NORWEGIAN REFUGEE COUNCIL

Terms of Reference

Humanitarian Data Protocol – Risk and Threats Modelling Consultancy

Summary

This document aims to describe the scope of the consultancy required for the Humanitarian Data Protocol project. It also describes the expected deliverables of the consultancy.

The objective of this consultancy is to:

- Map the risk and threat scenarios for data sharing between humanitarian organizations, with a specific focus on Cash Voucher Assistance (CVA) activities
- Evaluate how existing and emerging peer to peer protocols may mitigate or address those risks, using the output of the other research led by the IFRC on data protocols
- Determine the level of vulnerability of the data points based on levels of sensitivity and needs to share with other organizations
- Identify emblematic cases of attempted or successful intrusion or interference on the transfer layer in humanitarian, social, or development data sharing processes
- Define the technical specifications of the hostile and defensive tools or systems used in those scenarios and identify any blockages or challenges faced by entities in trying to protect the sharing of relevant data.

Time Schedule

The IFRC aims to follow the estimated time schedule indicated below:

Estimated start date	Estimated duration	Estimated Effort (days)
28.11.2022	3 months	40

Introduction

Background and business objective

The Norwegian Refugee Council (NRC) is an independent humanitarian organization helping people forced to flee. NRC works to protect the rights of displaced and vulnerable persons during a crisis. Through its programmes, NRC provides assistance to meet immediate humanitarian needs, prevent further displacement and contribute to durable solutions. To

fulfill its duties and respond to people's needs, NRC cooperates with other local and international partners also through the sharing of information and data.

Sharing data among humanitarian actors is necessary to ensure good coordination, speed up delivery of assistance including cash and vouchers, reduce duplication, and ensure the most vulnerable are not left behind. But due to disparate systems, lack of common data models, and risks to data protection and security, meaningful and responsible data sharing and interoperability is limited and difficult to achieve without costly custom integrations.

A consortium comprised of the International Federation of Red Cross Red Crescent, Norwegian Refugee Council, Save the Children Norway embarked in a journey to look at digital identities for people with no official IDs and started the Dignified Identities in Cash Assistance (DIGID) project. The DIGID consortium's vision of interoperability started with digital identities so affected populations are recognized by humanitarian organizations. The consortium acknowledges the need for a peer-to-peer data transfer protocol that will allow organizations to transfer not just beneficiary data but also other assistance-related data safely and securely, particularly for cash assistance where large amounts of data are used for decision making. A protocol is a standard set of rules that allows systems to communicate with each other.

To achieve this vision, the consortium is proposing Humanitarian Data Protocol project, to which this term of reference will support a critical activity in the first phase. The project will focus on mapping the existing landscape and challenges, research of technology options and how they address risks and threat models and the validation of the key findings from the research with partner organizations. The consortium will engage with humanitarian actors, private sector, and institutions looking into emerging technology to develop such privacy protecting protocols.

Learnings from the research and validation will be used to develop a roadmap for interoperability among humanitarian organizations and actions necessary towards safe and secure implementation. Such roadmap will include an approach for building technology and piloting in field settings. The DIGID consortium will coordinate with CCD consortium that will be working on a complementary project on interoperability focusing on digital wallets and identities (data portability).

The overall objective of the project is to strengthen the humanitarian sector's ability to securely share data between organizations and with affected individuals related to the identification of beneficiaries and services provided to them through the development of a set of protocols and data sharing standards that both reduce the risk of data breaches and the loss of personally identifiable information of people at risk, while also promoting interoperability and user control.

Consultancy requirements

The NRC is looking for a consultant who will be able to:

- Map the risk and threat scenarios for data sharing between humanitarian organizations, with a specific focus on Cash Voucher Assistance (CVA) activities
- Evaluate how existing and emerging peer to peer protocol may mitigate or address those risks, using the output of the other research led by the IFRC on data protocols
- Determine the level of vulnerability of the data points based on levels of sensitivity and needs to share with other organizations
- Identify emblematic cases of attempted or successful intrusion or interference on the transfer layer in humanitarian, social, or development data sharing processes
- Define the technical specifications of the hostile and defensive tools or systems used in those scenarios and identify any blockages or challenges faced by entities in trying to protect the sharing of relevant data.

Proposed organizations to include in the consultation (list to be refined in the project):

- UN agencies, and affiliated entities (e.g., WFP, UNHCR, HDC),
- CCD network (a group of 14 NGOs) & other NGOs,
- Red Cross Red Crescent network (e.g., ICRC, National Societies)
- Privacy and Digital Rights organizations (AccessNow, EFF, EDRI, Open Technology Fund)
- Research centers working on cybersecurity (Stanford Security Laboratory, Center for Secure Information Systems).

The consultant will make sure the list of organizations covers different types of organizations working at different scale and in different contexts, also outside of the humanitarian space.

Key questions to be explored during the consultation (non-exhaustive list, to be refined in the project):

1. Does the project's problem statement resonate with the consulted organizations?
2. How important is the integrity and security of data transfer for consulted organizations? Would there be benefits from enhancing the safety of data sharing systems? What are the most critical data points that organizations would want to be able to share with/ obtain from others organization? Why?
3. Which scenarios currently in-scope for consulted organizations, including for CVA activities, require or would benefit from safer data transfer mechanisms and protocols?
4. What are the most common risks and threats related to the data transfer protocol when it comes to data sharing? And what are the most severe? How do they commonly operate?

5. What kind of example can be found of attempted or successful intrusion or interference on the transfer layer in humanitarian, social, or development data sharing processes?
6. What are the tools or systems currently used by the organizations to prevent or mitigate the most common risk scenarios?
7. What are the primary data types targeted in the risk\threat scenarios mapped? What is the level of sensitivity of those data points? i.e. confidential (personally identifiable), public, restricted.
8. Where do the organizations' targeted data reside before and\or after the compromised data transfers (e.g. on-premise, in the cloud, using databases, in Excel files, etc.)?
9. What are the specific challenges and issues related to improving the safety and security of data sharing and interoperability from a technological standpoint?
10. Have the organizations already identified any potential solutions, or have any recommendations to address the challenges/ issues faced?
11. To which extent consulted organizations are prepared to promote, implement, and support an interoperability protocol once available?
12. Do consulted organizations have any existing or future technical/research work that is relevant with this project's objectives? And any opportunities to collaborate?

Goal and deliverables of the consultancy

Expected deliverable for this consultancy include:

- Inception Report including methodology, confirmation of high-level timeline, proposed activities & milestones to achieve the objectives of the consultancy, also include risks to mitigate in the project,
- Literature review summary including highlights on gaps that need further research,
- Documented meeting minutes after all consultations,
- Slide decks and other materials as required to support the running of the consultations,
- Regular reports and updates – written or oral, as required and requested – to the project core team, in particular the project manager.
- Final report, setting out analysis and findings, summarizing the risk \ threats landscape, the common vulnerabilities in CVA data sharing scenarios across organizations, the technical challenges detected while securing the sharing data and relevant data points prioritized by consulted organizations. The report should also include:
    - A list of the organizations and relevant contacts engaged in the process,
    - A mapping of the risk\threat scenarios that are commons to humanitarians' organizations executing Cash Transfer programs,
    - A list of the primary data points and data type for those scenarios, ordered by priority based on the value it would represent for another organization, and with an assessment on its level of sensitivity,

    - An evaluation of system and techniques used to mitigate/ address relevant risks through existing/emerging protocol
    - A list of the challenges currently faced by the organizations (i.e. technical, sensitivity, etc…) to secure these primary data points
    - A selection of concrete case studies based on documented events relevant to the topic
    - Summary of key insights and recommendations from the consulted organizations.
- Validation workshop with key stakeholders to enable finalizing of final reports as needed; sharing of draft versions of the report with relevant stakeholders, via the NRC\IFRC project focal point, for feedback before being finalized.

The consultant is expected to work independently, with minimal supervision, and be able to assume and manage the responsibility for assigned fields of expertise. The consultant will report to the NRC Digital Specialist and to the IFRC Project Manager and will get technical support from the project core team subject matter experts, as needed.

Consultant location

The work of the consultant is expected to be conducted remotely. Given that the consultations will involve stakeholders from different time zones, some flexibility will be expected from the consultant to attend important meetings and accommodate time zone differences. Being based or have ability to travel to Geneva is a nice to have.

Consultant knowledge and skills

Required:

- Strong knowledge of cybersecurity essentials, familiarity with data transfer and protocol layer technologies
- Strong analytical skills, ability to abstract and represent graphically
- Mapping of business processes to systems/tools
- Experience in data analysis
- Understanding of data models, data governance and policies
- Proficient in assessing data security and data protection, including risk management
- Knowledge of Cash and Voucher Assistance in the humanitarian sector
- Experience working with non-profit sector particularly humanitarian organizations
- Ability to work and coordinate with various stakeholders
- Experience with remote facilitation
- Excellent writing and communication skills
- Ability to work within a multi-cultural, multilingual, multidisciplinary environment
- Fluent in English

Preferred:

- Has a network of technology providers, research or advocacy institutions, innovation labs, and thinktanks, that could help advise or contribute to the discussions around systems interoperability
- Engineering\ICT degree and\or Business analysis certification or experience in business analysis of tech systems
- Knowledge of other languages

Schedule for payment of fees

Monthly or single invoice with activity reports, to be paid upon validation and acceptance of deliverables by reporting lines.

Proposal requirements

Proposal should include consultant's resume or CV, a summary of relevant experiences, daily rate (in CHF) and an estimate of the efforts (in days) with dates of availability.

Errata corrige: This application is open to both individuals and companies, not only companies as previously erroneously communicated.

Deadline for submission is November 12, 2022 at midnight CET

Applications should be submitted at the following addresses: giulio.coppi@nrc.no **and** tariq.riebl@nrc.no with the following subject: **ECHO HDP 2022 – Risk Threat Modelling**

Focal points

NRC Digital Specialist: Giulio Coppi

NRC PSIU Director: Tariq Riebl

IFRC Project Manager: Thomas Raffort

IFRC Cash Transfer Programming: Joseph Oliveros

-End of the document-