United Nations Children's Fund

Social Protection Section

Terms of Reference

Design, Development, and Implementation of enhanced Integrated SSN MIS Components for the Ministry of Labour and Social Affairs, Iraq

- Background
- Purpose & Objectives
- Scope of Work
- Key Deliverables & Timeline
- Functional Requirements
- Non-Functional Requirements
- Security Requirements
- Development Approach
- Team Composition and Qualifications
- Quality Assurance and Monitoring
- Intellectual Property and Data Ownership
- Coordination
- Reporting requirements
- Handover and Capacity Building
- Location and Duration
- Evaluation process and methods
- Payment Schedule
- Financial Administration
- General Terms and Conditions

November - 2025

Section	Content
Background	The Government of Iraq, through the Ministry of Labor and Social Affairs (MoLSA), is working to enhance its Social Safety Network (SSN) to better serve vulnerable populations. The current SSN Management Information System (MIS) provides core functionalities but requires significant enhancement to meet evolving needs for case management, beneficiaries feedback, and proactive communication. Additionally, Archiving and Revenue systems are required. To improve the effectiveness, responsiveness, and inclusiveness of social assistance programs, MoLSA, with the support from UNICEF, aims to integrate six critical new components into the existing SSN MIS as part of the EU-UN joint program of reforming Social protection in Iraq. This integration includes: Case Identification & Management, a Grievance Redress Mechanism (GRM), Beneficiary Outreach & Communication, Electronic Archiving and Outputs, Revenue Accounting System, and Shock Responsive\Climate Change. These additions will improve service delivery for complex cases, provide structured channels for complaints and appeals, and enable effective, two-way communication with beneficiaries, aligning with national digital transformation objectives. This phase focuses on adding these modules and ensuring their seamless integration with the current infrastructure, paving the way for a future, comprehensive system overhaul.
Purpose and Objectives	This assignment will design, develop, and integrate modular, API-ready components for the SSN MIS including Case Management, GRM, Beneficiary Outreach, Electronic Archiving and a Social Protection Fund Revenue & Payment module. All components must be interoperable with the current legacy SSN MIS and future enhanced SSN MIS to be developed by SPC/MoLSA, ensuring continuity and safe coexistence during transition: • **Case Identification & Management:** To provide social workers with digital tools for identifying, tracking, referring, and managing complex beneficiary cases, linking them to necessary services. • **Grievance Redress Mechanism (GRM):** To establish a systematic process for receiving, tracking, resolving, and reporting on complaints and appeals from beneficiaries and applicants. • **Beneficiary Outreach & Communication:** To create a platform for proactive communication with beneficiaries and gather feedback through various digital channels. • **Electronic Archiving System:** Digitize formal paper-based documents into a structured electronic archive, enabling organized access, improving

<table>
<tr><td></td><td>administrative efficiency, and ensuring secure, reliable storage of official records.

• Social Protection Fund Revenue and Payment Management System: Develop an independent module within the SSN MIS to manage the revenues and payments of the Social Protection Fund, in compliance with Social Protection Law No. 11.

• Shock-Responsive / Climate Change: Develop an online form for social workers to register IDPs displaced from their original locations due to climate-related factors.

The objective is to enhance the immediate capacity of the MoLSA to manage social protection programs more effectively and inclusively, while ensuring these new components are built with future-readiness in mind.</td></tr>
<tr><td>Scope of Work</td><td>The contractor will:

1. Design and Develop: Create the six new modules based on detailed functional requirements (to be finalized during the inception phase) and best practices.
2. Integrate: Ensure the modules are decoupled and interoperable with both the existing SSN MIS and any new/enhanced SSN MIS commissioned by SPC/MoLSA.
3. Ensure Compatibility: Design the modules to be modular, scalable, mobile-responsive, and multilingual (Arabic primarily), with API-readiness for future systems.
4. Provide Technical Support: Offer technical support and maintenance for the new modules for one year post-deployment.
5. Documentation & Training: Deliver comprehensive documentation and conduct training for MoLSA staff.</td></tr>
<tr><td>Key Deliverables & Timeline</td><td>
<table>
<tr><th>Milestone</th><th>Description</th><th>Timeline</th></tr>
<tr><td>Inception Report</td><td>Detailing methodology, work plan, and timelines.</td><td>Week 2</td></tr>
<tr><td>System Design</td><td>Finalized architecture for the new modules & integration plan with existing MIS.</td><td>Week 5</td></tr>
<tr><td>MVP</td><td>Finalized the phased MVP for all modules demonstrating core functionality, demo data and initial performance test.</td><td>Week 17</td></tr>
<tr><td>Full Build</td><td>Full deployment of the integrated modules.</td><td>Week 22</td></tr>
<tr><td>Integrated UAT</td><td>Performance & security tests, end-to-end flows, coexistence tests with legacy MIS.</td><td>Week 26</td></tr>
</table>
</td></tr>
</table>

	Final Deployment	Live system with full features in addition to training report, handover, maintenance plan.	Week 30	
	Handover	End of 1-year support after full implementation.	Week 82	
Functional Requirements	**1. Case Management:** ▪ Digital case tracking dashboard for social workers. ▪ Risk categorization (low, medium, high, and potentially others like Health/Education). ▪ Intervention planning and referral tools. ▪ Offline capability with synchronization. ▪ Secure API for data exchange with the existing MIS (beneficiary details) and future systems. ▪ Create built-in real-time dashboards and downloadable reports to track registrations and trends. **2. Grievance Redress Mechanism (GRM):** ▪ Multi-channel intake (online portal, social worker interface, hotline integration). ▪ Triage, classification, and routing system. ▪ Workflow engine with escalation procedures. ▪ Automated notifications (SMS/email). ▪ Reporting and analytics features. ▪ Integration link to beneficiary profiles in the existing MIS. ▪ Capture the calls logs from the implemented Digital IP PBX. ▪ Create built-in real-time dashboards and downloadable reports to track registrations and trends. **3. Beneficiary Outreach & Communication:** ▪ Integration with SMS gateways (and potentially WhatsApp/Telegram). ▪ Message template creation and management. ▪ Automated/scheduled message delivery. ▪ Feedback capture mechanisms. ▪ Linkage to beneficiary contact details in the existing MIS. ▪ Create built-in real-time dashboards and downloadable reports to track registrations and trends. **4. Electronic Archiving System:** ▪ Scan documents with high quality, naming files according to the approved coding system (beneficiary number + document type). ▪ Upload files to the electronic archiving system, entering metadata for each document: name, date, and issuing authority. ▪ Verify the integrity of the archive by reviewing the uploaded files and ensuring they can be opened and viewed. ▪ Generate an electronic notification indicating the completion of the archiving process, which is sent to the relevant archiving unit or department. ▪ Create built-in real-time dashboards and downloadable reports to track registrations and trends.			

	5. Social Protection Fund Revenue and Payment Management System ▪ Fund Revenues: Record and classify incoming amounts from multiple sources by origin and type of revenue, in alignment with the legal framework. ▪ Management of Beneficiaries in Violation of Eligibility Rules: ▪ Category 1: Full termination of benefits in cases of major violations. ▪ Category 2: Continued benefits with adjustments in beneficiary records for minor violations. ▪ In both cases, the system must calculate the overpaid amounts, generate installment repayment schedules according to the law, and monitor repayment progress. ▪ Integration: The system must provide an API-based mechanism for interoperability with the SSN MIS, ensuring seamless data exchange and operational continuity. ▪ Create built-in real-time dashboards and downloadable reports to track registrations and trends. **6. Shock Responsive\ Climate change** ▪ Develop an online form accessible through the platform for social workers to register IDPs displaced due to climate-related factors. ▪ Ensure the form captures key data fields (household details, location of origin, reason for displacement, current location, and basic needs). ▪ Provide secure user authentication for social workers to access and submit the form. ▪ Enable offline data entry with automatic synchronization once internet connection is restored. ▪ Create built-in real-time dashboards and downloadable reports to track registrations and trends. **7. System Administration:** ▪ Establish role-based access controls with clearly defined permissions for different user types (social worker, supervisor, administrator). ▪ Maintain a detailed audit trail of all system transactions and user activities. ▪ Provide centralized real-time operational dashboards for system usage, process performance, and case progress monitoring. ▪ Allow administrators to configure certain system parameters without requiring developer support. **8. System Integration:** ▪ Designing stable, versioned APIs (OAuth2/JWT, REST/JSON) and an API sandbox for testing. ▪ Delivering adaptors/connectors to the legacy MIS and the future MIS (if available during the contract), including interface specs and end-to-end tests. ▪ Future MIS Compatibility: Provide stable versioned interfaces, a mapping document (entities, events, errors), and change-control procedures so the future MIS vendor can integrate without breaking

	changes. Participate in joint technical sessions and update specs accordingly. ▪ Participating in technical working sessions with the future MIS vendor to align data models, events, and security standards, and updating integration docs accordingly. ▪ Providing a coexistence & cutover plan (read-only/read-write modes, conflict resolution, and rollback).
Non-Functional Requirements	These sections (Non-Functional Requirements, Security, Handover, Team Composition, QA, IP, Coordination, Reporting, Evaluation, Payment) should be adapted from the TOR, with a strong emphasis on: • Integration: The ability to seamlessly connect with the current MIS is paramount. Bidders must demonstrate experience in integrating new modules into legacy systems. • APIs: Development of secure, well-documented APIs (e.g., using OAuth 2.0, JWT) for both current integration and future use. • Modern but Compatible Tech: Using modern, yet compatible, technologies that won't hinder the current system but can be carried forward into Phase Two. • Evaluation: The technical evaluation should prioritize proven experience in systems integration and the specific technologies proposed for the new modules and APIs. • Responsive web-based interface (mobile/tablet/desktop). • Arabic and Kurdish UI language support. • GDPR-compliant data handling and secure login protocols. • Open-source or license-free backend preferred. • Hosting Environment: The MIS should be designed to support on-premise hosting at MOLSA's servers, system deployment should comply with MOLSA recommended approach and capable of future migration between hosting environments (cloud-to-on-prem or vice versa) without data loss. • Disaster Recovery: The system must have a disaster recovery plan to be developed in coordination with MOLSA to ensure business continuity in case of outages or failures
Security Requirements	UNICEF shall reserve the right to assess the quality and accurateness of outsourced software development and operational maintenance of the system / application, whether it be through security assurance testing or through external security assessment. The Solution / Service shall be protected from unwanted network traffic by network filtering or separating measures that lay outside of the system; such as externally controlled routers and firewalls. The system also shall have proper end-point protection, with the following minimum requirements: • malicious code protection measures • host firewall configured utilizing, at a minimum, least privileged access controls (services, user, communication access). **1. Validation of Security Controls** UNICEF shall reserve the right to periodically validate the implementation of the security requirements outlined in this document via:

	• Security Assurance Testing • Vulnerability Testing • Penetration Testing • Audits • On-site checks **2. Identification, Authentication and Authorization** a) The service provider shall follow the principle of least privilege, guaranteeing that users, group, role, and device identifiers will be unique, assigned to each entity (user or process). Each application user role shall have a correspondent database connection according to its privileges. b) The service provider shall centrally manage the user account using federated identities and whenever possible integrate their solution with the UNICEF Identity Management System. c) In case authentication is password based; the password shall forcefully adhere to the common best practice quality requirements and will be forcefully renewed frequently. The allocation of authenticators will be controlled and management through a formal process. d) Multi-factor authentication will be used for privileged accounts and user access outside of UNICEF trusted network. e) All the user and system accounts shall be disabled after a defined period of inactivity, in accordance with organizational standards. All default accounts and or passwords shall be removed or changed. Approvals will be required for creation, deletion or modification of any account. f) All access from external networks will traverse specific entry and exit points where external communication is terminated and re-established into a UNICEF controlled ICT ecosystem. g) Account lockout features will be used for invalid authentication attempts. h) Application code shall never contain any credentials. **3. Availability and Deletion** Systems availability shall be set according to Service Level Agreements, to meet the Confidentiality, Integrity and Availability requirements commensurate with its classification, as noted above. Any deletion of confidential / personal data must be done so that it cannot be reconstructed. **4. Cryptography** a) The service provider shall use best practice or industry standard secure data exchange protocols b) and keep them up to date, as per defined UNICEF standards. Outdated and / or compromised c) protocols shall never be used. d) All passwords shall be encrypted with best current practices or strong industry standards cryptographic algorithms and secure keys. The keys will be generated using strong cryptographic algorithms. e) Key files must be protected from unauthorized modification using an application that enforces automatic reconciliation from an authoritative source.

	f) Encryption keys shall be securely stored outside of the systems on which they are used. **5. Secure Development** a) The system shall be engineered following the 'security by design' principles. b) Development and tests of the system will be done with fictitious or pseudonymized information. c) Access to program source code and associated items - such as designs, specifications, testing and validation plans - shall be strictly controlled; to prevent the introduction of unauthorized functionality. d) The system shall display generic error messages that do not disclose detailed information such as process logs, account or system information. e) Executable code will not be implemented on an operational system until evidence of conforming to the testing criteria (user approval, QA, or the equivalent) is acquired and the associated program source libraries have been updated. **6. Security Operations** a) The system shall be hardened, which means that: • only the services and network ports necessary for efficient operation are up and running • all application code is patched and kept up to date and • limiting the accounts and removing, changing or disabling default accounts and passwords Note: In order to ensure proper risk driven methodology is followed, patches shall fall into one of the following categories, which are classified by the application / system vendor.; critical, noncritical. The patching window SLA, shall be formally documented by both vendor and UNICEF's Designated Authority (D.A.). b) Servers and applications shall be configured to run with the minimum system authorizations necessary. The service provider shall ensure the implementation of the appropriate technical and organizational measures. c) The system must be configured to display generic error messages that do not disclose detailed information such as process logs, account or system information. d) The production environment shall be separated from the test and development environments; preferably on logically and physically different systems. e) Development and test environment shall have the same patch level as the production environment. f) The production environment shall not have any development tools. g) Configuration/ Application source code/ customized work shall be protected from unauthorized access / modification and reside in non-production environment with proper back-up / resiliency policy. h) The system shall have malicious code protection measures. Logs generated by malicious code protection measures shall be monitored. **7. Vulnerability Management**

	a) The service provider is required to run security tests. Test will run prior to the launch of the system and periodically afterwards; with a minimum frequency of once a year. b) The service provider is required to report on the results of the security scans and the remediations taken. These reports will be sent to UNICEF's Chief of IT Security or the relevant focal point(s). c) Critical security patches shall be applied following established testing / change management processes. **8. Change Management** a) Any changes to UNICEF system(s) or software shall be agreed upon between ICT and the business division / office owner of the affected system and third party. b) Changes to system and/or application post baseline will be documented (version / build number), along with description via a formal change management process. The service provider shall report the following information about patches, at a minimum: type, version, reason, post test results after implementation. Patches that fail testing will also be recorded and documented. c) The updating of the operational software, applications and program libraries will only be performed by trained and qualified administrators upon appropriate management authorization. **9. Log Management and Monitoring** a) The system shall generate and process auditing tracks covering all actions taken on personal data, including data access only. b) Authentication validation activities and all changes in authorization shall be logged and securely stored, with limited access. c) Access to content, key information and or any modifications to operational program libraries shall be logged and restricted. d) Logs and events will be generated in a format that can be easily parsed and used as an input for logging process management. e) Integrity log checking shall be performed to ensure consistency. f) The system, application, as well as underlying services and or networks, shall be monitored and activities logged. **10. Security Incident Management** A security breach shall be viewed as: • a failure in security controls which leads to the accidental, unlawful or unauthorized access, destruction, loss or alteration of data / information that processed / stored on system • a failure in security controls which leads to the accidental, unlawful or unauthorized access to ICT resources, such as - but not limited to - computing resources (processing and storage / services) and communication resources (infrastructure). a) Security breaches shall immediately be communicated to UNICEF's Point of Contact. b) A security incident notification and escalation procedure shall be formally documented.

Development Approach	The solution shall follow an Agile methodology with iterative deliveries, structured in the following phases: 1. Requirements Gathering & Systems Assessment 2. Design & Architecture Finalization 3. Development & Internal Testing 4. Piloting 5. System Administration Training & Capacity Building 6. Deployment & Maintenance Handover.
Team Composition and Qualifications	Outline the expected qualifications: • Developer (min. 5 years in relevant tech stack) • UI/UX Designer • Database Specialist • QA Tester.
Quality Assurance and Monitoring	• Weekly status updates to project manager. • UAT with government counterparts. • Acceptance criteria and sign-off process. • Testing reports
Intellectual Property and Data Ownership	• All source code belongs to MOLSA. • Data privacy must align with UNICEF policies, such as the UNICEF Data Protection Policy, and Iraq national regulations
Coordination	A technical steering committee shall be established to oversee the implementation of the project. The committee should include representatives from MoLSA and UNICEF. The committee will meet monthly and may convene additional ad-hoc meetings as needed to address emerging issues and ensure smooth coordination across stakeholders.
Reporting Requirements	• Weekly written progress reports. • Change and incident reports. • End-of-project final report summarizing activities and outcomes.
Handover and Capacity Building	The Contractor shall ensure a full and smooth transfer of the enhanced SSN MIS to MoLSA, including technical ownership and staff capacity building. The handover must include: • **Full System Delivery:** Transfer of all developed components, including the complete source code, database scripts, APIs, credentials, and system configurations, ensuring MoLSA's full ownership and control. • **Intellectual Property Rights:** All software, documentation, and related work products developed under this assignment shall be the sole property of MoLSA. • **Technical Documentation:** Provision of complete system documentation, including architecture design, API specifications, installation manuals, administrator guides, and user manuals. • **Training and Knowledge Transfer:** Delivery of practical training sessions for MoLSA IT staff and system users, along with editable training materials (manuals, guides, FAQs). The training should cover system administration for

<table>
<tr><td></td><td>all the integrated modules including all subsections. System technology orientation should be provided to MOLSA technical team.
Final Handover and Acceptance: All handover activities, including system deployment, training completion, source code delivery, and signed handover certificates, must be finalized before project closure.</td></tr>
<tr><td>Evaluation process and methodology</td><td>
1. Initial Technical Evaluation Pass/Fill approach:
Vendor must be passed all the requirements below to be considered for the technical evaluation process:
<table>
<tr><th>MANDATORY REQUIREMENTS</th><th>SUPPORTING DOCUMENTS</th><th>SCORE</th></tr>
<tr><td>Lead bidder is a legal entity regulated and licensed in the country of registration</td><td>A copy of the certificate of incorporation (i.e., company legal registration) or equivalent document verifying legal status is to be provided.</td><td>Pass / Fail</td></tr>
<tr><td>Demonstrated experience in MIS or digital system development in the public or Governmental sector</td><td>At least two relevant examples, reference letters and supporting documents.</td><td>Pass / Fail</td></tr>
</table>
Then Bid shall be evaluated based on technical and financial criteria. The ratio weight between technical and financial criteria is (70:30).
2. Technical Evaluation:
The Bid shall be technically evaluated as below:
<table>
<tr><th></th><th>Technical evaluation Criteria</th><th>Max. Points Obtainable</th></tr>
<tr><td>i</td><td>Company and organizational profile</td><td>20</td></tr>
<tr><td></td><td>Company Background and Presence in Iraq: Evaluation based on the firm's history, establishment, and understanding of the local context. The scores will be calculated as follows:
Presence in Iraq = 5 points</td><td>5</td></tr>
<tr><td></td><td>Relative Experience: Assessment of past similar projects and the firm's engagement/operations in Iraq with evidence considering the minimum 3 years requirement. The scores will be calculated as follows:
3-5 years=2 scores; 6 years=3 scores; 7 years=4 scores; +8 years=5 scores</td><td>5</td></tr>
</table>
</td></tr>
</table>

		Reputation and Success Track Record: Consideration of the company's reputation, reliability, and success in delivering projects in Iraq. (Evidence provided for successful implementation of similar Projects in Iraq). The company provide evidence supporting this which could include client testimonials, industry reports, media coverage, online reviews, and feedback from stakeholders or partners. The scores will be calculated as follows: One evidence -3 points, two evidence – 5 points and three or more evidence provided – 10 points.	10
	ii	**Proposed work plan and approach**	**30**
		Compliance with the ToR objectives and proposed system architecture aligned with modular design principles and API-readiness. As follows: System Architecture- 8 points, Future Expansion Plan- 4, Offline Registration Plan- 3 points.	15
		Proposed development approach (Agile/iterative preferred) and quality assurance strategy as following: Admin, Monitoring and Reporting Portals-4 points, QA plan- 2 points, Capacity Building Plan- 2 points, Development Approach- 2 points.	10
		Feasibility of timeline and clear project milestones.	5
	iii	**Company Key Resources**	**20**
		Appropriate technical resources with the right skills/expertise, qualifications (e.g certified developers) to deliver the outputs required; Key technical skills/expertise of Individual team members to be used to execute the assignment; Qualifications/level of education of key staff that will be assigned to this project, evidence of expertise/experience of each individual team member etc. The technical proposal should include the following: a) Technical Expertise and Skills of the team (16 points) The CVs of proposed team members, with the required qualification based on the required task. The CVs will be assessed against the depth and length of the experience and the strength of expertise and skills mentioned in this section. Relevant academic qualifications and certifications in information technology, cybersecurity, network infrastructure, or related fields will be necessary. Key qualifications and certifications of the team members will be evaluated and scored using the following criteria:	20

		Qualified Front End and Back End Developer/s = 4 points, Qualified Database Specialist/s = 4 points; Qualified UI/UX Specialist/s= 4 points: Qualified QA Specialist/s= 4 points. Certifications and qualifications are based on relevance as mentioned above. b) Expertise and Skills of the team leader (4 points) The CVs of proposed team leader/s with the required qualification based on the required task. The CVs will be assessed against the depth and length of the experience and the strength of expertise and skills mentioned in this section. Relevant academic qualifications and certifications in leading relevant technical projects will be required = 4 points.	
		Total out of 70 (minimum passing score is 49)	**70**

3. Financial Evaluation:
The bidder will be financially scored based on formula below: The total weight of the bidder will be the cumulative of the formulas (Technical and Financial).
Bidder (A) = (Maximum score for price proposal (30 points) x Price of lowest priced proposal among technically passed bidders)/Price of proposal (A)

Payment Schedule

Link payments to deliverables:

Milestone	Amount	Condition
Inception Report	20%	Upon approval
MVP Delivery	25%	Functional demo
Final Delivery	50%	Deployment, testing and documentation
End of Support	5%	Approval of Final Handover package

Financial Administration

UNICEF will make payments to the contractor in US $ Dollars if it's an entity registered outside of Iraq with a bank account outside of Iraq or in IQD Iraq Dinar if the company is registered in Iraq, with a bank account in Iraq according to percentages of completed work certified by the supervising committee and approved by UNICEF focal person at Iraq Country Office.

If the financial offer is in:

1. IQD (Iraq Dinars), it is important for a bidder to have an IQD bank account.
2. If a bidder quote in any other currency i.e. US Dollar (USD), below shall apply:
   a) Awards will be made based on the currency of their offer. The bidder is required to have a bank account in the currency of their offer.

	b) If a bidder has quoted in USD (US Dollar) or any other currency, for evaluation purposes only, proposals submitted in USD or any other currency will be converted into IQD using the United Nations rate of exchange in effect on the submission deadline date
General Terms and Conditions	• Adherence to UNICEF's rules and regulations. • Confidentiality clauses.

Prepared by:

Karwan Nazar Dawood
Social Policy Specialist

Ali Rasheed
ICT/T4D Officer

Reviewed by:

Erika Strand
Digitally signed by Erika Strand
Date: 2025.11.13 11:43:43 +03'00'

Approved by:

Laetitia Bazzi
Digitally signed by Laetitia Bazzi
Date: 2025.11.17 09:37:05 +03'00'

ANNEX 1: Shock Responsive\ Climate Change

Household Registration Form for Climate-Induced Displaced Families

Section A: Household Identification

Household ID (assigned by social worker)
Date of registration
Governorate / District / Community
Current residence (formal / informal camp / host community)
Previous place of residence (village/district)
Cause of displacement (drought, salinity, flood, other)

Section B: Household Composition

Head of Household (Name, Age, Gender, ID if available)
Number of family members
Children (Name, Age, Gender, Education status, Disability status, Vaccination status)
Pregnant/Lactating women

Section C: Socio-Economic Status

Income sources (agriculture, daily labor, none, other)
Access to PDS (Yes/No, card number if available)
Shelter type (permanent, temporary, rented, hosted)
Access to water, sanitation, electricity

Section D: Child-Specific Needs

Current school enrollment (Yes/No, grade)
Barriers to education (distance, costs, overcrowding, no school available)
Health issues (malnutrition, chronic illness, disability)
Child protection concerns (child labor, early marriage, psychosocial distress)

Section E: Access to Social Protection

Registered in Social Protection Network (Yes/No)
Awareness of entitlements (cash, food, health, education subsidies (As an Example, actual entitlements will be discussed with SP team Karwan and MOLSA later)
Assistance received (type, frequency, by which agency)

Section F: Priorities & Referrals

Immediate needs (food, cash, education, health, shelter)
Referral to: [ ] MoLSA [ ] MoE [ ] MoH [ ] Local NGO
Notes by social worker

ANNEX 2: Case Identification

Screening and Assessment Summary Form

Case Code:	**Date(s) Form Opened:** **Date(s) Form Reviewed:** **Date Form Closed:**	**Social worker:** **Department:**
How was the family identified: ☐During enrolment visit ☐SSN Renewals ☐Routine Family Visit & Monitoring ☐Referred by a third party. ☐ Family made contact. **Note**:		
Family Members Interviewed	☐Father ☐Mother ☐Main carer (other than parent) ☐Child (indicate who, and how many)	
Family Address & Contact Details **SSN Code**	**Provide full address and contact details and SSN code:**	
SPECIFY DOMAIN(S) OF IDENTIFIED ISSUE(S): **SPECIFY LEVEL OF RISK:** **DETAILS**: **ACTION:** ☐ **Refer** ☐ **Monitor** ☐ **No further action** ☐ **Issue addressed.** ☐**Urgent intervention in the next 24-48h** ☐ **Fuller Assessment Required**		

☐**Consent for referral was obtained**
1. ASSESSMENT WITH THE CHILD & CHILD WISHES
Child(ren) Name(s) & Age:
Main observations after speaking with the child(ren) (wishes, physical & emotional state, behaviour, safety and wellbeing)
DOMAIN 1. RISK ASSOCIATED WITH HOUSEHOLD COMPOSITION
☐Separated and Single Parent Families ☐ Large Family ☐ **Low Risk/Early Help** ☐ **Medium Risk/Complex Needs** ☐ **Acute Needs/High Risk** ☐ **Protective Factor** **Notes, Action taken during the visit, Further action recommended.**
DOMAIN 2. RISK ASSOCIATED WITH CHARACTERISTICS & CAPACITIES OF PRIMARY CAREGIVERS
☐ Caregiver has an age-related challenge to meet needs. ☐ Caregiver has a disability-related challenge to meet needs. ☐ Caregiver has a challenge to meet needs because it belongs to a Minority or Marginalised Group ☐ Caregiver has a challenge to meet needs because it is recently Displaced, Refugee ☐ **Low Risk/Early Help** ☐ **Medium Risk/Complex Needs** ☐ **Acute Needs/High Risk** ☐ **Protective Factor:** **Notes, Action taken during the visit, Further action recommended.**
DOMAIN 3. RISK ASSOCIATED WITH SOCIOECONOMIC STATUS
☐Low-Income Family ☐Employment Status: ☐Housing Instability ☐Geographic Location

☐High Risk Neighbourhood

☐ **Low Risk/Early Help** ☐ **Medium Risk/Complex Needs** ☐ **Acute Needs/High Risk**
☐ **Protective Factor:**

Notes, Action taken during the visit, Further action recommended.

DOMAIN 4: RISK ASSOCIATED WITH ADULT HEALTH CONDITIONS, DISABILITIES

☐Unaddressed Disabilities
☐Unmet Medical Needs
☐Significant Injury
☐Mental Health Issues

☐ **Low Risk/Early Help** ☐ **Medium Risk/Complex Needs** ☐ **Acute Needs/High Risk**
☐ **Protective Factor:**

Notes, Action taken during the visit, Further action recommended.

DOMAIN 5. RISK ASSOCIATED WITH CHILD'S WELL-BEING, HEALTH & EDUCATION

☐ Overall General Wellbeing & General Health:
☐ Child with Special Needs and/or Disability:
☐Child Mental Health
☐Educational Risk Factors
☐Child Support Network

☐ **No Risk** ☐ **Low Risk/Early Help** ☐ **Medium Risk/Complex Needs** ☐ **Acute Needs/High Risk**
☐ **Protective Factor**

Notes, Action taken during the visit, Further action recommended.

DOMAIN 6. CHILD PROTECTION CONCERNS

☐ General Protection of Children:
☐ Neglect:
☐ Physical Abuse:
☐ Emotional Abuse:
☐ Sexual Abuse:

☐ Child Marriage:
☐ Child Labour
☐ Child Substance Misuse/Exposure to Substance Misuse:
☐ Child in Conflict with the Law

☐ **Low Risk/Early Help** ☐ **Medium Risk/Complex Needs** ☐ **Acute Needs/High Risk**
☐ **Protective Factor**

Notes, Action taken during the visit, Further action recommended.

DOMAIN 7. RISK ASSOCIATED WITH GENDER-BASED VIOLENCE (GBV) & SUBSTANCE ABUSE

☐ Previous GBV Incidents
- ☐ Family members with history of perpetrating violence
- ☐ Family members with history of substance abuse
- ☐ Family members with history of mental health

☐ Risk Factors of GBV & Substance Abuse
- ☐ Disability
- ☐ Isolation of children, woman
- ☐ Fearful women and children
- ☐ Unemployment and/or financial strains
- ☐ Large family size
- ☐ Early marriage
- ☐ Coercive control
- ☐ Rigid adherence to traditional gender roles that subordinates women/normalises violence.
- ☐ Visible bruises on women/or children
- ☐ Any other factors

☐ History of Substance Abuse

☐ **Low Risk/Early Help** ☐ **Medium Risk/Complex Needs** ☐ **Acute Needs/High Risk**
☐ **Protective Factor:**

Notes, Action taken during the visit, Further action recommended.

DOMAIN 8 ADDITIONAL CONCERNS

☐ Caregiver Strain:
☐ Family Social Isolation:
☐ Unhealthy Family Dynamics:

☐ Psychosocial Concerns: ☐ Lack of Documentation: ☐ Legal Aid need: ☐ **Low Risk/Early Help** ☐ **Medium Risk/Complex Needs** ☐ **Acute Needs/High Risk** ☐ **Protective Factor:** **Notes, Action taken during the visit, Further action recommended.**
PROTECTIVE FACTORS:
☐ Individual Protective Factors Parents/Caregivers ☐ Child's Protective Factors ☐ Family Strengths & Resilience ☐ Community & Environmental Protective Factors

ANNEX 3: Draft Complaint form

First Name	**Second Name**	**Last Name**
Mother's name	**Applicant or beneficiary?**	**Governorate**
District	**Address**	**Phone number**
Department: Men dep Women Dep	**Qi Card Number if beneficiary**	**Do you want to submit:** • Compliment • Complaint • Comment
Date of the request	**Statement by person appealing**: This is my notice of appeal against .....TBC	**Which scheme is your comment, compliment or complaint about?** • SSN program • Education Grant • Cash Pilot • Food Basket ETC...

Details of your comment, compliment or complaint:		