TESS Stream 3: Request for Technology Solutions (RTS)

Please read this document before filling in the accompanying RTS response template spreadsheet. Proposals must be submitted by email to TESS@wfp.org by midnight (GMT+2) on 31 August 2019.

1. Background

The safety and security of UN/NGO personnel is an essential consideration when planning operations. Security Communications Systems (SCS), also referred to as 'security communications', are often the only way to communicate in remote and challenging areas. SCSs are also one of the key tools to support UN/NGO personnel during security incidents.

Technology is changing the way that the United Nations (UN) and non-governmental organisations (NGOs) plan field operations. This change is also influencing how we manage UN/NGO security communications. Acknowledging this change, the Telecommunications Security Standards project (TESS) was initiated in 2018 to review the current UN/NGO SCS standards and propose a new way forward based on the new business requirements.

TESS is an interagency project, requested and initiated by the Inter-Agency Security Management Network (IASMN) and the Emergency Telecommunications Cluster (ETC), and mandated by the United Nations Department of Safety and Security (UNDSS). The project is facilitated by the World Food Programme. The TESS project is managed in three separate project tracks ("streams"), this RTS relates to TESS Stream 3 – the longer term standards.

TESS is looking to test technology-based connectivity solutions that will improve the overall usability of SCS for UN/NGO personnel while lowering costs and increasing operational efficiency.

This RTS document outlines eight use cases (scenarios) and related technical requirements that the UN/NGO community is seeking to find viable security communications solutions to match.

While TESS works on three layers: connectivity, applications and procedures, this RTS is specifically looking at solutions that fulfil the *connectivity* layer requirement. The application and procedure layers will be addressed separately to this RTS.

The outcome of this RTS process will be a shortlist of technologies that will be taken forward to a TESS laboratory and field test phase to validate if the proposed technologies meet the stated requirements of the future UN/NGO security communications standard. The TESS project's final objective is to define the new UN/NGO security communications standard and put it to the IASMN for endorsement in June 2020.

This RTS is not part of a procurement process and, as such, approximate and non-binding pricing estimates for investment and running costs are welcome, but not required, in response to this RTS.

For more background on the TESS project visit the ETC website at this link: www.etcluster.org/telecommunications-security-standards-tess-project/

2. Architecture

As stated in the background section above, TESS Stream 3 is focused on three layers:

Layer	Description	In the scope of this RTS?
1. Connectivity	The platform that provides data connectivity to a user anywhere and anytime.	**Yes**
2. Application	The application software that users' and the Security Operation Centre employ to communicate between each other from their user device.	No
3. Procedures	The supporting security procedures documented as a set of business processes that users must comply to.	No

The "connectivity" layer architecture of the security communication system (SCS) has three minimum mandatory requirements that are outlined in the following table. All three of these requirements must be met by the solution proposed for each use case presented in the next section.

Layer	Mandatory Minimum Requirement	Description	RTS
1. Connectivity	a. Bring Your Own Device (BYOD)	End-users can use their own smartphone device to connect to the SCS data connection.	**X**
	b. Data only	The SCS connectivity layer must ensure each user device (mobile smartphone) has, at all times and no matter where they are, a data connection with a minimum bandwidth of 40 kbps (uplink/downlink) to the public internet to cater, at minimum, for a VoIP connection through commercial and public applications such as Whatsapp, Signal, Viber, etc.	**X**
	c. Security Operations Centre (SOC) communication	The SCS data connection must allow any end-user smartphone device, at any time and from anywhere, to contact/connect to the Security Operations Centre (SOC). Equivalently, the SOC must be able to contact/connect any end-user smartphone device at any given time via the data connection, no matter the user's physical location. The SOC is a hub site, situated within the operational area, that provides safety and security support to	**X**

		UN/NGO personnel ("end-users") in the field and connects to the users via a public internet data connection.	

3. The UN/NGO context and related use cases

UN/NGO operations are carried out in different contexts, in response to different types of development work, crises or emergency events, that occur over different timeframes. A UN/NGO worker ("user") operates in a diverse range of contexts and environments which have different personal and organisational security implications.

As such, UN or NGO personnel might be working in urban settings, a field office location or spread across unpredictable deep field locations. Irrespective of their environment or context, a user must be able to access the SCS at all times no matter where they are..

TESS has defined eight specific use cases that pose a technical challenge to provide data connectivity services to users using commonly available connectivity methods easily found in a "stable" environment. These "problem" use cases are defined in the table below.

Use Case Reference	Description	RTS
Use case 1: **"Lone Ranger"**	A single user is located in a remote area (anywhere in the world) where there is no public mobile data service available. The user must have a two-way (up/down) data connectivity service to their mobile device irrespective of their location or time of day.	**X**
Use case 2: **"Lone Vehicle"**	While on mission a vehicle with several end-users drives through a remote area (anywhere in the world) where there is no public mobile data service available. The vehicle, and each (up to 5 per car) users in and around the vehicle must have a two-way (up/down) data connectivity service to their mobile device irrespective of their location or time of day.	**X**
Use case 3: **"Camp"**	End-users work in a well-defined and physically confined geographical area, e.g. a refugee or resettlement camp, a work compound, or a staff accommodation complex. All users must have a two-way (up/down) data connectivity service to their mobile device irrespective of their location in the geographical area or time of day. Number of users between 5 up to many hundreds. For planning purposes assume at least 1 square kilometre camp size.	**X**
Use case 4: **"Rapid Deployment Camp"**	This is a variant of the "Camp" use case but in the context of a rapid deployment operation where data connectivity needs to be established within a very short lead time. Typical context will be: 1) a sudden	**X**

	onset disaster (eg. earthquake, cyclone, flood) where end-users surge into a geographical area to manage the UN/NGO response, or 2) temporary camp for a displaced population. Number of users between 5 up to many hundreds. For planning purposes assume at least 1 square kilometre.	
Use case 5: **"Disconnected City"**	This is a variant of the "Camp" use case where end-users work in a larger geographical area, e.g. a city or town, where there is no public mobile data service available. Number of users between 5 up to many hundreds.	**X**
Use case 6: **"Brown Out"**	This use case caters for operations where in normal day-to-day operations there is a public mobile data service available but, for any given reason, the normal data service becomes suddenly and temporarily unavailable for hours or days (while the mobile voice/SMS service remains up). In this use case, the user requires a two-way (up/down) data connectivity service to their mobile device on a contingency basis when the normal public data network is unavailable. Number of users between 5 up to many hundreds.	**X**
Use case 7: **"Black Out"**	This is a variant of the "Brown Out" use case where all fixed and mobile network operator services (voice/SMS *and* data) fail or are unavailable. In this use case, the user requires a two-way (up/down) data connectivity service to their mobile device on a contingency basis when the normal public data network is unavailable. Number of users between 5 up to many hundreds.	**X**
Use case 8: **"No Data Roaming"**	This use case caters for instances where data services on the local mobile telephone networks are available, but data roaming onto these networks is either unavailable, limited, or too expensive to use. In this use case, the user requires a two-way (up/down) data connectivity service to their mobile device. This use case caters for users that travel frequently for their work to any location in the world.	**X**

4. How to respond to this RTS

This is a public and open call for proposals to propose technology solutions for one or more of the above use cases that satisfy the stated mandatory minimum requirements. The proposals should be based on solutions from the responding company or organisation.

Proposals must be submitted by email to TESS@wfp.org by midnight (GMT+2) on 31 August 2019. All questions in the response template spreadsheet must be answered in the template and submitted with any supporting documentation.

5. Where do we go after the RTS?

- **31 August 2019:** deadline for RTS submissions.
- **16-18 September 2019:** meeting in Munich, Germany, for shortlisted organisations to pitch their proposed technology solutions in person or online. The objective of this meeting will be to shortlist those proposals that will be invited to the test phase. Note: an opportunity for public pitching as well as closed pitching to members of the TESS Inter-Agency Steering Group will be possible.
- **30 September 2019:** The TESS Inter-Agency Steering Group shortlists technology solutions deemed useful for laboratory (lab) and field testing.
- **November 2019 to April 2020**: lab and field testing of selected solutions shortlisted from the RTS process.
- **June 2020:** TESS recommendation for the future UN/NGO SCS standards to be presented for formal endorsement to the Interagency Security Management Network (IASMN) and the Emergency Telecommunications Cluster (ETC). This recommendation will be based on technological solutions, and will not be linked to specific products, vendors and manufacturers.
- ***Beyond June 2020:*** a tender process is scheduled to be launched based on the new future UN/NGO SCS standards endorsed by the IASMN. This process will be open to any supplier, vendor or manufacturer, irrespective if their technology has been involved in the field tests or not. This tender process is outside of the scope of TESS Stream 3.

6. When answering this RTS, please be informed:

- This RTS is a non-binding inquiry and does not constitute a solicitation, and is not part of a tendering process. The TESS project reserves the right to change or cancel this process or any of its requirements at any time during the process.
- The purpose of this RTS is to obtain concrete proposals that describe technical connectivity solutions which can meet technical requirements in one or more of the eight defined use cases described in this RTS document.
- This RTS is a non-committal process. As such, it is not a requirement to provide financial information at this stage of the process. If financial information (e.g. for investment and running costs), these will be considered as indicative, informal and non-committal.
- The information contained in your proposal will be evaluated on a technical basis to determine if your proposed solution(s) will be taken forward to the lab/field testing phase of the TESS project.
- By submitting your proposal, you agree we can use your input as part of the TESS project, and can be discussed publicly.
- The proposals will be reviewed by the TESS Interagency Steering Group, which consists of project stakeholders including inter-agency partners coming from UN agencies, NGOs, ETC partner organisations, and other entities enlisted to provide technical

support. Any confidential information in the proposals or subsequent discussions will only be open to the abovementioned parties.

- When you submit your response, you must disclose any restriction on the use or realisation of your proposal that you know of, such as the need for a license in respect of any proprietary technology or other intellectual property rights.
- Subject to any restrictions that you have disclosed, you agree to grant the World Food Programme (WFP), as facilitator of the TESS project, a non-exclusive, transferable, sub-licensable, royalty-free, perpetual, irrevocable, right and license to use, reproduce, publish, translate, sub-license, copy, modify, delete, enhance, distribute and otherwise exploit your proposal in any way, in connection with WFP's mission and the TESS project. You acknowledge that WFP has no duty of confidentiality, attribution or compensation for your proposal, and you agree to indemnify, defend and hold WFP harmless if you or anyone else claims otherwise, claims they have rights in your proposal or if your proposal otherwise violates applicable laws.
- Nothing in this document, or any other document entered into in connection with the TESS project, shall imply a waiver, expressed or implied, by WFP, the United Nations and the Food and Agriculture Organization of the United Nations of any privileges and immunities enjoyed by them pursuant to the 1946 Convention on the Privileges and Immunities of the United Nations, the 1947 Convention on the Privileges and Immunities of the Specialized Agencies, customary international law, other relevant international or national agreements, and under domestic law.