the identity and the employment certificate issued by the employer, the beneficiaries will be asked to go to a NSSF branch to provide their biometrics and collect their membership card.</p> <p>The registration is mainly done online, via the web portal, computer application, or mobile app. The biometrics are collected at the NSSF branch.</p>
<b>Proof of Identity and Uniqueness during Enrolment</b>	No	No	No	Yes



<b>Equipment Used</b>	Commune/ Sangkat tablet	Commune/ Sangkat tablet	FP's own smartphone, usually	Registration: Employer's own smartphone/ computer  Biometrics Collection: Computer and devices at the NSSF branch
<b>Beneficiary Management</b>				
<b>Data Storage</b>	IDPoor Database	NSAF Database	DDW Database	NSSF Database
<b>Unique Identifier for Beneficiaries</b>	14 Digits Equity Card Number (Before), 10 Digits Equity Card Number (Present)	None	PWD Card Number	Beneficiary ID

**The absence of comprehensive data protection legislation exacerbates the challenges posed by different digital ID systems.** ID systems should be underpinned by legal frameworks that safeguard individual data, privacy, and user rights. Many countries have adopted general data protection and privacy laws that apply not only to the ID system, but to other government or private-sector activities that involve the processing of personal data (World Bank 2019). In accordance with international best practices, these laws typically provide for fundamental data protection principles, such as purpose limitation, and data minimization, a set of user rights to correct, access and request deletion of personal data, and independent monitoring and enforcement (World Bank 2017). While efforts have been made to address these gaps by supporting key institutions, including the GS-NSPC, in the development of policy frameworks on interoperability, information security and cybersecurity, and privacy protection, Cambodia still lacks a cross-sectoral data protection legislation, which means that, different digital ID systems have varying levels of privacy protection, user rights, and options for recourse in case of a data breach.

**Various digital ID programs are governed by their own policies and decrees that are enforced by different ministries.** Significant policies, in chronological order, include:

- (a) The Sub-Decree No. 252 on the Management, Use, and Protection of Identification Data, 2021 (Sub-Decree No. 252, 2021) governs personal identification data managed by the Ministry of Interior but does not extend to identification data held by other entities;
- (b) Cambodia's poverty identification system, IDPoor, which is governed by the Data Protection Policy (2022) published on its website; and
- (c) In July 2023, Cambodia enacted a landmark Law on Civil Registration, Vital Statistics and Identification (CRVS-ID Law, 2023), guaranteeing 'a legal identity for all, which is essential to accessing education, health care, property, and many other benefits and social protections'.

For a detailed legal and regulatory analysis of regulations governing Cambodia's digital ID systems see **Appendix 3**.

**Moreover, the fragmented approach places an undue burden on beneficiaries, who are required to bring or produce identification documents that they may not possess.** This constraint poses a real risk of exclusion or delays in accessing benefits, especially for those most in need. Hence, there is also a need to explore and study how technologies, including biometrics, can be used to provide more convenience in verifying beneficiaries' identity without the need for them to bring along identification documents.

**Compounding these challenges is the absence of an integrated social protection registry**—a centralized database that compiles information on poor and vulnerable households, their socioeconomic status, and the programs with which they are registered. Currently, social assistance programs assign different beneficiary IDs without the ability to cross-reference or trace whether individuals are enrolled in multiple programs or if other members of their household may qualify for additional support (e.g., elderly persons or persons with disabilities).

**Acknowledging these critical issues, and in alignment with the ongoing digital transformation agenda, the Royal Government has put forward the Digital Transformation Strategic Plan in Social Protection 2024–2028 and has placed particular emphasis on the harmonization of registration systems and data management across various social protection initiatives.**

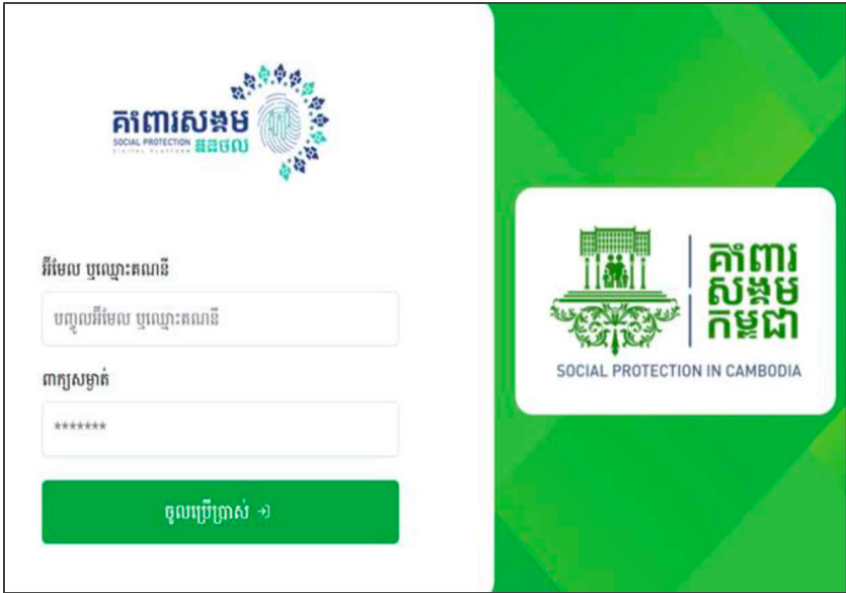
## Harmonization Initiatives

**The harmonization effort was launched to integrate and streamline registration processes, improve data accuracy, and enhance service delivery efficiency.** It comprises two core elements: the Social Registry (SR) and the Digital Social Protection Platform (DSPP). These are governed by Sub-Decree No. 38 on Harmonization of the Social Protection Registration System and Data Management, 2024 (Harmonization Sub-Decree) which establishes a legal framework for the integration and management of social protection data systems and identifies the National Social Protection Council (NSPC) as the entity leading and managing them.

**The SR functions as an 'integrated registration database' that links the beneficiary (or potential beneficiary) data from multiple SP programs.** Critically, a Social Protection ID (SPID) linked to the national ID database is being rolled out to ensure the uniqueness and accuracy of each beneficiary record. The SPID will 'deduplicate' these databases and ensure that each individual has the same identifying information in any of the databases in question. Ultimately, administrative data from other sources, such as land, property, and asset registries will also be linked, thus helping to refine and automate targeting.

**The DSPP is the front-end interface for beneficiary enrolment and transactions.** It facilitates registration and validation of social protection identification data while enabling efficient delivery of social assistance and social security services. This system uses an integrated digital gateway to minimize duplication and fragmentation in Cambodia's social protection registration and data management. Figure 2 demonstrates how these systems are intended to simplify the beneficiary enrolment and management processes across programs.

**Figure 2: Beneficiary enrolment as envisioned under the Digital Social Protection Platform**

System	IDPoor	Family Package	PWD	NSSF	...and all social programs
Beneficiary Enrolment					
Administrator	Commune/Sangkat Focal Points (FPs) for DSPP <sup>4</sup> (+Chief for approval steps)				
User Interface	DSPP <div></div>				
Enrolment Procedure	Same as status quo	Same as status quo	Same as status quo	Same as status quo	Same as status quo
Proof of Identity and Uniqueness during Enrolment	Biometric data (2 fingerprints + face photo) and scanned copies of supporting documents				
Equipment Used	Commune/ Sangkat laptop, camera, and fingerprint scanner				
Beneficiary Management					
Data Storage – core identity data	SR				
Data storage – program-specific data	IDPoor Database	NSAF Database	DDW Database	NSSF Database	... program databases
Unique Identifier for Beneficiaries	SPID number, backed by biometric deduplication and verification against MOI Khmer ID Database				

<sup>4</sup> Usually 2-3 FPs are assigned, through a formal selection by the commune/sangkat council.

## Harmonization Progress

**The rollout of the SR and DSPP has progressed in distinct phases.** From April to July 2023, a pilot of the SR was conducted in two communes in Kampong Cham province and two sangkats in Siem Reap province to harmonize data management of the IDPoor, the Patient Management and Registration System (PMRS), Health-Social Protection Information System (H-SPIS), the Cash Transfer Program for Pregnant Women (PW-CTP), and the National ID database. More than 55,000 unique SPIDs were generated, including records both with and without national ID numbers, and without the capture of biometric data. Interoperable data exchange between databases was also successfully enabled via CamDX, Cambodia’s national data exchange platform.

**Following these positive outcomes, and with the endorsement of the Royal Government of Cambodia, the GS-NSPC put forward a scale-up strategy.** The first phase of this strategy was implemented in November 1, 2024, and involved the nationwide expansion of the SR, integrating it with key institutions, including the National Social Security Fund (NSSF), National Payment Certification Agency (NPCA), Ministry of Planning’s Identification of Poor Households (IDPoor) system, and the National Social Assistance Fund (NSAF), extending coverage across all 25 provinces. Building on this momentum, the second phase, which is currently ongoing, saw the rollout of the DSPP in 22 communes/sangkats within two districts—one each in Kampong Cham and Siem Reap.

**Figure 3: Timeline of DSPP/SR rollout**

Period	Milestone
April – July 2023	<b>Pilot</b> <ul style="list-style-type: none"><li>- SR piloted with IDPoor, PMRS, H-SPIS, PW-CTP, and National ID data in 2 communes in Kampong Cham Province and 2 sangkats in Siem Reap Province</li></ul>
November 1, 2024	<b>Scale-up Phase 1</b> <ul style="list-style-type: none"><li>- SR expands to integrate data from NSSF, NPCA, IDPoor, and NSAF – covers 25 provinces (Nationwide)</li></ul>
January 2, 2025 – present	<b>Scale-up Phase 2</b> <ul style="list-style-type: none"><li>- DSPP introduced for Family Package beneficiary enrolment in 22 communes/sangkats across 2 provinces (Kampong Cham and Siem Reap)</li></ul>
Planned for Q3 of 2025	<b>Scale-up Phase 3</b> <ul style="list-style-type: none"><li>- DSPP use and SR coverage will expand to 209 communes/sangkats across 2 provinces (Kampong Cham and Siem Reap)</li></ul>
Planned for Q4 of 2025 or Early 2026	<b>National Scale</b> <ul style="list-style-type: none"><li>- DSPP use and SR coverage will expand to all of Cambodia</li></ul>

## Key Achievements

**Figure 4: Number of Registration Via DSPP (By Program)**

No.	Program	Number of Registration Via DSPP
1	Family Core Assistance (Base Benefits)	820
2	PWD	41
3	Elderly	363
4	Pregnant Woman	226
5	Support During Childbirth	20
6	Children Under Two Years Old	26
<b>Total:</b>		<b>1496</b>

Data was extracted on Tuesday, May 20, 2025, at 11:15 AM (Local Time)

**Figure 5: Number of Registration Via DSPP (By Commune/Sangkat)**

No.	Province	Name of Commune/Sangkat (in Khmer)	Name of Commune/Sangkat (in English)	Number of Registration Via DSPP
1	Kampong Cham Province	ខ្នុរដំបង	Khnor Dambang Commune	8
2		គោករវៀង	Kouk Rovieng Commune	36
3		ផ្ដៅជុំ	Pdau Chum Commune	13
4		ព្រៃចារ	Prey Char Commune	0
5		ព្រីងជ្រុំ	Pring Chrum Commune	28
6		សំពង់ជ័យ	Sampong Chey Commune	66
7		ស្ដើងជ័យ	Sdaeung Chey Commune	6
8		សូទិញ	Soutib Commune	66
9		ស្រម៉ែ	Sramar Commune	11
10		ត្រពាំងគរ	Trapeang Kor Commune	9
11	Siem Reap Province	ស្លក្រាម	Sla Kram Sangkat	70
12		ស្វាយដង្គំ	Svay Dankum Sangkat	12
13		គោកចក	Kok Chak Sangkat	223
14		សាលាកំរើក	Sala Kamreuk Sangkat	198
15		នគរធំ	Nokor Thum Sangkat	21
16		ជ្រៅវ	Chreav Sangkat	78

17		ចុងឃ្លៀស	Chong Khnies Sangkat	48
18		សំបួរ	Sngkat Sambuor Sangkat	218
19		សៀមរាប	Siem Reab Sangkat	240
20		ស្រងែ	Srangae Sangkat	19
21		ក្របីរៀល	Krabei Riel Sangkat	64
22		ទឹកវិល	Tuek Vil Sangkat	62
Total:				1496

Data was extracted on Tuesday, May 20, 2025, at 11:15 AM (Local Time)

## About this Assessment

To ensure accountability, learning, and continuous improvement, the GS-NSPC formally requested the World Bank to conduct an independent assessment of the first and second rollout phases. Following this request, the World Bank team engaged in a series of consultations with the GS-NSPC and other key stakeholders involved in Cambodia's digital social protection initiatives. These discussions aimed to clarify institutional roles, understand stakeholder expectations, and identify opportunities for broader collaboration, both within the scope of the current evaluation and in support of future engagements.

The evaluation's scope, objectives, and methodological approach were subsequently defined through a collaborative process with the GS-NSPC. These design decisions were made in consideration of the pilot's implementation stage and the availability of evidence, recognizing that the project was not yet mature enough to support a comprehensive outcome evaluation. As such, the evaluation was specifically designed to focus on the implementation aspect, specifically the users' experience, technical performance, and implementation gaps.

## Objectives

This evaluation was conducted to generate actionable insights and evidence to inform the future expansion and refinement of the DSPP and SR in Cambodia. Its objectives are to assess:

1. **User experience:** The evaluation aims to understand the user experience of the newly introduced platform compared to the status quo, focusing mainly on registration officers and commune chiefs. This includes assessing perceived ease of use, speed and efficiency of registration, error frequency, troubleshooting mechanisms, and the overall satisfaction of users with the system. The evaluation also explores changes in frontline user workload and beneficiaries' accessibility and engagement with the platform.
2. **Technical performance:** The evaluation analyzes the technical performance of the DSPP systems and devices deployed, and the overall SR system infrastructure. This component evaluates whether the technology meets operational requirements in real-world settings and

identifies any persistent technical constraints that could impact national-scale implementation.

3. **Gaps and opportunities:** The evaluation aims to identify critical gaps in relations to the process, policy, and technical aspects that must be addressed for effective national scale-up. This includes analyzing challenges related to staff readiness, registration protocols, handling of cases without formal ID, data protection, grievance redress mechanisms, and infrastructure limitations. The findings are intended to inform the refinement of standard operating procedures (SOPs), training modules, system design, and support mechanisms for broader deployment. An analysis of the legal and regulatory framework was also conducted to assess if sufficient infrastructures are in place to support the rollout.

## Methodology

**This evaluation employed a mixed-methods approach, comprising field visits, key informant interviews (KIs), and desk research.** This approach was chosen to ensure a comprehensive understanding of how the platform functions in real-world settings, particularly from the perspectives of local implementers and key stakeholders. Results were also validated in a stakeholder consultation workshop. The details of each data collection activity are as follows:

### Field Visits

**Fieldwork was conducted through two rounds of site visits to communes in Kampong Cham and Siem Reap provinces.**<sup>5</sup> The primary data collection tools included semi-structured interviews in the form of group interviews and focus group discussions, self-administered surveys, and direct observation of the DSPP registration process.

#### Field Visit #1 (February 2025)

- The evaluation team visited **four communes/sangkats**—two in each province.
- The team conducted **group interviews** in each commune/sangkat with participants comprising commune/sangkat officers operating the DSPP registration system, commune/sangkat chiefs, village chiefs, and members of the commune/sangkat council. These discussions were also joined by representatives from the GS-NSPC and NSAF, allowing for multistakeholder dialogue and shared reflection on implementation challenges and early successes.
- During these visits GS-NSPC arranged for the commune/sangkat representatives to hold DSPP enrolment demonstrations with beneficiaries from their constituencies, allowing for **direct observation** of how the system functioned in practice. Observational data focused on the use and performance of biometric equipment, accuracy and speed of data entry, as well as logistical and environmental factors such as lighting, internet connectivity, and workspace conditions. These observational insights helped validate self-reported data and uncover workflow issues that may not be raised during interviews or surveys.

---

<sup>5</sup> For a full list of the communes and sangkats visited, see

## Field Visit #2 (March 2025)

- The evaluation team consulted with **twelve communes/sangkats** on this visit.<sup>6</sup> Although only two locations were visited, GS-NSPC facilitated the participation of representatives from surrounding communes/sangkats to converge at each site. Five communes were represented at the session in Kampong Cham and seven sangkats in Siem Reap.
- In this round, the evaluation employed a **focus group discussion (FGD)**, bringing together a mix of officers and chiefs (or council representatives) from multiple communes/sangkats.<sup>7</sup> Two FGDs were conducted in total, one in each province, with 10 to 15 participants per session. Each discussion lasted between 50 and 60 minutes and followed a pre-designed list of semi-structured questions developed by the evaluation team.
- The evaluation also collected data through a self-administered **survey** completed by commune/sangkat officers and chiefs. The survey was designed to capture key performance indicators related to user experience, system usability, technical reliability, satisfaction with technical support, and infrastructure readiness.<sup>8</sup>

### Key Informant Interviews (KIIs)

**The evaluation team held nine semi-structured KIIs in Phnom Penh.** The interview subjects represented a range of social protection program operators and broader stakeholders of the social protection and digitalization agendas in Cambodia. A full list of the organizations interviewed is included in Appendix 1: Sampling Details.

### Desk Research

**The evaluation team reviewed public and internal written materials regarding the DSPP and SR.** These included policy and legal documents, operational guidelines, and system architecture documentation. This desk review contextualized field and KII findings within the broader framework of Cambodia's social protection system. The materials were shared by GS-NSPC and KII subjects, and also obtained through online research.

### Stakeholder Consultation Workshop

The World Bank and GS-NSPC co-hosted a stakeholder consultation workshop in Phnom Penh in May 2025. The workshop included a feedback session in which participants shared their reactions to preliminary assessment findings reported by World Bank and their feedback on the DSPP/SR plan and early rollout experience. Workshop participants are listed in Appendix 1: Sampling Details.

---

<sup>6</sup> Three of the 12 communes/sangkats also participated in Field Visit #1, meaning the total number of communes/sangkats engaged was 13.

<sup>7</sup> Due to scheduling conflicts with a district-level meeting, only four commune chiefs were ultimately able to attend across both provinces, with the remainder of participants being commune officers or assistants directly responsible for DSPP implementation.

<sup>8</sup> Full survey results are included in Appendix 2: Survey Data.



## Analysis

The team synthesized findings from all data sources to assess the current state of the DSPP and SR initiatives. The findings are presented in three parts, based on the themes that emerged from the data:

- Part 1: User Experiences with DSPP & SR
- Part 2: Cambodia's ID Ecosystem – Overview & Technical Assessment
- Part 3: Legal & Regulatory Analysis

# Part 1: User Experiences with DSPP & SR

## Beneficiary Enrolment (DSPP)

**The DSPP is the “front end” interface that is intended to streamline all social assistance and social security transactions into one touchpoint for users.** The design and current status of the DSPP are outlined above in Part 1: Digital Social Protection Initiatives in Cambodia. At the time of writing, NSAF’s Family Package is the only social program whose platform has been harmonized with the DSPP—and only for beneficiary enrolment (not other functions). The Field Visit Findings presented below concern the use of DSPP to create records for Family Package beneficiaries in 22 communes/sangkats participating in this phase of scale-up. The KII Findings discuss both current DSPP implementation and also perspectives on future phases of scale-up.

## Field Visit Findings

### *About DSPP Users*

**The focal points assigned to operate the DSPP at the commune and sangkat levels are commune/sangkat officers and chiefs.** Under the current protocol, officers carry the primary responsibility for system operation, data entry, and biometric capturing. Chiefs, on the other hand, are responsible for reviewing and approving registrations and updates. However, field observations revealed considerable variation in how these responsibilities are implemented in practice. Given the frequent offsite obligations of chiefs, such as attending district- or provincial-level meetings, and their limited digital literacy or lack of familiarity with computer-based applications, officers frequently assume the review and approval functions to ensure the timely processing of registrations and the prompt delivery of benefits to households, particularly those in urgent need. A notable improvement was observed in Kampong Cham province, where chiefs can now review and approve registrations using a mobile app. This introduction is especially valuable in reducing dependence on in-office approvals and encouraging chiefs’ engagement in the approval process.

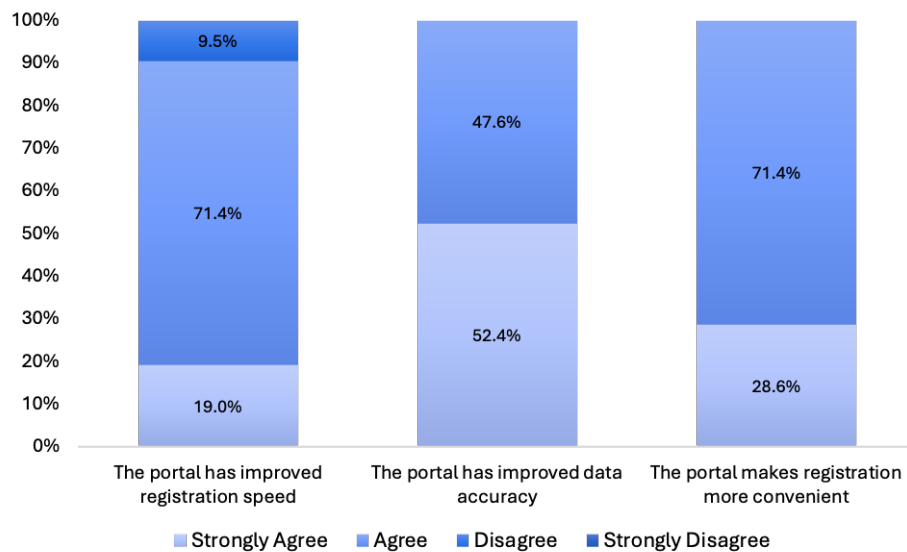
**The selection of officers responsible for the portal operations follows a formal process initiated during commune/sangkat council meetings.** Proposed focal points are discussed during the meeting and then formally approved by the chief. Typically, each commune/sangkat assigns two to three officers to use the portal. These individuals often already hold roles related to public administration, local governance, or public service delivery. They also emphasized that operating the portal does not constitute an additional burden but is instead regarded as a valuable add-on that supports them in carrying out their role during the enrolment process.

**The selected officers received four full-day training sessions from the GS-NSPC in Phnom Penh, Kampong Cham, and Siem Reap.** The trainings covered a wide range of topics, including system navigation, biometric data collection, data protection and cybersecurity, and specific roles and responsibilities of the officers and chiefs. Officers especially appreciated the inclusion of practical exercises and the opportunity to test the platform over an extended one-month period prior to the official rollout. Many noted that hands-on practice was the most valuable aspects of training in familiarizing them with the portal. Overall, participants considered the trainings adequate in equipping them with the essential competencies to operate the system effectively.

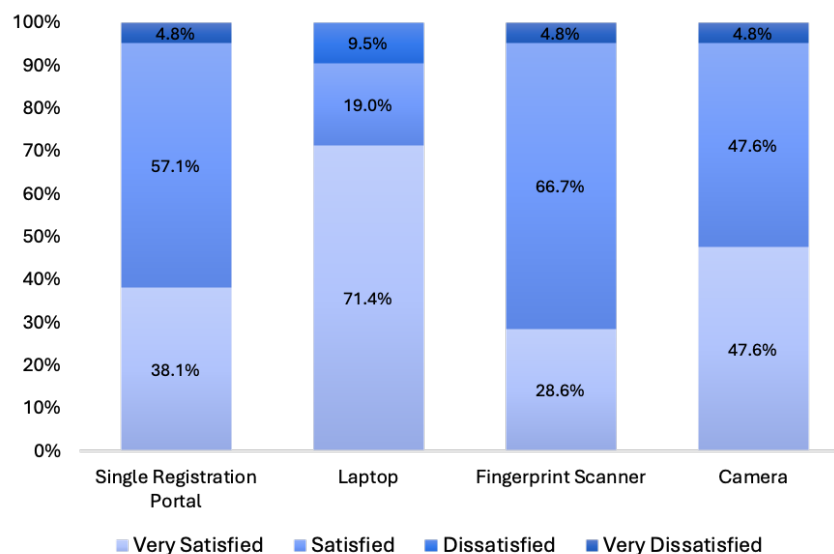
### Evaluation on User Experiences

**The evaluation consistently found that officers and chiefs reported high overall satisfaction with the portal and the equipment provided to support its implementation.** Survey data showed that more than 95% of respondents reported being either very satisfied or satisfied with the Single Registration Portal, fingerprint scanner, and camera, while over 90% expressed satisfaction with the laptop. Furthermore, 90% of respondents strongly agreed or agreed that the portal improves the speed of registration and updates, while all respondents strongly agreed or agreed that the portal improves data accuracy and makes the registration and update process more convenient for both chiefs and officers.

**Figure 4: Users' Satisfaction with DSPP, Laptop, Scanner, Camera**



**Figure 5: Perceived Improvements Compared to Previous Registration/Update Process**



Many officers and chiefs expressed a sense of pride and satisfaction in participating in piloting the portal, which they believe strengthens transparency, improves data accuracy, and ultimately delivers greater **services** to vulnerable households. A detailed evaluation of the user experience is as follows:

### Convenience

**Officers consistently expressed appreciation for the way that the DSPP reduces redundancy in registration processes—though there is still room for improvement within the platform flow.**

With the DSPP, officers can use Single Sign-On and enter beneficiary information once and apply it across multiple programs. However, officers also noted that when a single beneficiary is eligible for multiple programs—such as an elderly person who also has a disability—the system currently requires separate approvals for each benefit. While the development team acknowledged this issue and is preparing a system update, the current process still involves duplicative data entry and approval steps, reducing some of the anticipated gains in efficiency.

**More importantly, officers feel that the portal addresses several of the inconveniences associated with the tablet-based system.** Some of these inconveniences include difficulty capturing photos, system freezes during peak hours (typically 8–9 a.m.), loss of functionality after 5 p.m., and a lack of access to real-time registration data or reporting features. Survey data strongly reinforces this view, with all respondents either strongly agreeing or agreeing that the portal makes the registration and update process more convenient for officers.

**It is important to highlight that a critical factor contributing to the overall satisfaction of officers and chiefs, as consistently emphasized during the focus group discussions, has been the technical support provided by the development team through a Telegram channel.** Officers reported that most technical issues were resolved within minutes, minimizing disruptions and maintaining the momentum of registration activities. Survey results confirmed this positive experience, with over 95% of respondents reporting that they were very satisfied or satisfied with the technical support received. Yet, the sustainability of this support model remains uncertain, as it relies heavily on real-time human intervention. With the upcoming national rollout, it is unclear whether this level of support can be scaled or if additional investments in troubleshooting tools or a technical helpdesk will be needed to maintain system performance and user satisfaction.

### Speed

**The impact of the DSPP on time-per-registration is unclear.** Some commune/sangkat officers reported that the introduction of the portal has reduced the time required for the registration and updating process, with one officer noting that the average time per beneficiary had dropped from approximately 30 minutes to 15 minutes. However, survey data suggests a more nuanced picture: although nearly all respondents agreed that the portal has improved registration and update speed, there were no significant differences in the average reported time spent per registration or update before and after the introduction of the portal, with reported times consistently ranging from less than 15 minutes to 30 minutes. Nonetheless, a majority of respondents (approximately 65–70%) indicated that they usually complete each registration in under 15 minutes. As these are self-

reported estimates—given the portal does not currently track registration time—adding a feature to automatically record enrolment duration could enhance future monitoring and system optimization.

**Insights from FGDs confirmed these mixed findings.** Officers expressed varied views on their time spent using the tablet compared to the portal. It was noted that officers who reported spending more time per enrolment on the portal generally encountered challenges with the fingerprint scanning device (an issue that has since been resolved as discussed in a later section), often requiring repeated attempts to capture usable prints, which contributed to longer enrolment times. Despite these variations, there was broad consensus that the differences in speed between the two devices were relatively minor and that their respective strengths make them well-suited for different contexts, allowing them to complement each other in practice. For example, some officers reported challenges using the tablet's camera to capture clear digital photos of beneficiaries, which could delay the registration process. In such cases, they preferred using the DSPP on laptops, as the camera offered superior photo quality for both beneficiaries and supporting documents. Conversely, officers emphasized that tablets remain especially useful for conducting on-site registrations or updates at households or in villages, where mobility is critical.

#### Accuracy

**Officers and chiefs praised DSPP's biometric capturing features and identity verification functions, citing that these functions are essential for improving data accuracy.** The requirement for an ID card during registration or updates improves data quality and allows the portal to conduct identity checks against the Ministry of Interior (MOI)'s national ID database. This functionality, along with the collection of fingerprints and photos, are designed to reduce fraud, prevent duplicate registrations, and significantly improve the overall accuracy of beneficiary databases. Moreover, GS-NSPC has indicated plans to expand the use of biometrics in the future, potentially enabling biometric data to serve as an alternative means of identity verification during registration and updates, reducing the reliance on physical ID cards.

**Officers generally expressed being very satisfied with the DSPP's biometric tools (camera, fingerprint scanner, and associated software).** They particularly highlighted the quality of the camera and the system's automated validation capabilities. Many explained that these functions improve data accuracy and enable deduplication of records. Survey data reinforced this positive assessment, with all respondents either strongly agreeing or agreeing that the portal has improved data accuracy.

**Interestingly, when asked about cases where enrolment requests were rejected due to data entry errors, nearly all chiefs participating in the FGDs reported that they rarely encountered such cases.** According to the FGDs participants, this was largely attributed to the fact that commune/sangkat offices rely on lists of eligible beneficiaries identified by village chiefs, which are typically pre-screened prior to enrolment—meaning errors would be unlikely. When issues do arise, officers and chiefs typically reach out to the GS-NSPC technical team for clarification or support. There was at least one reported case in which a chief noticed incorrect beneficiary information during

the review process and requested that the individual return for re-registration, highlighting the continued importance of maintaining the chief's involvement for human oversight.

### Data Transparency and Monitoring

**A critical enhancement introduced by the DSPP is the ability to access, extract, and monitor real-time registration and program data at the commune/sangkat level.** This represents a significant departure from the previous tablet-based system, which does not provide access to enrolment data and reporting features. Without real-time data or built-in reporting tools, officers reportedly had to manually track registrations using paper or informal spreadsheets. This approach not only increased administrative burdens but also heightened the risk of errors, inconsistencies, and incomplete records. Furthermore, provincial offices provided only aggregated statistics at the district and provincial levels, leaving officers without timely, local-level data. This limited the ability of officers and chiefs to effectively monitor progress, identify and address gaps, or adjust outreach strategies to reach underrepresented or hard-to-reach populations.

**During the FGDs, officers consistently praised the DSPP's data management capabilities, describing them as a significant improvement over past practices.** This sentiment was further reinforced by survey results, with 43% of respondents identifying improved data management through enhanced data access as one of the key benefits introduced by the portal. With the introduction of the DSPP, officers and chiefs now have access to detailed, real-time registration data immediately after submission, including the number of registrants, time and date of registration, and program-specific enrolment data.

**Several requests emerged from the field for further customization and disaggregation of data.** Officers noted that they would benefit from the ability to extract data disaggregated by village, broken down by program type, and differentiated at both the household and individual levels. Officers also expressed interest in being able to export data in Excel format to support local reporting, planning, and performance monitoring. Encouragingly, the NSPC has reportedly developed these advanced reporting features and is currently reviewing the timeline for their rollout.

### Challenges and Requests

#### Biometrics Collection

**The most frequently cited challenge across both Kampong Cham and Siem Reap provinces involved the collection of fingerprint data.** While officers reported that the technology generally performed well under ideal conditions, several factors consistently undermined its effectiveness. Among the most common were faint or worn fingerprints, particularly among elderly individuals and farmers, as well as missing or damaged fingers among PWDs. Officers noted a key improvement after the NSPC lowered the fingerprint scanner's sensitivity threshold from 95% to 80%, significantly reducing number of failed scans. To maintain accuracy, GS-NSPC also introduced AI-driven functionality to improve fingerprint quality. Despite these measures, some cases still required human intervention to grant exemptions for beneficiaries whose prints could not be captured. While the threshold adjustment enabled smoother collection of fingerprint data, concerns remain about

potential impacts on accuracy as the DSPP scales nationally. A more detailed analysis of DSPP's biometric performance is provided in Part 2.

**Officers noted that it was easier to capture portrait photos of beneficiaries (compared to fingerprints) except for a few cases.** Infants and toddlers were particularly difficult to photograph, as they often moved during the image capture process. Officers sometimes needed to hold the child in place, resulting in photos that occasionally included the officer's hand. Additionally, the lack of standardized photo backdrops in many commune/sangkat offices meant that photo quality varied depending on the setting and available space. Environmental factors, such as poor lighting or strong winds (particularly when working in open-air settings), can also pose disruption to the process. While the use of standardized photo backdrops has been considered, GS-NSPC noted that using such equipment for on-site enrolment raises concerns about portability and practicality, particularly in remote or hard-to-reach areas. To address these challenges, the GS-NSPC has incorporated AI-driven functionality into the portal to enhance image quality and process captured photos, such as face counting, cropping, rotation, and other transformations aimed at standardizing photos and improving overall consistency, regardless of where or how the images are captured. Nonetheless, maintaining a level of standardization in the photo capturing process is essential as consistent, high-quality image are critical for accurate identity verification, minimizing errors, and ensuring the overall reliability and trust in the database. Best practices and recommendations are discussed in more detail in Part 2.

**Despite these challenges, officers broadly praised the DSPP's built-in camera lighting.** They feel that this feature has helped to improve the consistency and clarity of images, compared to the previous system. Encouragingly, by the time of the second field visit, officers demonstrated awareness of some best practices in portrait photography, including ensuring adequate lighting, using non-distracting backgrounds, and confirming that only the beneficiary's face appeared in the frame.

#### Data Protection and Privacy

**FGDs revealed that officers have incorporated consent practices into the biometric collection process.** Across all surveyed communes/sangkats, officers consistently reported that they inform beneficiaries about the purpose of collecting biometric data and request their consent before proceeding with fingerprint scans or taking photographs. Officers reported that they did not encounter any cases in which beneficiaries objected to the collection of biometric data or photographs. It can be observed that this acceptance was generally pragmatic and transactional, as beneficiaries were primarily motivated by the immediate outcome of benefit eligibility rather than by a comprehensive understanding of data privacy rights.

**GS-NSPC has stated that it is adopting the data protection rules of the programs it is harmonizing, while working towards a more robust data protection framework.** To support and standardize consent practices, the NSPC explained that they adapted data protection and privacy procedures from prior guidelines established by program operators, while making efforts to communicate the basic principles of data protection and privacy to officers and chiefs. However, it

remains unclear whether the NSPC has adopted rules to incorporate data protection safeguards, and the Harmonization Sub-Decree does not reference data protection and privacy procedures of other programs. A more detailed legal and regulatory assessment is provided in Part 3.

### Role Delegation

**Although chiefs are formally assigned responsibility for reviewing and approving enrolment and update requests submitted through the DSPP, the evaluation found that, in practice, these tasks are frequently handled by officers, a practice reportedly carried over from the use of the earlier tablet-based system.** Observations from the first field visit revealed that officers often handled the review and approval of enrolment requests independently, without waiting for the chief to verify and approve the submissions. In contrast, some officers in other communes/sangkats emphasized that they must be formally delegated this responsibility by the chief before performing such tasks. By the second field visit, officers and chiefs across all participating communes/sangkats consistently confirmed that formal delegation from the chief is required, and it is recommended for the chiefs to formally issue a nomination letter or directive to formalize this delegation. In one commune, monthly meetings have become a valuable forum for reviewing enrolment progress and for discussing and resolving implementation challenges.

**Two key factors explain the delegation of review and approval responsibilities to officers.** The first is the low level of digital literacy among chiefs, which limits their ability to operate the DSPP without support. In some communes/sangkats, officers reported physically bringing the laptop to the chief, logging into the chief's account, and guiding the chief through the approval process. Although survey data shows that all respondents strongly agreed and agreed that the portal is easy to use, the shift from a tablet-based system to a computer-based one represents a substantial learning curve, particularly for individuals with little prior experience using computers. Testimonies from the FGDs highlighted that officers themselves required an adjustment period to become familiar with the provided laptop, whereas adapting to the tablet system was generally easier because its interface more closely resembled that of a smartphone. The second key reason driving delegation is the frequent absence of chiefs from the commune office due to off-site responsibilities, including mandatory district- or provincial-level meetings and outreach activities at the village level.

**While this delegation has helped maintain operational efficiency, it also raises important accountability concerns.** And as previously discussed, encouraging the chiefs' involvement in the review and approval stage is essential for maintaining human oversight and preventing errors, and GS-NSPC has acknowledged this issue and expressed its commitment to developing a solution that ensures proper oversight while preserving operational efficiency. Against this backdrop, the introduction of the mobile app version of the review and approval function can be regarded as a promising solution, with strong potential to strengthen the engagement of chiefs by enabling them to participate in the process even when they have limited digital literacy and are away from the office. Feedback gathered during the field visits also highlighted other areas for improvement, notably the need for refresher trainings as system updates or new features are introduced. In addition, there is a clear demand for digital literacy training tailored to older staff, particularly chiefs, to ensure they are better equipped to engage with the system independently and confidently.



## Mobility

**A commonly reported challenge raised by both officers and chiefs is the limited mobility of the DSPP and its associated devices.** The laptop, camera, and fingerprint scanner are difficult to carry when conducting enrolment and update campaigns at the village and household levels. These outreach activities are crucial for increasing enrolment rates, particularly in remote areas and among elderly populations and PWDs, thereby supporting efforts to expand the reach of social assistance programs to the most vulnerable households. Although the DSPP has been widely praised and enjoys strong support across communes/sangkats of both provinces, FGDs consistently revealed a preference among officers and chiefs to use the tablet, rather than the DSPP and its devices, for registration and updates during house visits or village-level outreach campaigns. Recognizing this operational constraint, the GS-NSPC is currently working to enable fingerprint capturing directly through tablets, leveraging the DSPP's compatibility across platforms to enhance flexibility and ensure that essential biometric functions can be carried out even during house visits and village-level enrolment campaigns.

## Infrastructure

**The effectiveness of the DSPP is dependent on the availability of reliable infrastructure, particularly stable electricity and internet access.** For electricity, most communes/sangkats did not report significant issues. However, officers and chiefs noted that disruptions often occur during the hot season or as a result of road construction activities that impact local power supply. In response, several officers and chiefs requested support in securing backup solutions such as power banks and generators.

**Regarding internet access, all communes/sangkats participating in the FGDs reported having Wi-Fi routers installed at their offices, though the speed and reliability of connectivity varied across locations.** While most communes/sangkats did not experience severe internet disruptions, some officers highlighted connectivity as a recurring challenge, especially during house visits and outreach campaigns in remote areas where mobile network coverage is poor. In cases where Wi-Fi is unavailable, officers often rely on their smartphone's mobile hotspot. However, this approach is highly dependent on local network strength, and several officers noted that poor mobile coverage in their communes/sangkats or in some target villages.

**In addition to these infrastructure challenges, one officer raised concerns about overcrowding at the commune/sangkat office following outreach efforts to inform beneficiaries of enrolment and update opportunities.** As a result of the campaign, approximately 200 beneficiaries arrived at the commune/sangkat office around the same time, leading to long wait times and logistical bottlenecks. The officer reported that overcrowding complicated efforts to clearly explain program entitlements and payment procedures to beneficiaries. This confusion contributed to downstream issues, with some beneficiaries later encountering difficulties in claiming their benefits due to misunderstandings about payment timelines and requirements. While important, this issue falls outside the scope of the DSPP system evaluation and is more closely related to the internal coordination and communication practices of the commune/sangkat office.

## Payment Delays

**Another key challenge consistently raised by officers and chiefs during both field visits was the delay in benefit payments to beneficiaries.** Officers reported that several beneficiaries were unable to claim their payments on the expected date, although it should be noted that these issues were predominantly reported among beneficiaries enrolled in the social assistance program for pregnant women. During the first field visit, representatives from NSAF, who were present on-site, explained that these delays were often caused by system-detected duplications when officers registered or updated beneficiaries using the portal. To resolve these cases, beneficiaries were advised to file a formal complaint.

**The technical role of DSPP in these delays is unclear, but to end users they seem connected.**

During the second field visit, some communes/sangkats observed a few cases of payment delays associated with enrolment done through the DSPP, although these claims were not uniformly confirmed across the two provinces. When asked whether payment delays were a common issue under social assistance programs, most officers and chiefs indicated that such delays had been a challenge even prior to the rollout of the DSPP. As such, it remains unclear whether the introduction of the DSPP has contributed to, or exacerbated, the incidence of payment delays. Whether the technical issue originates in the DSPP, the NSAF system, or elsewhere, GS-NSPC should be aware that to beneficiaries the distinction will not matter and delays experienced will be associated with the new DSPP system from their perspectives. This perception places additional pressure on commune officers and chiefs, who are the first point of contact for concerned beneficiaries. Officers noted that they are frequently required to answer questions about payment status and, in some cases, have even faced accusations of withholding funds or engaging in corrupt practices when payments are delayed. These dynamics highlight the importance of clear communication and back-end coordination between systems to protect the credibility of frontline implementers and sustain trust.

## Other Challenges and Requests

**A recurring issue highlighted in FGDs and survey data was the lack of required identification documents—particularly Khmer ID cards—among beneficiaries, especially the elderly.** Officers noted that it is common for elderly individuals to forgo renewing expired or lost ID cards, as they often perceive little need for formal identification. When enrolling such individuals, some communes/sangkats have opted to use the tablet, which allows birth certificates to substitute for ID cards during enrolment. Because the DSPP require ID card number to verify beneficiary's identity against MOI's National ID Database, officers are often encouraged to upload the National ID card though the platform also allows for the use of alternative documents (i.e. Birth Certificates) but identity verification is not available for this option. However, this flexibility may not be fully understood by the end users as observed during the field visit. A common workaround for handling households lacking ID cards as reported by the officers and chiefs is the issuing of a verification letter by the chief confirming that the beneficiary possesses an ID card that is currently under renewal. Officers then upload this letter, which includes the beneficiary's Khmer ID number, into the system as a temporary substitute for the ID card when enrolling beneficiaries in social assistance programs.

**In addition to these operational challenges, officers and chiefs put forward a number of requests to improve implementation.** First, they expressed strong interest in enhanced data access, requesting more detailed reporting features that disaggregate enrolment data by program, village, household, and individual levels, along with the ability to export data in Excel format. Second, officers requested the ability to enrol beneficiaries in multiple programs simultaneously, noting that the current process requires sequential approvals by the chief before registering the same beneficiary in another program. Third, to address connectivity constraints during house visits and outreach campaigns, officers and chiefs requested an offline version of the DSPP. Fourth, several communes/sangkats asked for additional equipment, including power banks or generators to prepare for power outages and multi-function printers (for printing and photocopying), as well as printer ink. Fifth, some communes/sangkats proposed the incorporation of grievance procedures directly into the portal, noting that the current complaint resolution process is often slow (this functionality is reportedly in the process of conceptualization by the GS-NSPC). Finally, a few officers raised the possibility of introducing some monetary incentives for each enrolment, highlighting that the IDPoor program currently offers approximately 1,500 riels per registrant as incentives.

## Responses from Beneficiaries

**As part of the evaluation, the team conducted brief interviews with beneficiaries of social assistance programs during both field visits.** While the introduction of the DSPP primarily affects the operational experience of officers and chiefs, it is also important to understand beneficiaries' perceptions of its implementation.

**The majority of beneficiaries interviewed, many of whom were elderly individuals and PWDs, reported no noticeable change in their enrolment or update experience as a result of the DSPP.** From their perspective, the most critical concern remained the timely receipt of benefits, rather than the procedural details of the registration process. Nonetheless, beneficiaries welcomed the opportunity to participate in the programs and consistently emphasized the importance of the support they receive in meeting basic needs.

**Beneficiaries did not report concerns about the introduction of biometric data collection.** A specific focus of the evaluation team was to explore beneficiary views on the collection of biometric data, particularly fingerprint scans and portrait photographs. All interviewed beneficiaries claimed that they understood the purpose of providing biometric information and viewed it as a necessary step to qualify for program benefits. None expressed concerns regarding the collection or use of their biometric data, nor did they raise questions about privacy or data security. Beneficiaries generally perceived these requirements pragmatically, focusing on the direct link between compliance and access to financial assistance. While all beneficiaries noted that they did not experience any notable challenges during the enrolment process, some voiced a desire for increased benefits.

### *Perception on National Rollout of the DSPP*

**During the FGDs, officers and chiefs consistently expressed strong support for the national rollout of the DSPP.** They believe the portal would bring similar benefits to other communes/sangkats as it has to theirs. Survey data reinforced this optimism, with over 90% of respondents indicating that they believe the DSPP is ready for national scale-up. However, despite their confidence in the platform itself, officers and chiefs expressed more cautious views regarding the readiness of other communes/sangkats to adopt and implement the system, with only 71% of respondents expressing confidence that other communes/sangkats are ready to adopt the DSPP.

**In their recommendations for national scale-up, both officers and chiefs stressed the importance of ensuring that all implementing officers across the country have access to adequate training.** They recommended that future rollouts prioritize comprehensive training for officers and chiefs alike, including refresher sessions and specialized modules for older staff or those with limited digital literacy. They also recommended creating opportunities for experience sharing, where communes/sangkats with early implementation experience can share best practices with those newly adopting the system.

### Key Informant Interview Findings

**Social protection program operators have concerns about the pace and comprehensiveness of the DSPP software development process.** While they acknowledged that the GS-NSPC technical team has been very communicative and accessible during the process of harmonizing their existing apps with DSPP, they shared some specific challenges. The first issue is that their self-developed apps are very complex and difficult to replicate. Their programs have extensive, nuanced standard operating procedures (SOPs) and their digital tools need to reflect many conditionalities in enrolment questionnaires and benefit delivery process flows. These things cannot be coded properly without the guidance of someone who knows the SOPs in detail. The program operators feel that it would be most efficient for their own IT teams to own and implement the harmonization process (the World Bank understands that this agreement has been made already with at least one program). The second issue is the pace of DSPP development. Program operators noted that the process of recreating their apps in DSPP is moving slowly, and that even the one program that is integrated at present (the Family Package) does not have all of the functions that the original app provided (such as lodging and tracking complaints, or filing insurance claims). They worry that if those cannot be added to DSPP quickly, parallel apps will be required for a long time, especially since the GS-NSPC has not made it clear whether the existing apps will be phased out or retained, all of which will be confusing for end users. The presence of parallel apps also creates change management issues—every time a program's SOPs change slightly, it is necessary to update two interfaces and run two education campaigns for field teams. This creates more work and introduces more room for error. According to the GS-NSPC, the full functionality is ready for rollout, and delays are due to readiness of the operators' systems (this assessment could not investigate the source of delays further). Finally, operators from multiple programs also registered concern that focusing on or directing their resources toward integrating their platform with the DSPP will slow down innovation for their programs, because it requires returning to things that they already solved a few years ago.

**Operators also request a more structured harmonization process.** They shared that from their perspective it has felt like the DSPP development completed to date has been ad hoc without set rules and procedures for harmonization. They feel that before scaling up any further, GS-NSPC should establish a formal mechanism for IT teams from partner organizations to raise tickets for technical issues and track their resolution. GS-NSPC has already established such a system on the back-end: they receive requests through Telegram, but then enter them into their tracking system. Since operators have shared that they would value a more formal and transparent system, it would be useful to build out the front-end of the existing GS-NSPC system. (The operators did note that the response provided through Telegram has always been very swift and thorough, though).

**Operator representatives in Phnom Penh are concerned about the viability of using laptops at the commune/sangkat level in place of tablets.** First, they expect low digital literacy among commune/sangkat focal points to be a barrier to adoption. They noted that laptops do not have Khmer keyboards and that the Windows operating system (OS) is unfamiliar (whereas touchscreen tablet keyboards can be set to Khmer script and use an OS more similar to familiar smartphone interfaces). Second, they anticipate asset management challenges. The laptops are less portable (for household visits) and not self-contained (require an external camera and fingerprint scanner, meaning there are three devices to keep track of). Third, they question the sustainability of the plan—it is not clear where the resources will come from to obtain and maintain a national supply of laptops and biometric devices. Also on the topic of resources, it is not clear what will happen to the national set of tablets purchased for social protection program delivery. These equipment concerns contrast with the enthusiasm for the new equipment from the chiefs and officers interviewed for this evaluation (see Field Visit Findings). This makes sense—individual chiefs and officers were likely not thinking about national scale issues like asset management and resource sustainability. As for digital literacy challenges, the FGD respondents may have had some incentive to downplay these issues in order to not lose their new resources, or it may be that the communes and sangkats visited have average or high digital literacy levels, and the national operators are thinking of lower-capacity locations elsewhere in the country. The overall picture is surely nuanced, and both perspectives are helpful as the program prepares to scale up.

**The stakeholders interviewed have reservations about the logistics and ethics of collecting biometric fingerprint data.** While the Family Package program has a clear touchpoint from which to obtain this data (annual verification of beneficiaries for record renewal), other programs do not require regular in-person transactions with their beneficiaries, meaning that collecting the fingerprints of already-enrolled individuals would require extra mobilization. More fundamentally, operators expressed concerns about collecting biometric data in the absence of stronger data protection safeguards, security practices, and legal and regulatory frameworks. Conducting a Data Privacy Impact Assessment, as recommended in Part 3, would help to address these reservations.

**Finally, operators feel that more resources and predictability are needed to scale up the DSPP.** They are supportive of the initiative's objectives and appreciate the GS-NSPC's collaboration to date. However, all operators interviewed noted that participating in the harmonization effort has added significant work to their programs, and no extra resources have been allocated to account for this.

For smaller programs and teams this is especially challenging. Some operators also noted that to them it felt like the plans for harmonization have changed frequently, even after implementation was underway. They would like to have more stability and clear expectations so that their teams can plan accordingly.

## Beneficiary Management (SR)

**The SR is the back-end system that is meant to provide a centralized, consolidated database containing demographic and socio-economic details of beneficiaries and potential beneficiaries of various social protection schemes.** The design and current status of the SR are outlined above in Harmonization Progress. At the time of writing, the following programs are integrated into the SR: (i) the Family Package, (ii) the Health Equity Fund, (iii) the National Social Security Fund (NSSF), and (iv) the NSAF-financed civil service and veterans' pensions. The SR links these databases through the Social Protection ID (SPID) as well as the data exchange platform. This allows the Government of Cambodia and the NSPC to monitor these programs, ensure coherent policies across the social assistance and social insurance sectors and for targeting where relevant. This includes responding to natural disasters and other events as part of the 'shock-responsive' SP system.

**The Field Visits did not yield insights about the SR because commune/sangkat officials to not interact with it.** The KII Findings below synthesize stakeholder views on the SR, considering both the experience to date of partners who have onboarded into it and more general perspectives about the plan.

## Key Informant Interview Findings

**The details of SR's eventual data architecture are unclear to stakeholders, which is raising concerns about data storage and ownership.** The uncertainty stems from both official communications and the language of Sub-Decree 38 ANK.BK. One concern is that the SR may house program-specific beneficiary data (related to eligibility criteria, program usage, etc.), rather than strictly storing a minimal number of identity-related data fields to enable data sharing between otherwise separate program databases. The text of Articles 8 and 9 of the sub-decree in particular give this impression. Another concern is that, even if this data centralization is not the goal, the new process flow may expose program data to risks in transit, since it has to be channeled through the DSPP and SR on its way to program databases. Program operators see these possible scenarios as threats to both their control and oversight of their programs, and to their ability to comply with their own data protection standards. The NSPC has signaled its intention to formulate a sector-specific set of data protection regulations and has, through the support of UNICEF, contracted an international consultant to provide recommendations on the same.

**The potential data sharing application that would be most valued by the stakeholders interviewed is a possible connection to the MOI's civil registration and vital statistics (CRVS) data.** Most social programs deliver services to a main beneficiary and their dependents, and expend effort keeping records of dependents up to date. Accurate and timely CRVS data could automate the

process of adding and removing dependents following births and deaths. Some interview subjects went further, pointing out that if a unique identifier (UID) were issued from birth through the MOI system and accessible to social protection programs, this could achieve the same benefits as the SPID (plus other positive externalities in other sectors). Unlike MOI's National ID database, the CRVS database is currently not digitalized. However, the MOI's General Department for Identification (GDI) has developed a roadmap to digitalize the CRVS system and establish UIDs from birth, which would enable the data sharing on dependent updates discussed above.<sup>9</sup> GDI has also started to provide identity verification services via the National ID database. These developments suggest that GDI may eventually be able to play a more direct role in the digitalization of social protection than previously planned for.

## **Box 2: Stakeholder Consultation Workshop**

During the consultation workshop on the draft evaluation report, participants were grouped into three stakeholder categories: commune and sangkat officers and chiefs, representatives from relevant implementing operators, and officials from line ministries. Following the presentation of the evaluation findings on the implementation of the DSPP, each group engaged in a group discussion to share their reactions to the findings, identify gaps in the analysis, clarify misunderstandings, and jointly reflect on key challenges and opportunities ahead of the platform's scale-up. The session also served as a forum for open dialogue among stakeholders and the DSPP development team to build consensus and strengthen coordination.

### *Commune/Sangkat Officers and Chiefs:*

Commune and sangkat officers and chiefs expressed their agreement with the evaluation findings, particularly regarding the benefits provided by the DSPP, including the platform's role in reducing duplication, streamlining registration processes, and resolving common issues that were prevalent under the previous tablet-based system. Participants also praised the responsiveness of the technical support team, which was described as instrumental in resolving day-to-day issues during implementation.

To further improve the DSPP and support its future scale-up, officers and chiefs reiterated several recommendations or requests. These included enabling the registration and approval of beneficiaries across multiple programs in a single process, particularly for pregnant women who may be eligible for several linked benefits, developing a grievance module within the platform, adding offline functionality to support registration and update efforts in remote areas, and ensuring adequate provision of equipment and capacity-building support for commune-level users.

Looking ahead to the national rollout, participants acknowledged potential challenges. They anticipated that a significant increase in users may place additional strain on the system and could slow response times from the technical support team. They also noted that limited digital literacy

---

<sup>9</sup> As outlined in the Law on Civil Registration and Identification (2023) and the National Strategic Plan of Identification (NSPI) 2017-2026.

among commune/sangkat staff could become a barrier to adoption, reinforcing the need for training. Nevertheless, many commune/sangkat officers and chiefs expressed optimism, noting that while such challenges are expected, they believe that implementation will improve over time as more communes and sangkats become familiar with the platform.

In terms of communication, officers in both provinces affirmed that Telegram remains the preferred channel for interacting with the DSPP development team. However, they recommended creating province-specific Telegram groups to ensure timely responses and manage the expected increase in technical support needs. For beneficiary engagement, participants emphasized the importance of leveraging local authorities, particularly commune and sangkat officers and village-level authorities given that many beneficiaries either do not own mobile phones or lack the digital literacy.

Finally, participants urged national-level teams to ensure that systems are in place to meet the practical needs of commune and sangkat offices. They called for clear communication procedures between the DSPP development team and commune/sangkat focal points, regular or periodic training programs accompanied by regular assessments, and dedicated resources for equipment provision, maintenance, and replacement.

#### *Line Ministries*

In responding to the evaluation results, line ministries representatives did not have any notable inputs but underlined the need for greater clarity regarding the data collection methodology, particularly the sampling strategy used in the evaluation. They also expressed a preference for the evaluation to focus more directly on the technical aspects of the platform and its implementation challenges.

Participants acknowledged the potential of the DSPP to benefit their respective ministries and agencies, particularly through its capacity to connect registration portals across multiple social assistance programs, which is expected to streamline monitoring and facilitate deduplication. On the other hand, several anticipated challenges were raised in relation to the planned scale-up. Participants emphasized the need to address foundational issues, such as human resources, budgeting, and infrastructure readiness. Concerns were raised about whether the current capacity of the national data center is sufficient to manage increased usage, along with broader risks related to internet reliability, cybersecurity, data privacy, and digital literacy among users. The absence of a complaints management module was also highlighted as a critical gap requiring attention.

On the issue of stakeholder engagement, ministry representatives stressed the importance of clearly delineating institutional roles and responsibilities. They also requested dedicated resources to be allocated for capacity building and called for stronger collaboration between relevant ministries and implementing agencies. Lastly, the development of a clear work plan or roadmap for scale-up was viewed as essential to ensure a successful rollout. Overall, representatives expressed their willingness to work with the GS-NSPC and the DSPP development



team and some requested a separate meeting to enhance coordination and jointly define plans for the next phase of implementation.

### *Operators*

While operators did not offer additional feedback on the evaluation findings, they raised a range of operational and technical concerns that must be addressed to support a successful scale-up. A central issue discussed was the capacity of commune and sangkat offices to implement the DSPP. Operators believe that the DSPP differs from their app's original design, which could pose an initial learning curve for users. Moreover, digital literacy among commune/sangkat staff was another key concern among operators as many offices still lack staff with sufficient digital skills, and few, if any, have dedicated IT personnel. This, they argued, reinforces the need for training and capacity-building efforts, as well as the mobilization of additional resources.

Other prominent concerns included internet connectivity and equipment maintenance. Operators pointed to persistent problems with internet access in remote communes and sangkats, which have disrupted consistent use of the platform. They strongly recommended the development of offline functionality to allow uninterrupted registration. In addition, operators highlighted that laptops, fingerprint scanners, and printers deployed under the DSPP would require maintenance or replacement every 3-5 years, and appropriate budgeting for repairs and replacements should be planned from the outset.

Finally, discussions around the potential inclusion of a complaints management system revealed the need for greater clarity in its scope and purpose. Operators questioned whether the development team would merely transmit complaints to the appropriate authorities or take on a more direct role in resolution. They highlighted the importance of clearly defined roles and responsibilities and cautioned that care must be taken not to overstep boundaries or duplicate the formal responsibilities of the designated operators.

More broadly, operators expressed that significantly more work is needed to address key concerns before the DSPP can be successfully rolled out at scale. Some urged the development team to take the necessary time to gain a thorough understanding of each operator's roles and the specificities of their programs. They also stressed the importance of ensuring that program ownership remains with the respective operators, including the authority to innovate and develop program-specific functionalities within the broader DSPP framework.

## Part 1 Recommendations

The stakeholders consulted for this evaluation shared many specific suggestions for the DSPP and SR initiatives—both ways to improve, and things they value and feel should continue. These are reported in detail in Field Visit Findings. The World Bank team encourages the GS-NSPC to read this section carefully and consider all suggestions. What follows below is a synthesized set of recommendations, based on the main themes to emerge from the evaluation.

## **1. Continue to strengthen stakeholder consultation and communication**

While buy-in has increased in recent months, there is still some uncertainty among social protection program operators about the details of DSPP and SR implementation. A lack of details on data architecture, combined with unclear language in legal provisions, has led to concerns about data storage and program ownership in the long term. In the short term, operators have experienced challenges harmonizing their existing digital assets with these new initiatives. There is not full confidence in the new system's ability to protect the sensitive personal data it is collecting.

The GS-NSPC should clearly address all of these uncertainties in detail. Stakeholder consultation should be invested in as an urgent priority for the next phase of the DSPP/SR initiative, both to strengthen existing forums and to create new opportunities for open discussion. This could include:

- Regular touchpoint meetings
- “Co-creation” workshops<sup>10</sup> to design future phases of DSPP/SR collaboratively
- Proactive, transparent messaging about how data will flow in the new setup

Communication should also be two-way; in addition to sharing more details of its plans the GS-NSPC should seriously consider suggestions from program operators on how to adapt the DSPP/SR initiative.

## **2. Leverage existing resources**

There are multiple resources that may be under-utilized in the current plans for the DSPP/SR. One is the national network of Android tablets, which are valued by end users for their mobility and user friendliness. Another is the impressive digital transformation already achieved by social protection programs, in the form of developing very nuanced, advanced applications and databases and delivering national training campaigns on how to use them.

Suggestions for *how* to leverage these and other resources would require further analysis and consultation. The World Bank wishes only to note the serious potential of these features, and to encourage the GS-NSPC to pause and reflect on the current context before proceeding with the DSPP/SR scale-up.

## **3. Formalize Customer Relationship Management (CRM) processes**

The GS-NSPC should be commended for the extensive technical support they have provided to the communes and sangkats implementing the DSPP in this phase of roll-out, and for their active collaboration with program operator IT teams. However, this service is delivered on-demand through Telegram. This will not be sufficient or sustainable when the initiative scales up nationally.

A program of this scope requires a formal Customer Relationship Management (CRM) platform. Such a system would organize all types of incoming requests (such as complaints from program beneficiaries, questions from commune/sangkat officers, or bug notifications from operator IT

---

<sup>10</sup> See Interaction Design Foundation 2025 for more on this approach.

teams) and allow GS-NSPC to track their resolution. This would reduce the risk of missing any queries, and would allow for automated higher-level tracking of the frequency of various complaints, questions, and errors. The increased formality could also serve to increase confidence and trust in the new system. Elements of this system are already partially developed, as shown below:

Audience	Current System	Ideal Future System
Beneficiaries	Existing program grievance channels.  A DSPP Grievance Mechanism is drafted but not yet deployed.	A single CRM system with unique front-end interfaces tailored to these different audience types, and an integrated back-end that enables both high-level and granular monitoring.
Commune/ Sangkat Officials	Telegram	
Operator Parter IT Teams	Requests are sent via Telegram, but on the back-end they are logged in a monitoring system developed by GS-NSPC.	This should be co-created with program operators to ensure the valued features of their existing systems are retained. <sup>11</sup>

#### 4. Expand training program

End users from participating communes and sangkats greatly value the training provided by GS-NSPC (especially its hands-on, practical exercises), and urged that it be continued and expanded for the national scale-up. As recommended by these users, the GS-NSPC should prioritize comprehensive training for officers and chiefs alike in every commune/sangkat they engage. This could include:

- Developing a plan to extend the existing training program to the new communes and sangkats brought into the rollout. This will not be possible for GS-NSPC to deliver alone. The team should consider a train-the-trainer model in which national or provincial leaders from NSAF or MOI are trained and then train their subnational colleagues. This approach would require a quality control plan with random assessments and drop-in visits. In addition, leveraging existing government training infrastructure, such as the National School of Local Administration and the Cambodia Academy of Digital Transformation (CADT), can also offer a viable and sustainable channel to support large-scale training delivery.
- One way to manage quality control would be to create a practical test that commune/sangkat officials have to pass in order to operate DSPP. This would give GS-NSPC some reassurance that individuals they did not train directly are competent. GS-NSPC could also issue certificates to those who pass the test, identifying them as official DSPP operators. This could build pride and investment in the platform. The team would have to mitigate the risk of alienating anyone who struggles with the test, though—perhaps GS-NSPC could deploy its own trainers in these cases.

<sup>11</sup> During the consultation workshop, some stakeholders advocated for a centralized platform and others emphasized the importance of maintaining separate branding and communication channels for each program. Further discussion is required.

- Using the training framework to provide training not only at the point of introduction of DSPP/SR, but also refresher training for any platform updates that are rolled out in the future, off-cycle onboarding for new commune/sangkat focal points, and ongoing refresher training for all system users. While initial training should be delivered in person, ongoing refresher trainings could be delivered virtually (perhaps even through the DSPP interface).
- If capacity is available, adding new modules to the training program could add significant value. For example:
  - A fundamental course on laptop use and other basics, for older staff or those with limited digital literacy. This will be especially important for future locations where capacity may be lower.
  - An advanced course on data extraction and analysis for policymaking can be developed for enthusiastic users.

The development and delivery of such an extensive training program is a significant undertaking; GS-NSPC should allocate staff and financial resources to this objective.

## **5. Conduct sustainability assessment**

National operators and commune/sangkat teams alike had some questions about the financial sustainability of the DSPP/SR initiative. Developing and publicizing a budget sustainability plan would help to instill confidence in the system and remove barriers to participation. Considerations at the local level include things like power banks, generators, and mobile data packages to ensure system performance during power or WiFi outages. Considerations at the national level include the procurement, provision, remote management, and maintenance of thousands of laptops and accessories. A sustainability assessment would start with stakeholder interviews to understand the full spectrum of costs to consider. If such an assessment and financial plan already exists, it should be shared widely.

# Part 2: Cambodia's ID Ecosystem: Overview & Technical Assessment

## Introduction

The identification system landscape in Cambodia is evolving rapidly. The foundational elements of the system – the Khmer ID and the civil registration and vital statistics (CRVS) system – are administered by the Ministry of Interior (MOI). There have been plans to overhaul both for some time, which have been reiterated in the 'Cambodia Digital Government Policy 2022-2035' (MPTC 2022). This includes the digitalization of the birth and death registration processes and ramping up authentication services based on the national 'Khmer ID' database. There is also a new digital ID option from the Ministry of Post and Telecommunications (MPTC)'s Digital Government Committee (DGC), which could become part of the national level ID architecture once there is sufficient access to most of the population. In parallel, the expansion of social protection programs has led to multiple functional forms of identification. While the Khmer ID has long used biometrics for identity proofing, this technology is now being adopted by several functional ID systems. This raises questions about potential duplication of costs and the possible need to rationalize different elements of the system.

The description that follows is divided into four sections. The next section looks at the foundational elements of the system while Section 3 reviews the current state of functional IDs in the social protection sector. The fourth section describes the recently launched Social Protection ID (SPID) that aims to rationalize and improve on the existing set of functional IDs related to social protection and make interoperability and data sharing possible. Section 5 provides an initial assessment of and recommendations taking into account emerging good practice internationally with regard to digital public infrastructure (DPI). The last section summarizes.

## Cambodia's Foundational IDs

The two key elements of the foundational identification system in Cambodia are the civil registry and the Khmer National ID<sup>12</sup>. Both are administered by the General Department of Identification (GDI) in the MOI. The GDI aims to integrate the various ID-related databases into one Integrated Population Identification System (IPIS), which would issue individuals a unique identifier from birth until death.

## Civil Registration and Vital Statistics

The registration of new birth, death and marriage events are handled at the commune and sangkat levels. These are mandatory. These have been maintained in paper files at the commune/sangkat level with a parallel database maintained in Phnom Penh at the GDI headquarters. The focus of recent digitalization efforts has been on birth registration. Between 2002 and 2025, more than 20 million birth certificates have been issued of which only a small fraction have been digitalized. There

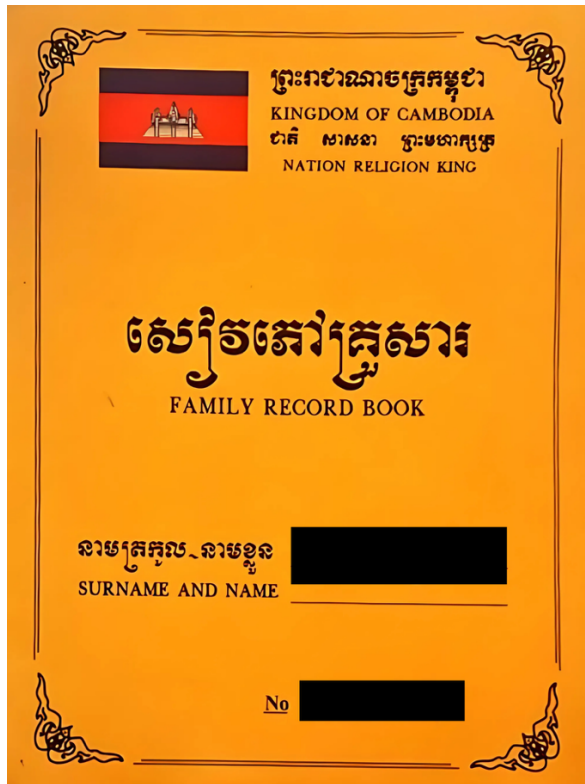
---

<sup>12</sup> We do not include a description of the family residence register or the passport here. Both are also administered by the GDI.

are pilots in place in three provinces to digitalize the process itself. However, these efforts have been delayed due to shortage of funds, mostly coming from international donors.

Another important form of identification is the Family Book. Also paper-based, there are requirements for families to be registered in their locality. These are often not updated and this can lead to problems in enrolment for services and programs that are targeted on families or where there are dependents covered by insurance (see NSSF below).

Figure 1 *Cambodia's Family Book*



The GDI intends to begin issuing unique ID numbers at birth in 2025. This ID number would be linked to the Khmer ID linking the identification of children with adults for the first time. The current birth registration rate is estimated to be around 92 percent of children between ages 0-5. This is on the high end of countries at a similar income level<sup>13</sup> although it is less clear how many parents have access to physical birth certificates (BCs). Due in part to the lack of digitalization and residual gaps in coverage, the BC is not required as proof of identity for many social protection programs.

## The Khmer ID

Cambodian citizens aged 15 and above are eligible for the Khmer ID and while it is not mandated, it is strongly encouraged and required for many interactions with the government as well as the

<sup>13</sup> The (non-weighted) average birth registration rate for lower middle income countries was 77% in 2021 (Clark, Metz, & Casher 2022).

financial sector. The GDI intends to reduce the age of eligibility to 5. Enrolment campaigns over the last decade have increased coverage significantly with estimates placing the share of the eligible population at around 90 percent. This compares well to countries at similar income levels<sup>14</sup>. Birth certificates are mandatory for enrolment.

Since 2012, ten fingerprints have been captured at enrolment for the purpose of deduplication.<sup>15</sup> There are between 4-5000 biometric capturing operators working at the commune level throughout the country. Registrations happen at post offices and under the remit of police officials where, in addition to the biometrics, a photo is captured along with a signature and a number of biographic variables. These are typically sent by flash drive to a place with a server where they are sent to HQ using provincial fiber-optic lines. If the data pass the deduplication test, a card is printed and sent to the district which then sends it to the commune for final delivery to the individual. There are currently about 300,000 enrolments per year and around 13 million cards have been issued.<sup>16</sup>

The Khmer ID card is embedded with an Integrated Chip. The card is valid for 10 years. All the data fields that are captured by the Khmer ID system are stored in the integrated chip in an encrypted format.<sup>17</sup> Nonetheless, since the chip has never been utilized for any kind of authentication, the GDI aims to stop issuing these smart cards by 2028. However, recent news reports suggest otherwise including the possibility of a shift to a new (and potentially costly) technology (Vibol 2025).

An important recent development is the availability of authentication services offered by the GDI. Since 2020, there has been an online business registration process facilitated by an API which provides electronic know your customer (e-KYC) verification. By 2024, there were close to 30,000,000 authentications performed (testing the systems capacity). The system provides four levels of assurance ranging from scoring data fields (matching yes/no) to live detection (since 2025). Charges depend on the level of assurance.

Cambodia enacted a landmark Law on Civil Registration, Vital Statistics and Identification ('CRVS-ID Law, 2023'), guaranteeing 'a legal identity for all, which is essential to accessing education, health care, property, and many other benefits and social protections'. The CRVS-ID Law, 2023 applies to procedures relating to civil registration, residence registration, preparation of vital statistics, personal identity registration, organization and management of the population register (CRVS-ID Law, Article 1). The National Institute of Statistics of the Ministry of Planning is the primary regulatory authority to collect, process, and disseminate vital statistics (CRVS-ID Law, Article 100). The provisions of CRVS-ID Law incorporates purpose limitation, data sharing controls, and data security requirements.

Sub-Decree No. 252, 2021 empowers the Ministry of Interior as the entity responsible for collecting, compiling, and safeguarding ID data. Sub-Decree No. 252, 2021 applies to identification data that

---

<sup>14</sup> The average enrolment rate for national ID systems in lower middle income countries is 91 percent (Clark, Metz, & Casher 2022).

<sup>15</sup> The collection of digits follows a 4-4-2 process.

<sup>16</sup> This includes replacements for lost or damaged cards for which there is no charge.

<sup>17</sup> The technology used is from Dermalog and is proprietary, ie., GDI does not have access to the underlying software.

originates from civil registration, Khmer nationality identity cards, residence statistics and management, passports, nationality, and other registration records. It requires the Ministry of Interior to ensure data protection during transmission and usage “by applying high-level technical security standards” but delegates the specifics to proclamations by the Ministry.<sup>18</sup> A translation of Sub-Decree No. 252, 2021 is not publicly available for review.

## Functional IDs for Social Protection Programs

### The IDPoor based Equity Card

The most important social protection program in Cambodia dating back to 2007, is the targeted health insurance program. This program determined the eligibility for free health care through a household assessment based on a proxy means test aimed at determining poverty status known as the IDPoor.

Since 2019, the social protection sector has expanded both in terms of coverage as well as the kind of services provided. A national pension scheme was introduced in legislation in 2019 but implementation was delayed until 2023 due to the COVID-19 pandemic. During the pandemic, a cash transfer scheme was implemented using the IDPoor database. Between 2020 and 2024, the number of households deemed eligible for this emergency cash transfer increased (despite some households being removed) and by 2025, there are approximately 2.8 million people living in these households. The temporary transfer program is in the process of being converted into the ‘family package’ program which will continue to make somewhat smaller transfers to these households.

The IDPoor Data Protection Policy, 2022 established by the Ministry of Planning, provides a framework for protecting personal data to enable access to benefits such as social transfers, healthcare, and other targeted social services. The IDPoor Data Protection Policy, 2022 is a “framework document” which aims to ensure that data is collected, stored, and handled fairly and transparently while respecting human rights (IDPoor 2025a). It applies to all personal data processed within the IDPoor system, including beneficiary information (names, addresses, health status, poverty classification) and data user details, with the Ministry of Planning serving as the data controller (IDPoor 2025a).

Each household is issued an ‘Equity Card’ (see Figure 1) which proves their eligibility for the subsidized health insurance program and now, for the family package, cash transfer. The on-demand process that has been utilized until now is described in Box 3, although in-depth, field analysis revealed many deviations from the formal process<sup>19</sup>. In terms of identification, the registration process requested but did not require that applicants provide their foundational IDs.

---

<sup>18</sup> Based on summary and translation provided by consultant, Darlin Nay.

<sup>19</sup> Angkor Research (2021) found that in most cases the documented process was not followed with many cases where partial or no interviews took place.



[illegible]

### Box 3: The On-Demand Identification Process for IDPoor

The following steps presents a stylized summary of the OD-IDP process:

- <sup>20</sup> In the communes/sangkats that we visited officials noted that they maintain a list of potentially poor households and use this as a basis for encouraging program enrolment. These field visits were not nationally representative, however, so this finding is anecdotal.

Group for IDPoor will review the requests and decide to interview the household or not. This step is done solely at the discretion and judgement of the Commune Sangkat Working Group.

2. The communes collect data on the potentially poor families using smart devices (tablets) provided to each commune. The devices have a specific application pre-loaded with relevant data collection instruments. Use of smart devices not only makes the OD-IDPoor process faster, but also less prone to errors. An intuitive user interface, instructive error messages, logical skip patterns, and automatic score calculations help simplify the process and reduce errors. Local implementers have been trained to use the application. Pictures are taken of household members during the interview.
3. The tablets automatically determine beneficiary status. During Commune Sangkat Council Meetings the council members review the results attained from the household interviews. The Commune/Sangkat Council may decide to overrule the score attained based on special circumstances of the household. After a final status is determined: 'extremely poor' (IDPoor 1), 'poor' (IDPoor 2), 'at risk' or 'non-poor' the data is transferred to the national IDPoor database. The tablets are automatically synced with the national IDPoor database and the information is updated in real time.

{Source: World Bank 2021}

## National Social Security Fund Member Card

The NSSF now covers around two million individual workers as well as their dependents. Employers are responsible for registering their employees via a web portal, computer-based application, or a mobile app. Once the data is verified, the employees must visit one of the 35 NSSF branches and to provide biometrics, including a photo and fingerprints (two thumbs). A card is typically issued at the same visit with a QR code that confirms that it is a genuine card. The family book and birth certificates are collected to verify dependents. The Khmer ID is required for the employee.<sup>21</sup> There is also an option for self-enrolment using the NSSF app or website. However, an in-person visit would still be required for the collection of biometrics.

Figure 3 Cambodia's National Social Security Fund Card



<sup>21</sup> At the NSSF headquarters in Phnom Penh, there is an office of the GDI that can issue Khmer IDs.

The NSSF is one of the entities that has used the authentication system offered by the GDI/MOI to verify the information on the Khmer ID during their enrolment process. Data is sent to GDI for real time 1:1 matching and results are verified by a staff member. If a field does not match, the record is rejected. The NSSF may then work with GDI to correct any errors that have led to the rejection. This is done only for members, not dependents. This allowed for internal deduplication using the collected fingerprints but this was eliminated when biographic checks with GDI were instituted. Biometrics are not compared to GDIs database due to privacy concerns. In terms of authentication, the NSSF card is presented at the relevant desk in hospitals and clinics and is checked through the QR code. Fingerprints have been used for authentication on what appears to be a pilot basis.<sup>22</sup>

## Cambodia's Person with Disability (PWD) Card

The Department of Disability and Welfare, at the Ministry of Social Affairs, Veterans and Youth Rehabilitation (MOSVY) provides benefits to disabled persons. The 2019 census found over 678,000 persons with disability (PWD) in Cambodia. Since 2020, the DDW has registered 335,000 PWD and issued cards to approximately 300,000<sup>23</sup>. The remainder did not receive cards due to issues with biographic data or photo quality. The identity of the PWD is verified by one or more of three foundational ID documents, namely, the Khmer ID, the birth certificate or the family book. Where applicable, the IDPoor card is also verified. The documents provided are photographed for future reference.

The commune or sangkat official interviews the PWD and enters information into a 'Disability Identification app', usually on a smartphone. The data are sent to the provincial level and from there to the national level. The cards have a QR code that contains biographical details and verifies that it is a legitimately issued card. In the new 'Family Package' program, the card provides evidence of eligibility for the categorical cash transfer that goes to households that meet the poverty criteria. The PWD card can also be used for access to free rehabilitation services, disability hiring quotes and transportation (city buses).

*Figure 4 Person with disability card*



<sup>22</sup> There appear to have been attempts to pilot fingerprint-based authentication at the point of service (ie., clinics, hospitals) but this does not appear to have been scaled up and future plans are not clear.

<sup>23</sup> Cards began to be issued in 2023.

### *The National Social Assistance Fund (NSAF)*

The NSAF was created in 2022 to serve as the payment agency for social assistance benefits as well as civil service pensions. In 2025, in addition to more than 700,000 cash transfer beneficiaries, the agency is responsible for the payment of around 126,000 veterans and 80,500 civil service pensioners. The cash transfer recipients receiving payments are currently verified with their Equity Cards by the payment service provider.<sup>24</sup> However, the government intends to shift towards payments into transactional accounts. This would require robust identification that would be acceptable for KYC purposes for opening bank accounts.

Civil servants are identified using the Khmer ID prior to retirement and they are paid into bank accounts that have been opened after verifying their identities through standard KYC processes. However, in the case of pensioners, concerns about fraud or errors including unreported deaths has led the agency to start implementing biometric capture of two thumbs. These biometrics would be used for confirming proof of life.

## The Social Protection ID Initiative

### Objectives of the New System

The purpose of the **Social Protection ID**, or **SPID** is to provide a unique identifier that allows various social protection programs to (i) ensure that no beneficiaries appear multiple times in the same database, (ii) allows for authentication at the point of delivery of the benefits, and (iii) allows linking of administrative databases for monitoring and targeting purposes. These functions are typically performed by a foundational ID system such as the Khmer ID and, as discussed below, this may still be the optimal approach in the future. However, the SPID is meant to address several shortcomings of the foundational ID system that make it difficult to use for the implementation of social programs.

Specifically, there are at least three gaps in the foundational system that the SPID attempts to address. First, the fact that the civil registry is not digitalized means that there is currently no way to cross check the identification proof in the form of a birth certificate for children as they are not eligible for a Khmer ID. Second, there are significant gaps in coverage of the Khmer ID among the poor who are the main beneficiaries of the Health Equity Card and the Family Package. Third, although the MOI now offers authentication services, this does not include allowing programs to access key data points during registration due, it seems, to regulatory restrictions on access to this information. Finally, there are likely to be capacity problems in terms of the volume of authentication requests that the MOI-GDI system can handle.

These are superable problems and the MOI is already planning to address many of them. The recommendations below, if implemented would allow for an eventual shift towards the foundational ID but require significant investment that might otherwise delay the roll out of the DSPP and the

---

<sup>24</sup> The process for payments to the program for pregnant mothers is somewhat different and more complicated due to the conditions that must be met in order to receive the benefits.

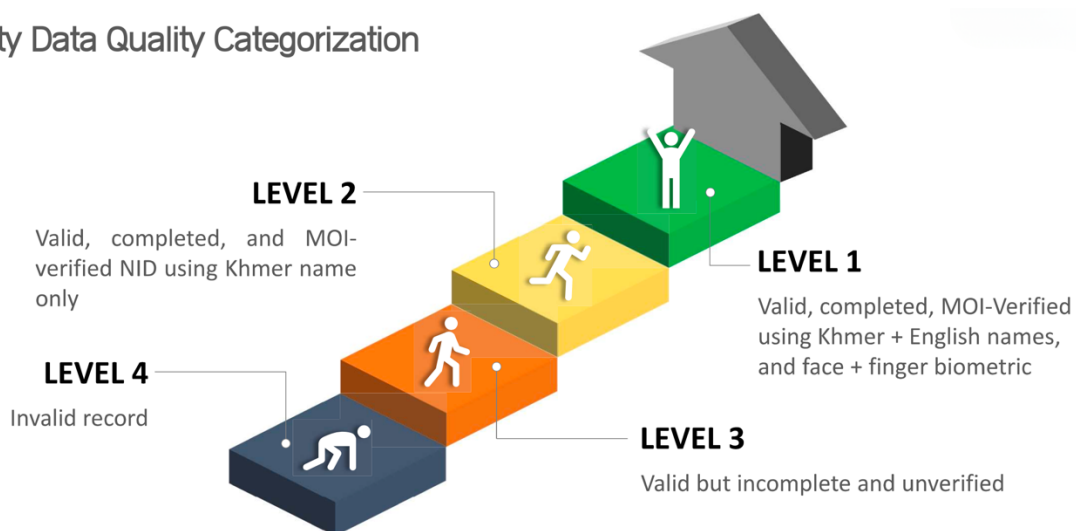
federated social registry. There are successful examples of this approach as in the case of Morocco as described in Box 4.

The starting point is the categorization of the quality of the ID of an individual beneficiary of one of the social protection programs. This recognizes the practical need for transition arrangements until all beneficiaries can reach the highest level of assurance (see Figure 5). The second level entails verification based on the MOI database. Most NSSF members fall into this category since the Khmer ID is required for registration. Many social assistance beneficiaries begin in categories 3 and 4. The new registration process for the family package, by far the largest SA program, can move these individuals to Category 1 as the SPID is issued for the first time.

At the core of the identity scheme is the use of biometric technologies, specifically facial and fingerprint recognition. These are used to capture biometric data during enrolment, ensure uniqueness through deduplication checks, and authenticate individuals when accessing services. This section emphasizes the importance of biometric data quality at the point of enrolment, as it directly affects the accuracy and reliability of subsequent biometric matching.

*Figure 5 Identification data quality ranking during transition period*

### Identity Data Quality Categorization



**Valid:** Khmer Name (First & Last), Date of Birth, Gender

**Completed:** Valid, Biometric, EngName, Address

#### Box 4: Morocco's National Population Register (NPR) and Social Register (SR)

When the Moroccan government launched the strategy to create the National Population Register (NPR), the civil registry was not digitized, and the national ID card, by its design, excluded minors and foreigners. This situation led to a proliferation of identifiers across social services, with systems that were not interoperable. The NPR and the Social Register (SR) were created to address this challenge and improve the identification and targeting of social programs.



Enrolment in the NPR allows for the collection of biometric data from citizens, including minors, and generates the civil and social digital identifier from birth (IDCS). The NPR is linked to the civil registry and the national identity card system to ensure optimal interoperability.

The Moroccan experience in identification systems highlights the importance of strong political support and the establishment of a solid legal and regulatory framework. The legal framework mandates enrolment in the NPR and obtaining the IDCS to access social programs and services. This has positioned the NPR as a first step in the delivery chain of social programs. In this sense, the SR was the first use case of the IDCS and serves as a single-entry point for social programs and provides a harmonized targeting system across social protection programs and services.

This complementary and coordinated approach enabled a rapid launch of the NPR and an increase in coverage rate during the first two years of implementation. Currently, the NPR covers more than 60% of the Moroccan population. It has also ensured the reliability and improvement of social programs. This dynamic was reinforced by the government strategy launched after the COVID-19 crisis to deeply reform social programs.

The additional costs related to the collection of biometric data were quickly amortized and pooled. Thanks to NPR and SR features (IDSC, scoring tools...), registration for the most important social programs in Morocco (representing more than 2.5% of GDP) is fully digitized and paperless. Programs collect a minimum of information during registration and recertification of beneficiaries' eligibility. Most of the information is collected via the interoperability platform, with exchanges facilitated by the IDCS.

## NSPC system architecture

The objective of implementing the SPID is threefold. First, it allows for deduplication of multiple databases so that they all recognize a particular individual as unique across the system. Second, it allows for data exchange across SP databases and eventually, with other administrative databases that can be useful in targeting (land registry, income tax, etc.). Third, it allows for 1:1 authentication. These functions are needed to implement the new, federated social protection registry. The 'social registry' is defined in the sub-decree on "Registration system harmonization and manage social protection data" as *'...an integrated registration database of the Royal Government, it stores data on social protection identity and socio-economic status data by creating a unique 10 (ten) digit social protection ID'*. A key element of the planned architecture is the Cambodia Data Exchange (CamDX), a unified data exchange layer or platform that enables services to identify individuals consistently across different platforms. By linking a harmonized unique identifier to service-specific IDs, CamDX ensures interoperability and a streamlined user experience.

Importantly, existing databases hosted by different government agencies will be maintained separately by each administrator.<sup>25</sup> This has the dual benefit of reducing the costs of 'plugging into'

---

<sup>25</sup> This is based on discussions with the NSPC. However, there appears to be some ambiguity in the sub-Decree, Article 8 which states that "GS-NSPC is authorized to verify, *store, manage*, develop, connect and secure social

the system as well as minimizing data aggregation<sup>26</sup>. Enrolment into supported services will be handled through a common portal, which presents users with a list of available schemes. While users enrol through a shared interface, each service retains operational independence, including its own mandates and data structures. The common system does not impose uniform data standards but rather acts as an interoperability layer, allowing diverse systems to connect and share identity information seamlessly. CamDX would eventually serve as the central mechanism for identity mapping.<sup>27</sup> This approach enables the identification of individuals across multiple services, supporting a unified management system and a single user portal for enrolment and access.

A key component of the new service is a centralized data repository, which will consolidate information previously stored within each individual service. This central repository will also include biometric data collected during enrolment.

An important element of the system is what data is stored centrally. This is ostensibly limited to a number of data fields related to identity including:

- Biographical data
  - Name, DoB, home address, family members etc.
- Biometric data
  - Face image
  - Fingerprint templates
- Transaction information

It is not yet clear how these data are protected at rest and during transit, either during an enrolment or when data is being used to either verify identity, perform deduplication checks, or for other purposes. The relevant safeguards and processes require further elaboration.

## Biometric capture process and use

The face and fingerprint enrolments are performed in local communes. Based on a small number of field visits, the location is general in the open air albeit covered, but relatively open to the elements. Lighting is by natural light meaning there is no control over illumination of subjects' faces which may cause biometric data issues. The space is not specifically designed for biometric data capture and there is no effort to provide a neutral background for face capture which may cause quality issues. There is a check made to ensure that there are not multiple people being captured in the photo and that there is only one face identified within the field of view.

---

protection data and social protection identity data, including demographic data and biometric data obtained from registration on NSPP and digital interaction between the databases of relevant ministries and institutions and the SR which registered social protection identity data must be verified with a common population identification system.” Emphasis added.

<sup>26</sup> Limiting data aggregation is useful for personal data protection in that it reduces the potential for both cyber attacks on the ‘honey pot’ database as well as making it more difficult to combine data on individuals for purposes to which they have not consented.

<sup>27</sup> Initially, a bespoke data exchange layer is being used due to limitations in the X-Road type system used by CamDX. Note that entities using CamDX will have to develop their own APIs to access the data sharing platform and achieve these benefits.

There are three main functions for biometrics in the scheme:

- Linking together records
- Deduplication checks for new enrolments
- Authentication of an individual against an existing record

Fingerprints are used for record linking and deduplication, face images are used to authenticate against an existing record. Fingerprint data collected by the different services up until now has varied quite considerably. The NSPC requirement is for the capture of two thumb prints from each individual. Meanwhile, the MOI Khmer ID scheme collects a full set of 10 prints; other schemes such as the NSAF and NSSF also collect two thumb prints. Also, it will be necessary to get confirmation of exception handling processes in the event either it is not possible to capture fingerprints of sufficient quality or individuals have missing fingers. Most, but not all, of the systems being brought together under the common portal collect fingerprint biometrics. It is understood that thumb prints are collected and no system uses fingerprints, aside from the MOI.

Deduplication in an identity system is the identification and removal of duplicate records in a database. The intention is to identify deliberate or accidental incidences when an individual who has already enrolled in the system attempts to enrol a second time. As such, it is important that any biometric modality that is used for deduplication is able to uniquely identify an individual in a population (possibly of the order of 10 million or more). It is important that the quality of biometric data captured for this purpose is high: poor quality biometric data (e.g. smudged fingerprints or blurred face images) will make it likely that matching errors will occur. Also, it is very challenging to perform deduplication in real-time, particularly for large populations and it requires significant computing resources to make this possible. These factors all need to be considered when implementing a deduplication function.

Deduplication of records uses fingerprints to identify existing records through comparison of prints captured during enrolment with existing records to identify where an individual has already enrolled. This process requires the biometric data to be able to match with sufficient accuracy to be able to uniquely identify an individual in the overall population enrolled in the system. This defines the first requirement of the biometric used in the identity scheme: it should provide the necessary accuracy to perform deduplication. The uniqueness of a biometric is often expressed in terms of *entropy*, expressed in *bits*, representing the amount of uncertainty or uniqueness in a system. For a single fingerprint, it is commonly estimated to be 10-20 bits, with a commonly accepted approximation of 13.3 bits for a single fingerprint (NIST 2004). Thus, for a system using two thumb prints, the entropy would be 26.6 bits.

It is possible to use this measure of entropy to estimate the theoretical maximum number of people that can be supported (Doddington et al 1998):

$$N \approx 2^H$$

Hence, for a system using 2 thumb prints, the maximum value of  $N \approx 2^{26.6}$ , or approximately 100 million individuals can be theoretically supported. However, this figure should be treated with



caution: it is a theoretical limit and there will be a number of factors including sensor noise, biometric errors, poor quality biometric data and biometric sampling errors will reduce the effective number of individuals that can be supported. Typically, a false acceptance rate of 0.01% is achieved for a fingerprint system using a single fingerprint - which translates to 0.02% for two fingerprints. It is advisable to use additional information to deduplicate a record if only two fingerprints are used: an additional biometric modality or biographical information can be used to augment an initial shortlist of possible matches and increase confidence in a deduplication decision.

In addition to broad operational and security criteria not directly related to the biometric functionality, a fingerprint system used in an identity system needs to:

- Be accurate enough to uniquely identify an individual within a population (for the Cambodian system this would be of the order of 18 million individuals)
- Biometric performance: errors (false non-match and false match rates) should be small enough for the use of the biometric system to be viable
- The biometric system is secure, particularly in relation to presentation attacks
- Only a very small proportion of the population are unable to provide suitable biometric data
- The biometric modality should be ubiquitous: all members of the population should possess the biometric modality
- It should be convenient and easy to use the technology
- Time to process a record to check for an existing entry in the database should be near real-time
- Biometric quality must be above a certain threshold to ensure data quality
- Capture equipment should be readily available at a realistic cost and is easy to use

It is very important to ensure that a biometric system selected meets the requirements. Evaluation of the system against these criteria is critical toward understanding functionality in the context of how the system is used. There are a number of standards that set out criteria for testing, notably ISO/IEC 19795 (Biometric performance testing and reporting), ISO/IEC 30107 (biometric presentation attack detection), ISO/IEC 29794 (Biometric sample quality). Performance testing should be tailored to the specific implementation and requirements of the system, reflecting how the biometric is captured, what it is used for and the environment in which biometric data is collected.

## The NSPC Biometric System

The approach to implementing biometrics by NSPC is fundamentally based on a combination of factors:

- Performance to meet the requirements of the identity system
- Cost effectiveness of the system
- Adoption of open source applications where possible
- Internal development of applications

The philosophy of approach has led to a number of key design and implementation decisions, notably the algorithms chosen for both fingerprint and face modalities. This in turn has a significant influence on how the system performs and whether it meets the requirements for the NSPC identity program.

Cost is a key factor in the design and implementation of the biometric functions: economic constraints on the system make it desirable to use freely available, open source libraries, functionality and applications. This is a desirable option, so long as it provides the necessary functionality in terms of matching accuracy and security. This is a very important consideration and, while there are clear benefits to implementing a biometric system that is not based on a commercially available product, particularly with respect to avoiding lock-in to a particular solution and providing a cost-effective solution, it is imperative that it performs as required, particularly in terms of matching accuracy for the particular population size that it is being used for.

A particular strength of the approach adopted by the NSPC is the development of internal capability. By using internal developers, the knowledge base in developing the system is retained by the department and provides a pool of knowledge and expertise. In addition, the functionality of the system used by the NSPC is well understood by the department and experts within the organization, consolidating the knowledge over the medium and long term: this is an aspect that is particularly important for the specific circumstances of the program.

The face biometric solution used by NSPC is based on feature extraction combined with an open source system for matching feature vectors: QDrant (QDrant 2025), an open source, vector matching system.

The enrolment process involves the capture of a face image, followed by the extraction of a feature vector to represent the particular individual.

An interesting innovation from the NSPC is the use of an open source database management system in the form of QDrant, an open source, vector database and similarity search engine. It is very important to understand the nature of this approach: rather than a closed system of biometric capture, feature extraction/template modelling and matching, the feature extraction/feature vector creation stage is distinct from the comparison stage. The QDrant solution is intended to be a flexible, generalized vector comparison application and it is in this context that it is used for matching a face feature vector from a biometric probe against the reference feature vector. This represents a novel approach to face biometrics: it has an advantage in that it is using a well-established vector search engine application but it is very unusual in that this is not the usual approach used for a face biometric system.

In addition to the face feature extraction and feature vector comparison, the face biometric solution includes a number of additional functions. Functions to perform image processing functions: performance face detection and alignment, face count to ensure only one face is present in the image captured, face image quality checking for blurriness and brightness are implemented using open source libraries but implemented by the NSPC technical team.

The face matching algorithm, using the QDrant vector comparison application, is ultimately based on the FaceNet (IEEE 2025) deep learning application from Google. It uses a deep convolutional neural network to extract feature vectors that are subsequently processed by the QDrant application. FaceNet is a leading open source CNN face recognition system/feature extraction system, making use of a particular learning approach to maximize the clustering of similar faces (i.e. from the same individual) while ensuring dissimilar faces are not matched. It is known to achieve a high level of accuracy in matching faces, with an emphasis on encoding face features into a feature vector. This is well matched for subsequent processing by an application such as QDrant.

Currently, the FaceNet face recognition system is using a standard, pre-trained solution which is not specifically trained for Khmer face structures or skin tones. This introduces some possible impact on the accuracy of the system and its ability to operate fairly across the population.

Some internal testing has been carried out with an **error rate of 95%** reported, being a combined measure of false positives and false negatives. However, this is not the usual convention for reporting accuracy: it would be expected that it would be expressed in terms of false match rate and false non-match rate in order to better understand the performance of the system in correctly matching individuals against their reference data as well as errors caused by non-mated<sup>28</sup> samples matching.

It is acknowledged by the project team that performance is not currently at required levels: it is intended to train the FaceNet model to be more representative of the Cambodian population and in the meantime additional biographical information is used to supplement the biometric matching decision.

The NPSC fingerprint system is based on two fingerprints: one taken from each hand, with thumb prints taken by preference over other digits. A total of 10 million fingerprint pairs are held in the database. It is noteworthy that, in contrast, the Khmer national identity scheme administered by the Ministry of the Interior captures a full set of ten prints from each individual.

Fingerprints are used to identify an individual and to access the system, i.e. it is used as a single factor identification against a record in addition as a deduplication check for new enrolments against existing records.

An open source automatic fingerprint identification system (AFIS) is used, mostly due to economic factors, with implementation performed and managed internally by the NPSC development team. Due to the fact that the system is not a commercial system, with the attendant levels of performance, it is necessary to perform a series of pre-processing filters on the data in order to attain the processing times necessary for the deduplication function of comparing newly acquired fingerprints against the overall database.

6 images from each person are collected during enrolment using a Secugen Hamster Pro 30 optical fingerprint scanner (SecuGen 2025). Multiple images are captured in order to increase the likelihood that a good quality image is captured amongst the 6. Fingerprint quality is assessed using the NFIQ quality tool (NIST 2024) and the highest scoring image is retained.

---

<sup>28</sup> i.e. samples from different people being incorrectly matched as from the same person

Images are processed to map fingerprint minutiae which is then passed through an AI model to produce a feature vector. The minutiae extraction process is performed using a standard open source library implemented by the NPSC development team. The feature vector produced by the AI model is processed by comparing it to data in the existing database to produce a subset of possible matches which are then processed for fingerprint matching. This step was deemed necessary due to a preference to avoid using a commercial system for cost reasons. The outcome of the intermediate processing of the data was to avoid a 1:N volume of comparisons (with N being of the order of 1-10 million which would incur significant processing overheads) and instead the fingerprint matching is performed on the top 1% of matches from the image processing stage.

The final matching of the input fingerprint against the matches from image processing stage is performed by a minutiae cylinder code algorithm, an open source application for matching minutiae templates. This approach supports large scale recognition tasks, albeit after the initial filtering stage.

Some limited testing has been performed on fingerprint data but only using synthetic fingerprints. Significant caution is needed when synthetic data is used: it is not widely accepted to be equivalent to using real data (i.e. data collected from humans) and it is not safe to base assessment of system performance on such data.

Off-line scenario testing using approximately 2000 fingerprint sets has been performed, from 300 people who have enrolled in the system, each providing 6 samples per finger/thumbs. This has a useful advantage in that it is real data collected in operational conditions.

The plan is to continue to develop the fingerprint solution, focusing on:

- Continuing the evaluation of the current system
- Fine tune the AI model used to process the minutiae
- Identify the optimum threshold for NFIQ fingerprint quality measures
- Research possible additional or alternative algorithms to use for matching

## Biometric Performance

The face biometric system is internally developed from a collection of open source applications and libraries, linking to an externally sourced non-expert feature vector application (QDrant). This is a relatively unusual approach to adopt for a national scale identity system: the cost implications of using a commercial system are a major factor in deciding the approach adopted. This will clearly have implications on how the system performs. Although it is possible to achieve the level of performance required for the effective delivery of required service levels (in terms of matching accuracy, speed of operation in particular) the use of open source libraries and an internal development team does not offer the depth of experience and expertise in successful delivery of a biometric system that would be expected in a proprietary system. It is not to say it is not possible to achieve the required levels of performance and functionality, but it makes testing of the system much more important in order to gain assurance that the system is fit for purpose.

Some testing has been performed on the system as implemented. An overall accuracy measure of 95% has been reported but without any context (size and demographic composition of test cohort,

test conditions, how images were captured and other test parameters) which makes it difficult to judge the significance of this figure. In addition, it is normal to report errors in terms of false match and false non-match (or false positives and false negatives as alternative nomenclature) which give a much better assessment of the overall performance of the system. It would also be useful to report additional measures such as failure to acquire and failure to enrol error rates as well as processing times in order to provide a full picture of system performance.

Similarly to the face biometric system, the fingerprint solution is implemented largely by internal development of open source applications and libraries, with the same challenges to the levels of performance that can be achieved as for the face system. The components are broadly available libraries that are used in a range of applications, particularly academic work and non-commercial solutions. This is not necessarily a reason to not use such an approach, but as per the face biometric system, it makes it very important to properly evaluate performance to ensure it is fit for purpose.

In terms of performance testing the system, some assessment using synthetic data has been made, but it is very important to understand the limited value of this and to not rely on this source of data. Over time it would be expected that the volume of data available to evaluate the performance of the system will increase as more people enrol in the system but it is important to consider the quality of that data, both in terms of the integrity of data within the database and data that is used to assess the performance of the system: if data quality is poor, then the identity system database is will not be effective in how it is used: there will be errors in matching with enrolled identities, deduplication functions will result in higher than acceptable errors and the system as a whole will not be able to be relied upon.

It is therefore important to perform quantifiable testing of the fingerprint system as soon as possible, in order to assess the effectiveness of the system as implemented and to ensure that data collected to date is of sufficient quality. There is a secondary benefit to performing testing of the fingerprint system (and the face biometric system as well) in that it should validate the approach taken by the development team in using open source and internally developed components, justifying the cost savings in adopting such an approach.

In addition to validating the open source approach of the project, it is also important to confirm if the use of two fingerprints per individual, rather than 8 or 10 as is commonly used in national identity schemes, results in the level of accuracy and discrimination between individuals to be able to perform the functions required (deduplication and identity authentication). In theory, two fingerprints should provide the necessary entropy to uniquely identify individuals in a population the size of Cambodia's, but in practice limits to fingerprint image quality and other factors may mean two prints is not enough.

## Part 2 Recommendations

As Cambodia's identification ecosystem continues to evolve and assuming that the SPID is scaled up to cover all social protection programs, the Government should consider a number of measures

to ensure that the system performs well and is financially sustainable. These measures can be usefully divided into short and longer term horizons.

### Foundational IDs

- *Digitalization of the civil registry and integration with the Khmer ID (short term)*

Perhaps the most important improvement to the system that can be implemented immediately is the digitalization of the civil registration processes, especially birth and death registration. To the extent that there are fiscal constraints, priority should be given to the flow of new registrations. That being said, it will be important and valuable to also create digital records for the stock of existing CRVS records. Without this, the population cannot realize the benefits of a digital system for several generations. This is not a new proposal and is already envisioned in the plans of the GDI and implemented in several provinces. Related to this is the integration with the Khmer ID which is also planned but not yet implemented. Experience from other countries suggests that the costs involved are not too high and the complete digitalization process can be achieved in a few years. The ultimate objective is a robust, unique ID from birth until death with universal coverage.

- *Achieving universal coverage of the Khmer ID (short term)*

As noted above, survey data suggest that recent efforts to expand coverage of the Khmer ID have been successful and achieved coverage rates in the 90+ percent range. However, as in most countries, the largest gaps are found among the lowest income groups (Clark, Metz, & Casher 2022). These also happen to be the main beneficiaries of social assistance programs like the Family Package. This program has now become Cambodia's flagship social assistance program making it possible to interact with this group on a regular basis. Efforts to coordinate with the GDI appear to be underway but could be further strengthened. More frequent mobile campaigns and outreach require modest additional financing. This group should also be exempted from any fees.<sup>29</sup>

- *Shift away from chip-based cards and introduction of digital ID (longer term)*

The current Khmer ID has a chip that has never been utilized and which adds to the costs of the system. Many countries have moved away from smart-card based ID systems due to high costs and the increasing ubiquity of mobile phones and QR code-based authentication. The Digital Government agency has already developed a digital ID (CamDigiKey) and over time and with better connectivity and increased smart phone penetration, this mode of authentication, including for on-line transactions, can be made widely available.

### Functional IDs

- *Harmonize and rationalize biometric capture processes (short term)*

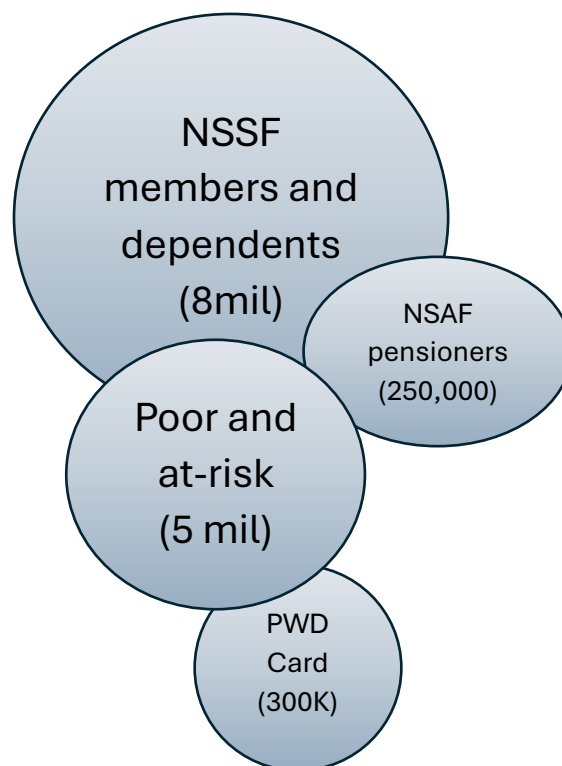
Currently, there are at least four government agencies collecting biometrics – the NSAF, NSSF, MOSVY and the IDPoor administered by the Ministry of Planning (MOP). As shown in the figure below,

---

<sup>29</sup> The recent sub-decree on Cambodian National Identity Cards (April 2025), Article 10, refers to the imposition of fees.

these programs combined cover roughly two-thirds of the population. There is some overlap between the populations covered by these programs (see Figure 6) and this overlap is likely to increase as Cambodia becomes an upper middle-income country and there are a growing number of households that move from one category or program to another. Moreover, the costs of biometric capturing devices and their lack of interoperability leads to unnecessary expenditures for the overall social protection system. The need to provide biometrics multiple times to different agencies also adds to the transaction costs of individuals. Consolidating procurement and maintenance of these systems across agencies and ensuring interoperability would reduce both costs.

Figure 6 *Coverage of functional IDs to be subsumed under SPID*



Note: Total Population = 17.4 million.

- *Test the NSPC biometric system (short term)*

In addition to the testing of the biometrics sub-systems, it is important to take account of the wider system in any evaluation, not least given the use of biographical information to confirm and valid biometric matching decisions. There are a number of good practice documents and digital identity guidelines that are relevant here. In particular, NIST's 800-63 suite of documents describing technical requirements for digital identity services offer a rich and deep source of information. Although it is specifically designed for the US government, there is value in understanding and applying the principles set out in the document set. It is particularly helpful in defining an approach to risk assessment and management that should inform and define what testing is required in order to gain and maintain assurance for the NSPC identity system.

- Testing outside the scope of the biometrics sub-system should focus on correlating biographical information and confirming it matches existing records, or records belonging to candidate identities in the case that a biometric match suggests there may be an existing record for an individual attempting to enrol.
- There is also a need to perform broad cyber security testing of the system, both the app used for enrolment and the database and back-end system. This is outside the scope of this report.
- These requirements apply to both the NSPC ID scheme and also the other ID schemes using the Cambodia Data Exchange API. Each of these will certainly need to have both biometric functionality and other components of their constituent systems evaluated in order to provide assurance across the ecosystem.
- Interoperability of the different systems should be evaluated. The biometric data captured by each system should be tested to ensure that it works across the different identity schemes and there are no incompatibilities that stop data being shared where required. This will include ensuring that differences in biographical data that is captured by different systems do not cause interoperability problems and that biometric data capture and processing by different systems are not incompatible with each other. This biometric testing will require the testing of sample data from one system against records held by other systems, in order to gain assurance that there is interoperability across the various identity schemes. This applies for both fingerprint and face modalities.

There are a number of standards that describe methodology and best practice for biometric testing. They cover performance testing which assesses the accuracy of a biometric system and security testing, with an emphasis on presentation attack detection (PAD). In addition to these main standards, there are additional standards that cover biometric data quality, biometric data interchange, biometric data quality and biometric enrolment. The standards that are relevant are:

- ISO/IEC 19795: Biometric performance testing and reporting
- ISO/IEC 30107: Biometric presentation attack detection
- ISO/IEC 29794: Biometric sample quality
- ISO/IEC 19794: Biometric data interchange formats
- ISO/IEC TR 29196: Guidance for biometric enrolment

There are a number of other standards and guidance documents that are also relevant to the development of an identity scheme, notably NIST 800-63 parts A and B, NCSC biometric guidance (NCSC 2019).

**ISO/IEC 19795** is focused on the performance testing of biometric systems. It provides a framework for the evaluation of the performance of a biometric system in terms of matching accuracy, speed and other measures. It describes the different types of testing (technology, operational and scenario modes), which metrics are important, how performance should be assessed including the definition of test protocols to conduct biometric performance tests (including test cohort composition, number of test subjects, test environment, and other factors). It also describes requirements for test reporting to ensure clarity and consistency in the reporting of biometric system evaluations.



**ISO/IEC 30107** is focused on presentation attack detection in biometric systems. Presentation attacks are a form of attack on biometric sensors using representation of biometric characteristics. These types of attacks are often known as spoofing attacks. Examples of these types of attacks include fingerprint overlays and photographic representations of faces.

**ISO/IEC 29794** is concerned with biometric sample quality. In the case of fingerprints, it is usual to use NFIQ and NFIQ2 to describe fingerprint capture quality. Face biometric systems have the OFIQ quality measure.

**ISO/IEC 19794** defines biometric interchange formats, providing a framework for storing, recording and transmitting biometric data.

**ISO/IEC 29196** is a technical report that provides guidance on the secure and usable implementation of biometric enrolment systems.

Of these standards, the most important to consider are ISO/IEC 19795 and ISO/IEC 30107 - performance and security are the key aspects of the biometric system that should be assessed and these standards provide the framework, methodology and best practice to evaluate them.

- *Introduce personal data protection regulations (short term)*

The DSPP provides the Government with a powerful tool for monitoring social programs. The intention is to eventually go beyond linking the SP databases so that the system can draw from various administrative databases which can be used for better targeting. This approach – used in advanced social protection delivery systems in countries like Chile and Turkey – helps minimize the costs and delays associated with data collection. Good international practice requires that individuals should consent to the use of their data for these purposes and this is explicitly stated in the sub-decree on data management<sup>30</sup>. This, and other aspects of personal data protection, requires a regulatory regime and an entity that enforces it. At present, there is no national data protection law in Cambodia, although one is being drafted. In the interim, a sectoral approach may be necessary. The NSPC and its members can issue such regulations until such time as national legislation is in place. International standards and good practice examples are available so that the NSPC does not have to reinvent the wheel (World Bank 2017). Robust personal data protection helps build trust in the overall system.

- *Convergence of identification services (longer term)*

There is an emerging consensus that government agencies using shared infrastructure is more efficient than a siloed approach. The concept of digital public infrastructure (DPI) includes data sharing, digital payments and identification system platforms, all of which are relevant to the DSPP. In the longer term, the Government should consider moving to a DPI approach in each of these areas. In the case of data sharing, the CamDX platform is already available and the NSPC plans to utilize it for data exchange. Similarly, the Bakong digital payment rails allow for all government to person (G2P)

---

<sup>30</sup> Article 5 says, “Ministries, institutions, and stakeholders must ensure that no social protection identity and socio - economic status data is shared with any natural person or legal entity without the consent of the original data owner.”

payments to flow from the Treasury directly to any bank account in contrast to the current bilateral arrangements that each agency has with specific banks.

Typically, the authoritative source of identity in a country is the national ID. In at least 60 countries around the world, the NID utilizes biometric deduplication to ensure uniqueness (Casher, Metz, & Clark 2023). This is not a trivial task and requires significant funding and expertise. While there are examples of functional biometric IDs operating in parallel, these are often criticized as incurring unnecessary expenses. For this reason, most countries have sooner or later harnessed the foundational ID to address the needs of multiple sectors including social protection. In Thailand, for example, the national ID is used to apply for social programs and serves as a financial address for payments. It is also used to link administrative databases for the purpose of targeting benefits to lower income groups. During COVID-19, this made it possible to have on-line applications for emergency relief allowing one of the fastest government responses to the crisis globally.

Some countries however, have found it difficult to integrate the foundational ID into social protection programs either due to gaps in coverage or the lack of a clear mandate. This was the case of Viet Nam until 2023 when a decree was issued mandating the agency responsible for the NID to work with line ministries and provide authentication services. Until then, each program issued its own form of identification. After the change in policy, the NID replaced the health insurance card and digitalized birth registrations are immediately reported to Viet Nam Social Security agency so that the newborn child is covered from birth. The foundational system has almost universal coverage.

Robust identification is crucial for SP programs, so in the absence of the foundational ID, countries have sometimes introduced biometric forms of ID for their social programs. Morocco is an example. The NID is administered by the Ministry of Interior and for reasons related to national security, is not accessible to other government programs. Instead, an additional layer has been added where uniqueness (identity-proofing) is rooted in the deduplication performed by the MOI but authentication and data exchange depend on this layer. This experience holds lessons for what is unfolding in Cambodia with regard to the SPID.

Following the short-term consolidation of biometric functional IDs recommended above, there are at least two options for the long run institutional arrangement for administering the SPID. The first would be for the MOI/GDI and the SPID to converge. In this scenario, the Khmer ID would eventually replace the SPID (as in the case of Viet Nam) and the GDI would provide the authentication services required by the various social programs. This would eliminate the duplication of biometric data collection. However, this would require a major shift in the institutional mandate and resources of the GDI.

Alternatively, the Moroccan approach<sup>31</sup> was to set up two new institutions, the Unified Social Registry and the National ID Agency. The USR was responsible for implementing the federated social registry that drew information from different administrative databases as needed for targeting and eligibility determination. The NIA administered the Unique ID Number (UIN) which was used by different social

---

<sup>31</sup> This was implemented with the support of a World Bank project. See World Bank 2025.

programs and was effectively universal. As in the case of Cambodia's SPID, the identify-proofing was rooted in the national ID administered by the MOI. Authentication services and interoperability were ensured by the integration of the UIN into all the relevant databases under the NIA.

In both cases, the government recognized the need to institutionalize identification services under appropriate legislation and regulation and to set up a robust governance framework. The policy was based on the need for the NIA and USR respectively, to focus on their core activities. In this sense, the model is similar to other countries where the identification and targeting functions are handled separately, each requiring dedicated staff and resources. To our knowledge, no country has an institutional arrangement where both functions are performed by the same entity.

### Summary and conclusions

As has been the case in many countries, a desire to improve the delivery system for social protection programs has been the main driver behind the current attempts to transform Cambodia's identification system.<sup>32</sup> The proposed Social Protection ID (SPID) has the potential to provide the growing SP programs a unique identifier that should allow harmonization of identity across programs and interoperability for data sharing. Eventually, the SPID can be leveraged to implement a federated social registry similar to what the most advanced countries in this area have achieved. Putting such a system into place, along with the legal and technical safeguards needed, will set Cambodia on a firm footing as its programs mature and coverage (especially social insurance) expands to cover most or all of the population.

It will be important to avoid duplication of costs, both in terms of transaction costs for beneficiaries and costs of equipment and manpower for administrators by fully replacing functional IDs with the SPID. However, in contrast to most advanced SP systems, the current approach does not rely directly on a foundational ID and, as a result, some degree of duplication is inevitable. While there may be advantages in separating the authentication layer of the system once unique identities are established (and even moving further to a federated system of authentication), there is little to gain from the parallel processes and the recurrent costs of collecting biometrics for both the SPID and the Khmer ID. These costs are not trivial as has been seen in countries with multiple biometric systems.<sup>33</sup> There are two options; first, to converge the two systems over the long run or to set up a new agency that would be responsible for managing the SPID. In either case, the current arrangement with the sub-Committee of the NSPC as implementing agency should be seen as an interim arrangement.

In the meantime, and prior to scaling up nationally, this note has highlighted the need for rigorous testing of the technology being used to collect biometric data from millions of Cambodians. The mass implementation should follow successful testing in the field and the training and supervision required to ensure that the technology is being applied appropriately.

---

<sup>32</sup> Other examples in Asia include India's Aadhaar and the Philippines, Philsys.

<sup>33</sup> A number of African countries (e.g., Ghana, Nigeria) have experienced high costs due to parallel biometric systems including where the national ID and the voter ID are managed separately.

# Part 3: Legal & Regulatory Framework Assessment

## I. Introduction

**This note analyzes the Sub-Decree on Harmonization, which governs the DSPP and SR, and other regulations in Cambodia governing Digital ID against international best practices relating to governance of Digital ID Programs.** International best-practices, including the World Bank's ID Enabling Environment Assessment, emphasize that data protection must be embedded from the outset, with clear legal authority, defined institutional mandates, and mechanisms for independent oversight and redress (World Bank 2017). In Cambodia, the rapid expansion of digital ID programs and the introduction of DSPP and the SR underscores the urgent need for comprehensive data protection laws. While recent policies and sub-decrees address aspects of data management and security, significant gaps remain in areas such as purpose limitation, data minimization, user rights, and independent monitoring and enforcement. Without these safeguards, the DSPP and the SR risk undermining public trust, exposing citizens to misuse of their data, and facing legal challenges that could jeopardize program sustainability. This analysis reviews Cambodia's digital ID legal landscape, benchmarks existing frameworks against international standards, and identifies critical reforms needed to ensure that the Digital Social Protection Platform and the Social Registry are inclusive, and foster trust.

**This note is structured as follows.** Part II provides an overview of international best practices for the regulation of Digital IDs, including the World Bank's ID Enabling Environment Assessment. Against this backdrop, Part III analyzes the legal and regulatory frameworks for digital ID schemes in Cambodia, such as the Law on Civil Registration, Vital Statistics and Identification, 2023, the Sub-Decree No. 252 on the Management, Use, and Protection of Identification Data, 2021, and IDPoor Data Protection Policy. This analysis is crucial to find out whether any existing Digital ID policies in Cambodia can serve as best practices for Sub-Decree No. 38 on Harmonization. Part IV benchmarks Sub-Decree No. 38 on Harmonization of the Social Protection Registration System and Data Management, 2024 for gaps with international best practices for the regulation of Digital IDs. Part V provides recommendations for amendments to Sub-Decree No. 38.

## II. Overview of Best Practices for Regulation of Digital IDs

**Privacy protections in Digital ID systems are crucial to foster inclusiveness and trust.** The World Bank's ID Enabling Environment Assessment ('IDEEA') prescribes the following principles for the protection of privacy for the effective governance of digital ID systems:

- (a) Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.
- (b) Establishing clear institutional mandates and accountability.
- (c) Enforcing legal and trust frameworks through independent oversight and adjudication of grievances (World Bank 2017).

**These principles are achieved through data protection laws that provide mandatory obligations on the processing and collection of data (World Bank 2019).** ID systems should be underpinned by legal frameworks that safeguard individual data, privacy, and user rights. Many countries have adopted general data protection and privacy laws that apply not only to the ID system, but to other government or private-sector activities that involve the processing of personal data. In accordance with international best practices, these laws typically have broad provisions and principles specific to the collection, storage and use of personal information, including:

- (a) Purpose limitation. The collection and use of personal data should be limited to purposes: (i) which are stated in law and thus can be known (at least in theory) to the individual at the time of the data collection; or (ii) for which the individual has given consent.
- (b) Proportionality and minimization. The data collected must be proportionate to the purpose of the ID system in to avoid unnecessary data collection and “function creep,” both of which can create privacy risks. This is often articulated as requiring that only the “minimum necessary” data should be collected to fulfil the intended purpose.
- (c) Lawfulness. The collection and use of personal data should be done on a lawful basis, e.g., involving consent, contractual necessity, compliance with legal obligation, protection of vital interests, public interest and/or legitimate interest.
- (d) Fairness and transparency. The collection and use of personal data should be done fairly and transparently.
- (e) Accuracy. Personal data should be accurate and up-to-date, and inaccuracies should be expediently corrected.
- (f) Storage limitations. Personal data should not be kept longer than is necessary for the purposes for which it is collected and processed.
- (g) Privacy-enhancing technologies. Requirements to use technologies that protect privacy (e.g., the tokenization of unique identity numbers) by eliminating or reducing the collection of personal data, preventing unnecessary or undesired processing of personal data, and facilitating compliance with data protection rules.
- (h) Accountability. The processing of personal data in accordance with the above principles should be monitored by an appropriate, independent authority, and by data subjects themselves.

Finally, users should have certain rights over data about them, including the ability to obtain and correct erroneous data about them, and to have mechanisms to seek redress to secure these rights.

**These principles are effectively enforced through independent oversight and enforcement.**

Data protection and privacy in general, and with respect to ID systems, are often subject to the oversight of an independent supervisory or regulatory authority to ensure compliance with privacy and data protection law, including protecting individuals’ rights.<sup>34</sup> The supervisory authority may handle public complaints. In terms of remedies, the authority may have the power to oblige the ID system to rectify, delete or destroy inaccurate or illegally collected data (World Bank 2019).

---

<sup>34</sup> See, for instance, provisions establishing data protection authorities in EU General Data Protection Regulation 2016/679; Sri Lanka Personal Data Protection Act 2022; Nigeria Data Protection Act 2023.

**Countries which have not incorporated principles as binding rules have subsequently faced challenges in implementation and data security.** For instance, Pakistan established the National Database and Registration Authority, 2000 ('NADRA'), to establish an improved and modernized system of registration along with "regulations for the due security, secrecy and necessary safeguards for protection and confidentiality of data and information contained in the registration and database systems" (Pakistan NADRA Ordinance, Section 7(j)). However, NADRA never enacted such binding protections, which may have contributed to systemic vulnerabilities (NADRA Pakistan 2025) that led to a breach which exposed the biometric and personal data of 2.7 million citizens (Ghulam 2024). India's digital ID system 'Aadhar' was also implemented without legal protections, which subsequently led to judicial challenges which threatened to upend the nationwide program (**Box 1**). India's experience with Aadhar may be particularly relevant for Cambodia, since like India, Cambodia too has a constitutional right to privacy, thereby making digital ID regulations vulnerable to potential constitutional challenges before courts.

**Box 1: India's Digital ID system and the 'Build Now, Legislate Later' Approach**

India's digital ID system 'Aadhaar' is a nationwide personal identification scheme based on which each resident is assigned a random 12-digit number by the Unique Identity Authority of India on the basis of biometric and demographic data. It is considered one of the most sophisticated biometric ID schemes. However, no personal data protection law was in place when Aadhaar commenced in 2009, raising privacy concerns and criticism. The 'build now, legislate later' approach resulted in claims in the Supreme Court of India. In August 2017, the Supreme Court found that the right to privacy is a fundamental right protected by the Indian Constitution. The following year the Supreme Court issued a majority judgment examining whether certain aspects of the Aadhaar ID system violated this right, noting the importance of balancing the fundamental right to privacy with fundamental rights "to food, shelter and employment." They held that mandatory use of the Aadhaar system to receive subsidies, benefits and services "whereby Government is doling out such benefits which are targeted at a particular deprived class" did not amount to a violation of the right to privacy.

Source: Justice Puttaswamy v. Union of India, Writ Petition (Civil) No 494 of 2012, Supreme Court of India, judgment delivered on 24 August 2017.

**Digital ID schemes with mandatory data governance requirements have provided users with recourse against data breaches.** India's policies relating to data sharing in the health sector incorporate privacy protections, data subject rights, and institutional oversight (National Health Authority of India 2012; Yojana 2022), and have seen widespread enrolment, although there is still scope for improvement on data breaches. Nigeria's experience also illustrates the importance of adopting comprehensive data protection regulations. Nigeria's National Identification Number system was implemented through the National Identity Management Commission (NIMC) established by the NIMC Act of 2007 (Nigeria NIMC Act 2007), well before the country adopted comprehensive data protection legislation in 2023. However, apart from the right to access personal

data, and a few sectoral regulations addressing data protection aspects,<sup>35</sup> no comprehensive data protection rules were introduced (Ogunmokun n.d.). Even though mandatory Digital IDs saw increased uptake from 2014, they lacked critical security protocols making them vulnerable to breach by cybercriminals due to the absence of comprehensive cybersecurity and data protection regulations (Ogunmokun n.d., p. 31). In 2019, the National Information Technology Development Agency ('NITDA') enacted the Nigerian Data Protection Regulation (NITDA 2019) which covered key issues such as data processing principles, lawful bases, data 'subjects' rights, cross border data flows, and enforcement mechanisms. Between 2019-2020, NITDA resolved 790 complaints, and conducted 15 investigations into alleged data breaches (Ogunmokun n.d., p.28). Therefore, the introduction of mandatory data governance requirements, with clear institutional mandates and enforcement can significantly contribute to fostering trust in digital ID systems.

### III. Analysis of Legal and Regulatory Safeguards in Cambodia's Digital ID Systems

**Cambodia lacks a cross-sectoral data protection legislation, and the draft law may have significant gaps with international best practices.** Led by the Ministry of Post and Telecommunications (MPTC), key areas covered by the draft law include data processing principles, responsibilities of data controllers and processors, data subject rights, cross-border data transfers, enforcement mechanisms, and penalties. The draft is not publicly available, but as per analysis from stakeholders, it has significant limitations, including (Greenleaf 2025):

- (a) Limited scope with provisions only applying to the private sector;
- (b) Restrictive cross-border data transfer provisions with data localization requirements;
- (c) Excessive delegation to ministerial regulations or 'Prakas'; and
- (d) Enforcement and monitoring powers vested in the MPTC, which is not administratively or financially independent of the government.

Therefore, even if the current draft of data protection legislation is adopted, there will still be substantial gaps with international best practices.

**The governance of digital IDs is fragmented due to the operation of various Digital ID programs (NSPC 2024) and the absence of cross-sectoral data protection legislation.** Cambodia has various Digital ID programs targeting different demographics which are governed by their own policies and rules and enforced by different ministries. Official translations of these policies are not available. Significant policies, in chronological order, include:

- (a) The Sub-Decree No. 252 on the Management, Use, and Protection of Identification Data, 2021 ('Sub-Decree No. 252, 2021') governs personal identification data managed by the Ministry of Interior but does not extend to identification data held by other entities;
- (b) Cambodia's poverty identification system, IDPoor, which is governed by the Data Protection Policy, 2022 published on its website;

---

<sup>35</sup> Appraisal of Nigeria legal and regulatory assessment for the proposed ID4D Project (P167183) (On file).

- (c) In July 2023, Cambodia enacted a landmark Law on Civil Registration, Vital Statistics and Identification ('CRVS-ID Law, 2023'), guaranteeing 'a legal identity for all, which is essential to accessing education, health care, property, and many other benefits and social protections';
- (d) The Sub-Decree No. 38 on Harmonization of the Social Protection Registration System and Data Management, 2024 ('Harmonization Sub-Decree') establishes a legal framework for the integration and management of social protection data systems in Cambodia through the Digital Social Protection Platform ('DSPP') and the Social Registry ('SR').

**Sub-Decree No. 252, 2021 empowers the Ministry of Interior as the entity responsible for collecting, compiling, and safeguarding ID data but lacks data protection safeguards.** Sub-Decree No. 252, 2021 applies to identification data that originates from civil registration, Khmer nationality identity cards, residence statistics and management, passports, nationality, and other registration records. It requires the Ministry of Interior to ensure data protection during transmission and usage "by applying high-level technical security standards" but delegates the specifics to proclamations by the Ministry.<sup>36</sup> A translation of Sub-Decree No. 252, 2021 is not publicly available for review.

**The IDPoor Data Protection Policy, 2022 established by the Ministry of Planning, provides a framework for protecting personal data to enable access to benefits such as social transfers, healthcare, and other targeted social services.** The IDPoor Data Protection Policy, 2022 is a "framework document" which aims to ensure that data is collected, stored, and handled fairly and transparently while respecting human rights (IDPoor 2025a). It applies to all personal data processed within the IDPoor system, including beneficiary information (names, addresses, health status, poverty classification) and data user details, with the Ministry of Planning serving as the data controller (IDPoor 2025a, Article 1).

**Unlike any other Digital ID regulation in Cambodia, the IDPoor Data Protection Policy, 2022 incorporates six fundamental data protection principles:** purpose specification (limiting data use to providing social services to the poor); fairness, lawfulness and transparency (requiring informed consent); data minimization (collecting only necessary information); confidentiality and security (implementing protective measures); retention limitation (storing data only as long as necessary); and accuracy (maintaining correct and updated information) (IDPoor 2025a, Article 5). It also establishes rights for data subjects, including access to their information and correction of inaccuracies, while requiring third-party data users to sign data sharing agreements (IDPoor 2025a, Articles 6,8). The policy is enforced through a complaint response mechanism via the Public IDPoor App, staff confidentiality requirements, and the appointment of a data protection focal person responsible for implementation (IDPoor 2025a, Articles 9,10).

**The CRVS ID Law, 2023 has purpose limitation and data security protections, but its provisions may not be applicable to the DSPP and SR.** The CRVS-ID Law, 2023 applies to procedures relating to civil registration, residence registration, preparation of vital statistics, personal identity registration, organization and management of the population register (CRVS-ID Law, Article 1). The

---

<sup>36</sup> Based on summary and translation provided by consultant, Darlin Nay.



National Institute of Statistics of the Ministry of Planning is the primary regulatory authority to collect, process, and disseminate vital statistics (CRVS-ID Law, Article 100). The provisions of CRVS-ID Law incorporates certain data protection safeguards:

- (a) **Purpose Limitation and Data Sharing Controls:** The disclosure or dissemination of the personal data in the registers under the CRVS ID Law is subject to authorization by ‘law, regulation or decision of the Minister of Interior’ (CRVS-ID Law, Article 150, 156, 161). The authority of public officials to use personal identity data is limited to only personal identity data necessary for the performance of their public functions (CRVS-ID Law, Article 161). The transmission of personally identifiable information (like names) to the National Institute of Statistics is prohibited (CRVS-ID Law, Article 102).
- (b) **Data Security Requirements:** Personal identity data registered into Khmer identity card record must be maintained in a manner that is secured and protected (CRVS-ID Law, Article 135, 160).

**Therefore, Digital ID regulations in Cambodia have substantial gaps with international best practices, and no existing regulation can serve as a best practice for Sub-Decree No. 38.** As stated above, Cambodia lacks a cross-sectoral data protection legislation and the current draft does not apply to the public sector, restricts cross-border data flows, and lacks an independent data protection authority.

- (a) Sub-Decree No. 252, 2021 only contains provisions relating to data security but delegates the framing of specific requirements to the Ministry of Interior.
- (b) The CRVS ID Law, 2023 has provisions relating to purpose limitation, data sharing, and data security, but lacks provisions regarding data subject rights and other important principles of data protection (transparency, fairness).
- (c) Compared to all other legal instruments, the IDPoor Data Protection Policy, 2022 incorporates six important data protection principles, provides for certain data subject rights, and appoints an authority for implementation. However, the IDPoor Data Protection Policy, 2022 is a ‘framework document’ which is published on its website, rather than being a Sub-Decree, which may impact its enforceability and reliability.

This summary forms important context for the next section which will analyze the Harmonization Sub-Decree which governs the DSPP and SR.

## IV. Analysis of Legal and Regulatory Safeguards in the Harmonization Sub-Decree

**The Harmonization Sub-Decree aims to establish the DSPP to minimize duplication and fragmentation of social protection data, and the SR for identification and registration of beneficiaries.** The National Social Protection Council (‘NSPC’) is designated as the primary authority responsible for leading and managing both the DSPP and SR. Its General Secretariat coordinates operations in collaboration with relevant ministries and institutions. From a data protection perspective, the Harmonization Sub-Decree includes a few important provisions:

- (a) Data sharing restrictions: Ministries and institutions must ensure that ‘no social protection identity and socio-economic status data is shared with any natural person or legal entity without the consent of the original data owner’ (Harmonization Sub-Decree, Article 5).
- (b) Data verification requirements: All social protection identity data must be verified against the national ID system of the Ministry of Interior ‘to ensure consistency and accuracy’ (Harmonization Sub-Decree, Articles 8, 12).
- (c) Data security obligation: The use of social protection identity data ‘must ensure the security of data and the confidentiality of personal privacy’ (Harmonization Sub-Decree, Article 14).
- (d) Transaction records: All transactions and data synchronization between systems must ‘make electronic records of all transactions to ensure security, consistency and inclusiveness of data’ (Harmonization Sub-Decree, Article 5).

**When assessed against the IDDEA principles and international best practices, the Harmonization Sub-Decree reveals several significant gaps.** The Harmonization Sub-Decree lacks data protection safeguards, even when compared to Cambodian digital ID policies. Provisions of the CRVS-ID Law, 2023 and the Sub-Decree No. 252, 2021 may be applicable to the personal data processed in the DSPP and SR due to the wide range of personal data that are covered under these policies. However, since different Ministries are responsible under the Harmonization Sub-Decree, CRVS-ID Law, 2023 and the Sub-Decree No. 252, 2021, the application of data protection safeguards in those policies to the DSPP and SR is doubtful. Gaps between international best practices and the Harmonization Sub-Decree are as follows:

- (a) Purpose Limitation and Data Minimization: The Harmonization Sub-Decree lacks clear provisions for purpose limitation and data minimization. It does not:
  - Require that data collected be proportionate to stated purposes;
  - Limit collection to minimum necessary data; and
  - Prevent “function creep” where data collected for one purpose is used for others.
- (b) Storage Limitations: The Harmonization Sub-Decree contains no provisions regarding data retention periods or deletion requirements. Without storage limitations:
  - Data may be kept indefinitely, increasing security risks;
  - Outdated or irrelevant data may accumulate in the system; and
  - Individual rights to erasure or deletion remain unaddressed.
- (c) Independent Oversight: One of the most critical gaps is the absence of independent oversight. The IDDEA principles emphasize “enforcement of legal and trust frameworks through independent oversight and adjudication of grievances”, yet:
  - The NSPC both operates the system and oversees itself;
  - No independent data protection authority exists; and
  - No specific mechanisms for individual complaints or appeals are established.
- (d) Privacy by Design and Security Standards: The Harmonization Sub-Decree makes only general references to data security without establishing specific requirements or standards. It fails to:

- Incorporate privacy-by-design principles;
- Require privacy impact assessments;
- Mandate specific security measures or breach notification procedures; and
- Establish technical standards for data protection.

(e) Data Subject Rights: The Harmonization Sub-Decree does not articulate rights for individuals whose data is collected, such as:

- Right to access their data;
- Right to rectification of inaccurate data;
- Right to object to processing;
- Right to erasure; and
- Right to data portability.

**Consolidation of multiple databases containing personal data may create significant additional privacy challenges, which can be addressed by a data protection impact assessment.** Unlike other Digital ID schemes in the past, SR and DSPP seek to integrate social protection data systems which may lead to specific privacy risks. The retention and analysis of huge amounts of personal data may lead to identification of patterns or ‘profiling’ of specific individuals (Article 29 Working Party, 2014.). At its core, consolidation of databases threatens compliance with fundamental principles of data protection, which dictate that processing of personal data be limited to what is adequate, relevant and necessary for the purpose for which data was collected.<sup>37</sup> When data processing activities are likely to result in a high risk to the privacy of individuals, then data controllers are usually required to carry out a ‘data protection impact assessment’ under international best practices (‘DPIA’) (EU 2018, Article 35; Sri Lanka Personal Data Protection Act 2022, Section 24; Article 29 Working Party 2017). Data protection authorities around the world recognize the combination of databases as one such ‘high risk’ data processing activity (Irish Data Protection Commission 2019). A DPIA usually requires the data processor to conduct the following assessments *before* carrying out an activity that poses a high risk to the privacy of individuals:

- (a) a systematic description of the data processing operations and their purposes;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risks to the rights of the individuals as per international best practices; and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data.

---

<sup>37</sup> See, for instance, formulation of data minimization principle in EU 2018, Article 5.

## V. Part 3 Recommendations

**Based on the analysis, the following reforms are recommended to strengthen the data protection safeguards in the Harmonization Sub-Decree to foster inclusiveness and trust in the DSPP and SR:**

- (a) Purpose limitation: Add explicit provisions requiring that data collection and processing be limited to specified, legitimate purposes related to social protection program administration.
- (b) Data minimization: Include requirements that only necessary data be collected, with criteria for determining necessity based on specific program objectives.
- (c) Storage limitations: Establish maximum retention periods for different categories of data, with requirements for secure deletion after expiration.
- (d) Individual rights: Articulate specific rights for data subjects, including access, rectification, and objection to processing in certain circumstances.
- (e) Data sharing: Sharing of personal data should be restricted only for the purposes for which the personal data was collected at the first instance. Data sharing for any other purposes, should trigger a fresh requirement to obtain consent.
- (f) Independent grievance mechanism: Create an independent body or process for addressing complaints related to data handling, separate from the operational functions of the NSPC.
- (g) Security standards: Specify minimum security standards for data storage, processing, and transmission, including encryption requirements for sensitive data.
- (h) Breach notification: Add provisions requiring notification to affected individuals and relevant authorities in case of data breaches.

The IDPoor Data Protection Guidelines may be referenced as a template for provisions for data subject rights, and fundamental principles of data protection.

**A revised Harmonization Sub-Decree may be introduced which revokes the current version and incorporates data protection safeguards.** As stated above, the current version of the Harmonization Sub-Decree makes it difficult to provide a level of privacy protection consistent with international best practices. To introduce additional data protection safeguards, individual rights, and an independent grievance redressal mechanism, the Harmonization Sub-Decree should be revoked and replaced by a new Sub-Decree. If revocation of the existing Harmonization Sub-Decree is not possible, then the Harmonization Sub-Decree may be amended to include more data protection safeguards and replace individual provisions.

**A DPIA should be conducted on the DSPP and SR so that the NSPC can implement legal, technical, and organizational safeguards to address privacy risks arising from integration of databases.** The assessment does not need to be commensurate with the level of detail of a full Data Protection Impact Assessment under the EU GDPR or comparable legislation. However, the DPIA should provide a level of detail that is sufficient to identify key compliance gaps and areas in which data protection can be enhanced, as well as the risks that these gaps may create in the use of the DSPP and SR. The ‘impact’ in a DPIA reflects the outcome of the materialization of a particular risk to the rights and freedoms of an individual. When determining the expected impact of a risk, it is

essential to consider that the consequences of a specific risk may be of very different nature, such as financial harm, psychological distress, or the impossibility to exercise a specific right or to access essential services.<sup>38</sup> Once such impacts are identified, the NSPC may identify and implement legal, technical and organizational safeguards which address the implications of specific privacy risks. A non-exhaustive list of such safeguards includes:

- (a) Deciding not to collect or store particular types of personal data.
- (b) Putting in place strict retention periods, designed to minimize the length of time that personal data is retained.
- (c) Reviewing physical and/or IT security in GS-NSPC or for a particular project team and making appropriate improvements where necessary.
- (d) Conducting general or project-specific training to ensure that personal data is handled securely.
- (e) Creating protocols for the handling of personal data within the project and ensuring that all relevant staff are trained in operating under the protocol.
- (f) Producing guidance for staff as reference point in the event of any uncertainty relating to the handling of personal data.
- (g) Assessing the need for new IT systems to safely process and store the personal data, and providing staff with training in any new system adopted.
- (h) Assessing the portability of using anonymized or pseudonymized data as part of the project to reduce identification risks and developing an appropriate anonymization protocol if the use of anonymized data is suitable.
- (i) Ensuring that individuals are fully informed about how their personal data will be used subject to their consent.
- (j) Providing a contact point for individuals to raise any concerns they may have with your organization.
- (k) If using external data processors, selecting appropriately experienced processors and putting in place legal arrangements to ensure compliance with data protection legislation.
- (l) Deciding not to proceed with a particular element of a project if the data privacy risks associated with it are inescapable and the benefits expected from this part of the project cannot justify those risks (Irish Data Protection Commission 2019).
- (m) Ensuring transparency as to what data is being captured from individuals and with whom it is being shared, along with mechanisms for individuals to (i) correct errors in their data when identified, and (ii) accept or reject requests for the sharing of their data when they have a right to do so.

---

<sup>38</sup> Privacy Impact Assessment of DAEM Registry, Commissioned by World Bank (On file).

# References

Article 29 Working Party. 2014. “Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU.” September 16. *Article 29 Data Protection Working Party*.

[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf)

Article 29 Working Party. 2017. “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.” October 4. *Article 29 Data Protection Working Party*.

<https://ec.europa.eu/newsroom/article29/items/611236>

Clark, Julia Michal; Metz, Anna Zita; Casher, Claire Susan. 2022. *ID4D Global Dataset 2021 : Volume 1 - Global ID Coverage Estimates (English)*. Washington, D.C. : World Bank Group. <http://documents.worldbank.org/curated/en/099705012232226786>

Casher, Claire; Metz, Anna Zita; Clark, Julia. 2023. *ID4D Global Dataset 2021: Volume 3 - Trends in Identification for Development (English)*. Washington, D.C. : World Bank Group.

<https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099031924132035631/p17634114229a80dc18ea11c4c279817517>

Data Protection Act (Nigeria Data Protection Act). 2023. *Data Protection Act (Nigeria Data Protection Act)*. 2023. Government of Nigeria.

Department of Identification of Poor Households (IDPoor). 2025a. “Data Protection Policy.” *The Identification of Poor Households Programme in Cambodia*. Accessed 25 April 2025.

<https://idpoor.gov.kh/en/data-protection-policy/>

Department of Identification of Poor Households (IDPoor). 2025b. *Household Data*. Accessed 22 April 2025. <https://app.idpoor.gov.kh/public-data-query#publichouseholddata>

Doddington, George R. et al. 1998. “Sheep, Goats, Lambs and Wolves: An Analysis of Differences in Speaker Recognition Performance.” *International Conference on Spoken Language Processing*.

DOI:[10.21437/ICSLP.1998-244](https://doi.org/10.21437/ICSLP.1998-244)

European Union (EU). 2018. “General Data Protection Regulation.” <https://gdpr-info.eu/>

GiZ. 2024. *IDPoor: The cornerstone of Cambodia’s social protection system*. Phnom Penh : GiZ. <https://www.giz.de/de/downloads/giz2024-en-ghpc-idpoor-2022-long-version.pdf>

Ghulam Shabir Arain. 2024. “Investigation confirms theft of 2.7M digital ID records in Pakistan.” *Biometric Update*. November 29. <https://www.biometricupdate.com/202411/investigation-confirms-theft-of-2-7m-digital-id-records-in-pakistan>

Greenleaf, Graham. 2025. "Cambodia's Draft Data Privacy Law: Too Much is Left to Delegated Prakas." *Privacy Laws & Business International Report* 15-19. May 7.

[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=5206970](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5206970)

IEEE. 2025. "FaceNet: A unified embedding for face recognition and clustering." *IEEE*. Accessed 17 March 2025. <https://ieeexplore.ieee.org/document/7298682>

Interaction Design Foundation. 2025. "Co-Creation in UX/UI Design." *Interaction Design Foundation*. Accessed 21 May 2025. [https://www.interaction-design.org/literature/topics/co-creation?srsId=AfmBOoo7yZP-F4TxOVXJM1\\_TB8fOjxVleBjKYTCmOTvyTVfnuhds7aNS](https://www.interaction-design.org/literature/topics/co-creation?srsId=AfmBOoo7yZP-F4TxOVXJM1_TB8fOjxVleBjKYTCmOTvyTVfnuhds7aNS)

Irish Data Protection Commission. 2019. *Guidance Note: Guide to Data Protection Impact Assessments*. [https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29\\_Oct19\\_0.pdf](https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29_Oct19_0.pdf)

Law on Civil Registration, Vital Statistics and Identification (CRVS-ID Law). 2023. *Law on Civil Registration, Vital Statistics and Identification*. 2023. Royal Government of Cambodia.

Ministry of Post and Telecommunications (MPTC). 2022. *Cambodia Digital Government Policy 2022-2035*.

[https://asset.cambodia.gov.kh/mptc/media/Cambodia\\_Digital\\_Government\\_Policy\\_2022\\_2035\\_English.pdf](https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf)

NADRA Pakistan. 2025. "National Registration & Biometric Policy Framework." *NADRA Pakistan*. Accessed 11 May 2025. <https://www.nadra.gov.pk/nr-and-bp-framework/>

National Cyber Security Centre (NCSC). 2019. "Biometric recognition and authentication systems." *National Cyber Security Centre*. Accessed 19 March 2025.

<https://www.ncsc.gov.uk/collection/biometrics>

The National Database and Registration Authority Ordinance (Pakistan NADRA Ordinance). 2000. *The National Database and Registration Authority Ordinance (Pakistan NADRA Ordinance)*. 2000. Government of Pakistan.

National Health Authority of India. 2012. *National Digital Health Mission: Health Data Management Policy*. [https://abdm.gov.in:8081/uploads/health\\_management\\_policy\\_bac9429a79.pdf](https://abdm.gov.in:8081/uploads/health_management_policy_bac9429a79.pdf)

National Identity Management Commission Act (Nigeria NIMC Act). 2007. *National Identity Management Commission Act (Nigeria NIMC Act)*. 2007. Government of Nigeria.

National Institute of Standards and Technology (NIST). 2004. "Fingerprint Image Quality." *National Institute of Standards and Technology*. Accessed 15 March 2025.

<https://www.nist.gov/publications/fingerprint-image-quality>

National Institute of Standards and Technology (NIST). 2024. “NFIQ 2.” *National Institute of Standards and Technology*. Accessed 17 March 2025. <https://www.nist.gov/services-resources/software/nfiq-2>

National Social Protection Council (NSPC). 2024. *National Social Protection Policy Framework 2024-2035*. [https://nspc.gov.kh/Images/National%20Social%20Protection%20Policy%20Framework%202024-2035\\_2025\\_02\\_20\\_15\\_45\\_55.pdf](https://nspc.gov.kh/Images/National%20Social%20Protection%20Policy%20Framework%202024-2035_2025_02_20_15_45_55.pdf)

Nigeria Information Technology Development Agency (NITDA). 2019. *Nigeria Data Protection Regulation*. <https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf>

Ogunmokun, Temitayo. n.d. *Assessing Data Protection in Nigeria: A Look at Biometric Identity, Surveillance, Encryption and Anonymity, and Cybercrimes*. <https://paradigmhq.org/wp-content/uploads/2022/01/Assessing-data-protection-in-NigeriaFinal.pdf>

Personal Data Protection Act, No. 9 (Sri Lanka Personal Data Protection Act). 2022. *Personal Data Protection Act, No. 9. 2022*. Government of Sri Lanka.

QDrant. 2025. “High-Performance Vector Search at Scale.” *Qdrant*. Accessed 17 March 2025. <https://qdrant.tech/>

SecuGen. 2025. “Hamster Pro 30.” *SecuGen*. Accessed 17 March 2025. <https://secugen.com/products/hamster-pro-30/>

Sub-Decree No. 38 on Harmonization of the Social Protection Registration System and Data Management (Harmonization Sub-Decree). 2024. *Sub-Decree No. 38 on Harmonization of the Social Protection Registration System and Data Management (Harmonization Sub-Decree)*. 2024. Royal Government of Cambodia.

Vibol, Torn. 2025 “Govt introduces new format ID card.” *Khmer Times*. April 4. [https://www.khmertimeskh.com/501664777/govt-introduces-new-format-id-card/#google\\_vignette](https://www.khmertimeskh.com/501664777/govt-introduces-new-format-id-card/#google_vignette)

World Bank. 2017. *ID Enabling Environment Assessment*. Washington, DC: World Bank Group. <https://documents1.worldbank.org/curated/en/881991559312326936/pdf/ID-Enabling-Environment-Assessment-Guidance-Note.pdf>

World Bank. 2019. “Data Protection and Privacy Laws.” In *ID4D Practitioner’s Guide*. Washington DC: World Bank Group. <https://id4d.worldbank.org/guide>

World Bank. 2021. *An Assessment of Cambodia’s Cash Transfer Program for the Poor and Vulnerable Households During COVID-19 (English)*. Washington, D.C.: World Bank Group. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/661201624622956583/an-assessment-of-cambodia-s-cash-transfer-program-for-the-poor-and-vulnerable-households-during-covid-19>



World Bank. 2025. *Implementation Completion and Results Report: Identity and Targeting for Social Protection Project, Morocco*. Washington, DC: World Bank Group.

<https://documents1.worldbank.org/curated/en/099040125102010830/pdf/BOSIB-25ebd7fd-677e-446a-b062-57f54deb076a.pdf>

Yojana, Pradhan Mantri Jan Arogya. 2022. *National Health Authority of India Data Sharing Guidelines*. <https://www.medianama.com/wp-content/uploads/2022/07/NHA-Data-Sharing-Guidelines.pdf>

# Appendix 1: Sampling Details

## *Field Visits*

The evaluation team consulted with a total of 13 communes and sangkats, 6 in Kampong Cham province and 7 in Siem Reap province, representing over 50 percent of the 22 communes and sangkats participating in the DSPP rollout. During the first field visit, the evaluation team requested the GS-NSPC to assist in selecting 2 communes in Kampong Cham and 2 sangkats in Siem Reap. The evaluation team specifically asked that the selected sites include a mix of relatively well-performing and lower-performing locations. This purposive sampling approach was deemed appropriate given the short timeframe since rollout—approximately one month at the time of data collection—and was intended to ensure that the selected sites had accumulated sufficient experience to generate meaningful insights.

During the second field visit, one location in each province was selected, and commune/sangkat officers from neighboring jurisdictions (five communes in Kampong Cham and seven sangkats in Siem Reap) were invited to participate in focus group discussions. Site selection and grouping for this round were based on geographic proximity, and the evaluation team again requested that GS-NSPC coordinate the selection while maintaining the mentioned criteria to ensure consistency.

The evaluation team met with Commune/Sangkat Chiefs, Officers, and social assistance beneficiaries in the following locations:

### **Kampong Cham**

- Kouk Rovieng
- Sdaeung Chey
- Sampong Chey
- Pring Chrum
- Soutib
- Khnor Dambang

### **Siem Reap**

- Tuek Vil
- Chong Khnies
- Sambuor
- Kok Chak
- Siem Reap
- Krabei Riel
- Sla Kram

The evaluation team acknowledges the limitations of this sampling approach, particularly the reliance on GS-NSPC to facilitate site selection. However, this collaboration was considered necessary, as GS-NSPC works directly with all participating communes and sangkats and was best positioned to identify those with sufficient implementation experience and insights to contribute

meaningfully at that stage of the evaluation. To help address this limitation, the evaluation team also organized a group discussion session during the national consultation workshop. This session allowed representatives from all 22 participating communes and sangkats to share their perspectives, validate or challenge the findings, and raise any additional insights or concerns that may not have been captured during the field visits.

#### Key Informant Interviews

The evaluation team met with representatives of the following organizations:

##### **Social Protection program operators**

- Department of Disability Welfare (DDW), Ministry of Social Affairs, Veterans, and Youth Rehabilitation (MOSVY)
- Department of Identification of Poor Households (IDPoor), Ministry of Planning (MOP)
- General Secretariat of the National Social Protection Council (GS-NSPC), Ministry of Economy and Finance (MOEF)
- National Social Assistance Fund (NSAF), MOSVY
- National Social Security Fund (NSSF), Ministry of Labour and Vocational Training (MOLVT)

##### **Other stakeholders**

- Digital Government Committee (DGC), Ministry of Post and Telecommunications (MPTC)
- General Department for Identification (GDI), Ministry of Interior (MOI)
- “Improving Social Protection and Health in Cambodia” project team, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)
- UNICEF

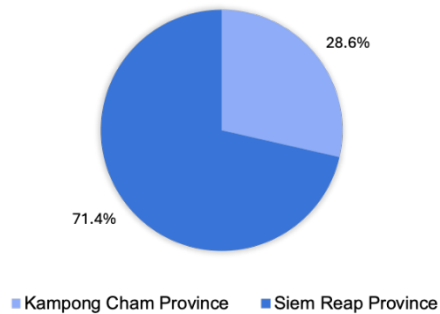
#### Stakeholder Consultation Workshop

Participants included representatives of:

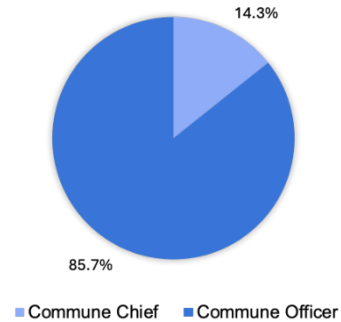
- The Board of Provincial Governors
- MOP (national and provincial branches)
- NSAF (national and provincial branches)
- MOI
- NSSF
- MOSVY
- General Secretariat of the Digital Government Committee
- NPCA
- NSPC Sub-Committee for Digital Social Protection
- NSPC General Secretariat for Digital Social Protection
- GiZ
- UNDP
- UNICEF

## Appendix 2: Survey Data

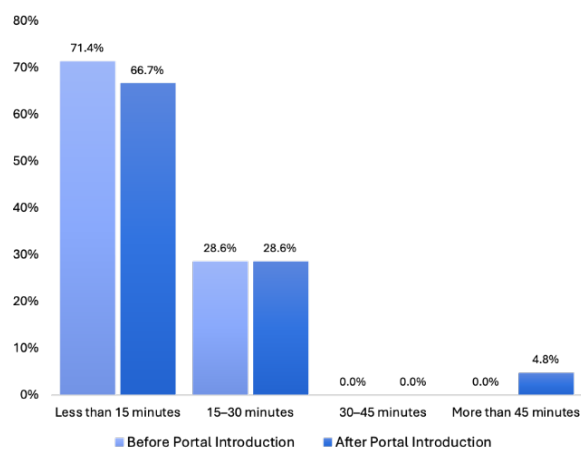
**Figure 2.1: Respondents' Province of Residence**



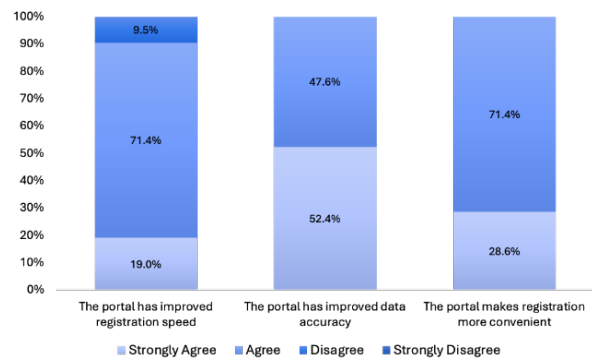
**Figure 2.2: Respondents' Position**



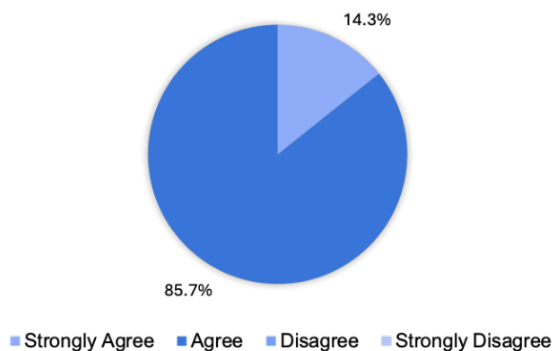
**Figure 2.3: Time Spent on Registration/Update Before and After DSPP Introduction**



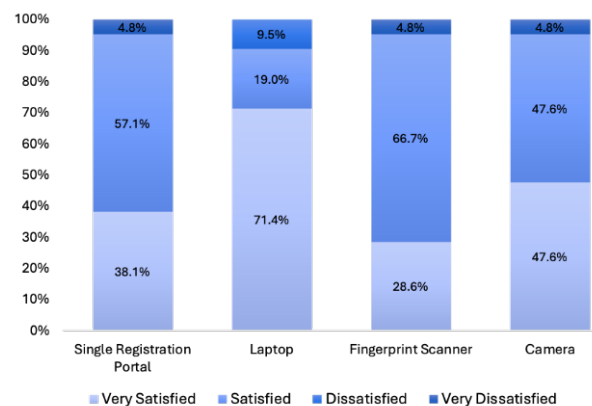
**Figure 2.4: Perceived Improvements Compared to Previous Registration/Update Process**



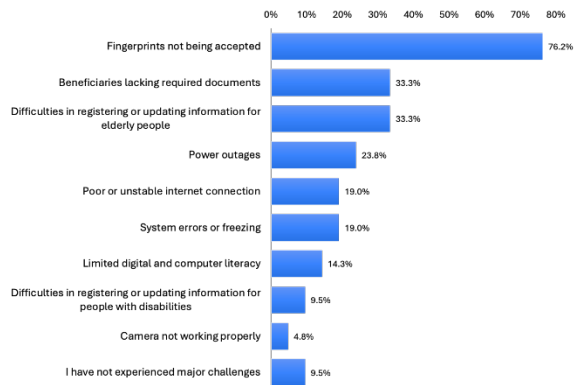
**Figure 2.5: Perceived Ease of Use of the DSPP**



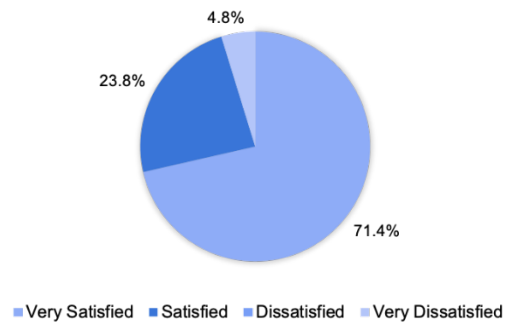
**Figure 2.6: Users' Satisfaction with DSPP, Laptop, Scanner, Camera**



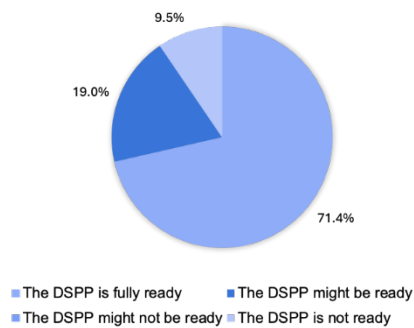
**Figure 2.7: Reported Challenges Experienced while Using the DSPP**



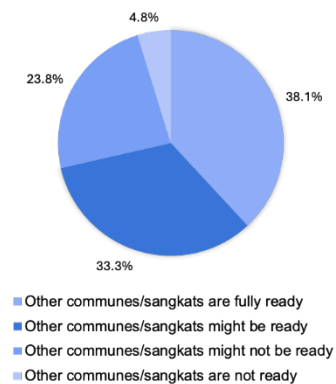
**Figure 2.8: Satisfaction with the Technical Support Team**



**Figure 2.9: Perceived Readiness of the DSPP for National Rollout**



**Figure 2.10: Perceived Readiness of Other Communes/Sangkats in Adopting and Implementing the DSPP**



## Appendix 3: Note on Impact Evaluation

**As agreed with GS-NSPC, this report constitutes a *process* evaluation of the early stages of the DSPP/SR rollout.** It is not an *impact* evaluation, which would assess the effects of the DSPP and SR on its target population, determining whether and to what extent it has achieved its intended outcomes (and identifying any unintended consequences). Impact evaluation is not possible at this early stage of the program, because some of the intended outcomes will take much longer to manifest. It is also not necessary – the GS-NSPC is seeking agile, policy-oriented feedback on how to approach their next phase of scale-up.

**However, the DSPP/SR is a great candidate for impact evaluation in the medium term.** There is a lack of evidence on digital transformation initiatives in the social protection sector, and capturing rigorous data on the impact of this innovation would be of great value globally. It would also arm the GS-NSPC with robust evidence of the impact of its work, which is useful for program advocacy and communications domestically.

**Pinpointing the impact of a program requires comparing it to a ‘counterfactual’ situation where all else is equal but the program is not implemented.** The Randomized Controlled Trial (RCT) research design is widely considered to be the most rigorous way to do this in development economics. In the case of the DSPP rollout, an RCT could involve randomly dividing communes/sangkats into a group that receives the program immediately and a “control group” that receives the program later, and comparing outcomes across the two groups (this can be particularly opportune if resource constraints mean that immediate rollout everywhere is not possible, anyways).

**When conducting an impact evaluation, it is best to start early and work in partnership with professional researchers.** Setting up such an RCT evaluation involves advanced planning to embed the two-group design into the official rollout plan. It’s also necessary to collect and analyze a lot of data to ensure that the two groups are comparable, and to enable assessment of the outcomes you care about (i.e. to have “before” values to compare with “after” values). RCT is also just one of many research design options. Academics from universities or research institutions can advise on these design questions and perform the necessary analysis. Working with a third party also adds credibility to the ultimate research results.

**Important first steps toward conducting an impact evaluation would include:**

- **Determining outcomes of interest** – GS-NSPC should agree on the priority outcomes that it wants to measure, as this will affect all other decisions.
- **Finding research partners** – GS-NSPC should start to discuss impact evaluation opportunities with universities/research institutes in Cambodia (and beyond, potentially).
- **Identifying resources** – the data collection required for impact evaluation can be resource-intensive, but many donors and stakeholders fund research on topics they are invested on. GS-NSPC should indicate to the World Bank team if they would like guidance on navigating these resources.

**Ideally, these steps should be taken as soon as possible.** The majority of innovative programs miss the window to embed an impact evaluation into their rollout, because they are in a rush to move forward. This ultimately costs them the ability to make robust claims about the impact of their work. GS-NSPC is currently at an ideal point in its journey to take action on impact evaluation before making any further moves in its national scale-up plan.

## Appendix 4: Consolidated Recommendations (Parts 1-3)

### Part 1: User Experience with DSPP & SR

**Continue to strengthen stakeholder consultation and communication:** The GS-NSPC should continue engaging actively with relevant stakeholders to address concerns and provide clarity on the implementation of the DSPP and SR. Strengthening stakeholder consultation should remain a top priority, with additional efforts to foster collaboration through regular touchpoint meetings and co-creation workshops. Transparent, two-way communication will be essential for building trust, addressing misconceptions, and reinforcing stakeholder buy-in.

**Leverage existing resources:** An assessment should be undertaken to identify how existing assets, such as the national network of Android tablets and the digital infrastructure developed by various social protection programs, can be more effectively utilized in the DSPP and SR rollout. Optimizing the use of these resources can help reduce costs and improve overall system efficiency.

**Formalize CRM processes:** To support the national scale-up, GS-NSPC should establish a formal CRM platform to systematically track, manage, and resolve user inquiries across multiple channels, streamlining service delivery, improving responsiveness, and fostering trust in the DSPP and SR.

**Expand training program:** In collaboration with key partners, GS-NSPC should design and implement a comprehensive training plan and expand capacity building efforts to include a train-the-trainer model, mechanisms for quality assurance, and a certification process for commune/sangkat officials. The training program should also incorporate periodic refresher courses and specialized modules, such as digital literacy for less experienced users and advanced data analysis for decision-makers.

**Conduct sustainability assessment:** To address concerns over the long-term financial and operational viability of the DSPP and SR, GS-NSPC should conduct and widely disseminate a comprehensive sustainability assessment. This should include planning for both local-level (e.g., power banks, mobile data packages) and national-level needs (e.g., equipment procurement and maintenance). The assessment process should involve consultation with key stakeholders to capture the full spectrum of cost considerations and support informed planning for future phases of implementation.

### Part 2: Cambodia's ID Ecosystem

**Improve Cambodia's foundational ID system:** In the short term, the government should prioritize the digitalization of civil registration, particularly for birth and death records, and accelerate efforts to achieve universal coverage of the Khmer ID. Over the longer term, Cambodia should consider transitioning from chip-based ID cards to digital ID solutions. This shift would help reduce system costs and capitalize on the country's growing mobile phone penetration to enable more accessible and scalable authentication mechanisms.



**Enhance Cambodia’s functional ID ecosystem:** To improve efficiency and reduce redundancy, biometric data collection across government agencies should be harmonized. The GS-NSPC’s biometric system should be rigorously tested, with assessments guided by international standards, such as the ISO/IEC series and NIST’s digital identity guidelines. Simultaneously, interim data protection regulations, either sectoral or cross-cutting, should be introduced while national legislation is being finalized. In the longer term, Cambodia should work toward the convergence of identification services within a unified DPI framework, integrating identity, data exchange, and payment platforms to streamline service delivery and ensure system-wide interoperability.

## Part 3: Legal & Regulatory Framework

**Strengthen data protection safeguards in the Harmonization Sub-Decree:** The current Harmonization Sub-Decree should either be repealed and replaced or substantively amended to incorporate essential data protection principles. These include provisions on purpose limitation, data minimization, storage duration, individual data subject rights, data sharing, independent grievance mechanisms, minimum security standards, and mandatory breach notification protocols. Strengthening these safeguards is critical to ensure consistency with international best practices and foster public trust in the DSPP and SR.

**Conduct a comprehensive Data Protection Impact Assessment (DPIA) on the DSPP and SR to address privacy risks arising from integration of databases:** Identify compliance gaps, privacy risks, and areas for improvement related to the integration of data across platforms within the DSPP and SR. The DPIA should propose appropriate legal, technical, and organizational safeguards to mitigate risks to individuals’ rights and freedoms, ensuring that data handling practices are transparent, secure, and aligned with global standards.