UNSMS

Security Management Operations Manual

Chapter XVII

GUIDELINES ON SECURITY COMMUNICATIONS SYSTEMS

Promulgation Date: March 2021
Version 5.1

Table of Contents

A. Introduction 2
B. Purpose of this document 2
C. SCS purpose and components 2
D. SCS connectivity requirements and scenarios 3
E. Implementing a country-based SCS 4
F. Standards for the use of the public mobile phone networks as SCS 5
G. Standards for the use of VHF/UHF radio networks as SCS 6
H. Standards for the use of satellite phones as SCS 8
I. Training 8
J. Final provisions 8
Annexes

Version 5.1
(March-2021)

A. Introduction

1. Security communications have changed over the years due to advances in technology. In response, the United Nations Security Management System (UNSMS) also modified the earlier approach and language around "Emergency Security Communications" (ECS) to support the overall security communication needs under all circumstances, and not only in emergencies.

2. Consequently, the UNSMS migrated its security communications approach from ECS, supported by conventional radio rooms, to security communications systems (SCS) supported by Security Operations Centres (SOCs) and implemented through the appropriate Standard Operating Procedures (SOPs).

3. To support these changes through new standards, an interagency collaborative project was adopted in 2018, referred to as the "Telecommunications Security Standards" (TESS) project. In 2020, this project was converted into a continuing service, called "{TESS+}".[1]

B. Purpose of this document

4. This document provides guidance on the adaptation to these changes, based on the findings and recommendations of the TESS project, while the TESS team continues to provide operational and tactical advice and support.[2]

5. The goal of this document is to provide practical overall guidance on the identification, implementation, operation, support and use of SCS by the UNSMS in support of the safety and security of UNSMS personnel.

C. SCS purpose and components

6. The SCS consists of a combination of technology solutions (connectivity and applications) and the relevant supporting SOPs.

7. The ultimate purpose of the SCS is for a SOC, or the local security point of contact, to be able to contact (and be contactable by) all UNSMS personnel, vehicles and offices within each operational area[3] at any given time.

[1] See Annex A for details on TESS and {TESS+}.
[2] See also paragraph 15 and Annex A.
[3] An operational area in this context can be defined as the Designated Area, Security Area or Security Risk Management Area.

8. If required by the Security Risk Management (SRM) process, the SCS should be monitored/operated by either a local or a remote SOC[4]. If no SOC is to be established for an operational area, UNSMS personnel should have at least one local security point of contact.

D. SCS connectivity requirements and scenarios

9. Each operational area should have the following connectivity setup:
    a. A primary SCS (supporting "operations as usual") and;
    b. A backup SCS (supporting "exceptional" or "emergency conditions" where the primary SCS has failed or is no longer available).

10. The applicable connectivity for a specific operational area can be determined using the following three scenarios:

10.1 Scenario A: Full availability of public mobile phone networks[5] for security telecommunications: This scenario covers an operational area adequately covered by a public mobile network infrastructure that is reliable, and has sufficient built-in redundancies.[6]
In this scenario, the primary SCS should be the public mobile phone network, and the backup SCS can be, for example, satellite systems for key UNSMS personnel.

10.2 Scenario B: Public mobile phone networks are available, but prone to downtime: This scenario covers an operational area where the public mobile phone network coverage is deemed sufficient for day-to-day operational and security communications, but is prone to occasional overload, is vulnerable to natural disasters, or shows occasional network unavailability due to capacity issues or political events.
In this scenario, the primary SCS can be the public mobile phone network, supporting "business as usual" operations but also requires a well-tested fallback or redundancy security telecommunications system in case the public mobile phone networks fail. Based on local parameters, this backup SCS might be a stand-by VHF/UHF radio network, a satellite-based solution for key UNSMS personnel, or other types of reliable communications systems.

[4] A Remote SOC is any SOC which is not physically located in the operational area, but is designated to support this operational area.

[5] A public mobile phone network is a public network providing telephony (voice), SMS and data services over a cellular network.

[6] See Annex E for a template checklist to assess a public mobile phone network.

10.3 Scenario C: Reliable public mobile phone networks are unavailable in the operational area: This scenario covers an operational area where the public mobile phone network service is insufficient or not sufficiently reliable, prompting the UNSMS to implement its own proprietary security telecommunications networks. The combined use of VHF/UHF networks (linking offices, UNSMS personnel and vehicles to SOCs) and satellite phones should be used as SCS.

E. Implementing a country-based SCS

Identifying the appropriate SCS

11. For each operational area, the final decision on security communications rests with the Designated Official (DO) and should be justified through and included in the country's SRM.

12. As part of the security planning arrangements, the most senior security professional[7] advises the DO/Security Management Team (SMT) in identifying the appropriate SCS for each operational area, based on the guidance of the TESS Team and local ICT Working Group (ICTWG) and in consultation with the Operations Management Team and Security Cell.

13. Identifying the appropriate SCS includes defining the primary and backup SCS connectivity systems, the applications, and the appropriate SOPs.

14. The choice of the appropriate connectivity technology of the SCS in a particular operational area depends on the local security environment, as assessed through each country's SRM process while also considering the technical readiness or constraints, costs, training and available support for both the primary and backup SCS as a security risk management measure.

15. As such, the identification of the appropriate SCS connectivity systems is a complex evaluation process, completed outside the SRM methodology and requiring specialised technical skills which may not be available locally. The TESS project, under the governance of the TESS Interagency Steering Group, is the main global focal point for advice on the SCS in the UNSMS, working closely with the Communications/ICT technical personnel in UNSMS organizations, UNDSS, the Inter-Agency Security Management Network and other UNSMS and NGO stakeholders. The single point of

[7] This is usually the Principal or Chief Security Adviser (P/CSA) or a Security Adviser (SA), including their officer-in-charge ad interim. Where a P/C/SA is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services, Country Security Focal Point (CSFP) or Local Security Assistant (if necessary) in countries where no international professional security adviser has been assigned or is present.

contact for TESS (and its longer-term institutionalized service {TESS+}) is TESS@wfp.org.

Country-level technical coordination, guidance and support

16. As standard practice, when feasible, each country should establish an ICTWG, comprising of the IT and telecommunications technical personnel from all UNSMS organisations, to be the local focal point for technical support and advice on the SCS to the most senior security professional, the Security Cell and the SMT. The Chair of the ICTWG can be invited to SMT meetings, as a technical advisor/expert. If local expertise is not available to form an ICTWG, TESS will provide direct advice and support to the most senior security professional, the Security Cell and the SMT.

17. TESS will provide onsite or remote guidance and support to field operations in the identification, the deployment and the operations of appropriate SCS connectivity solutions (including the identification of the primary and backup SCS), applications and procedures. All field operations will avail themselves of the TESS resources and expertise, who will make their SCS recommendations in consultation with the local ICTWG, security professionals and security focal points. The country UNSMS is strongly encouraged to adopt and implement the TESS assessment recommendations.

SOC and SOC staffing

18. The UNSMS-adopted standard for SCS is gradually moving away from the traditional radio-only systems. The concept of traditional "radio rooms" no longer reflects their role in the current and more diversified systems (such as automated vehicle tracking systems, customized security applications like eTA or SCAAN, and digital message broadcasting systems). In view of this, the term " SOC" should be used[8], as a more appropriate term, instead of "radio rooms".

19. Likewise, the term "SOC Assistants" should be used, rather than the legacy term "radio operators".

20. The Terms of Reference for the SOC and SOC Assistants should, therefore, be adjusted to appropriately reflect their roles and new tasks. Generic templates for these two TORs are attached in Annexes B and C. Based on these, the job positions for SOC Assistants should be properly graded to reflect their redefined roles and responsibilities.

F. Standards for the use of the public mobile phone networks as SCS

[8] It is recognized that not all operational areas will have the capacity to operate an onsite SOC and that alternative options are needed to be compliant with SCS requirements - including access to a security management hub (possibly with a 24/7 coverage). This is further elaborated in Annex D.

21. In cases where the use of the mobile phone network is adopted as primary or backup SCS, the SRM process should assist UNSMS members to determine which of their personnel should have access to smartphones and a mobile phone network, supported by a local contract with the appropriate mobile phone service provider(s).

Recommendations for country-level mobile phone contracts

22. At the country level, the Operations Management Teams should take the lead in negotiating a competitive contract with one or more local mobile phone network operators, preferably with one lead agency signing the agreement on behalf of all UNSMS organizations represented locally.
The individual UNSMS organizations should be able to benefit from the negotiated contract(s) under the umbrella negotiated terms and conditions of the contract(s). However, it will be the responsibility of each UNSMS organization, in line with their own internal procurement processes, to approve the process and contract.

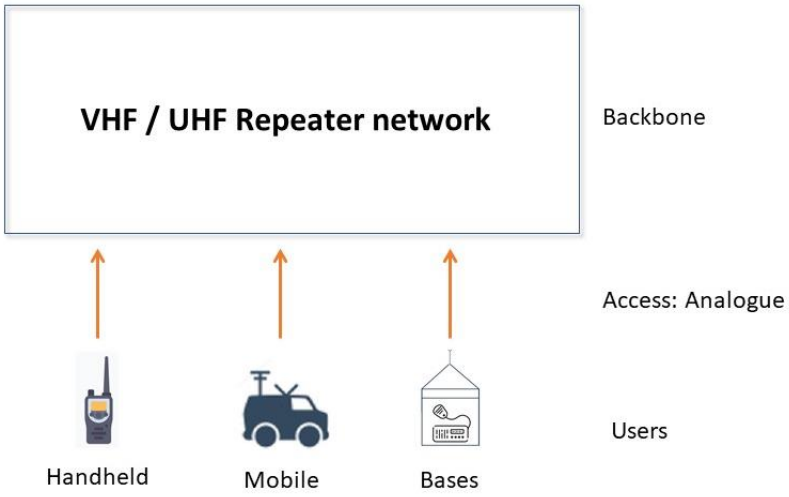
23. As a generic recommendation, these contracts can have the following features:
    a. All mobile phones from UNSMS personnel should be integrated into a "UNSMS fleet contract";
    b. The UNSMS fleet contract should define a fixed monthly rate for each mobile phone used by UNSMS personnel;
    c. Unlimited voice calls and SMS amongst the phones within the UNSMS fleet contract;
    d. At least 1 GB (Gigabyte) of data traffic per month;
    e. At least 1 hour of "off-fleet" voice calls per month (defined as voice calls with users outside of the "UNSMS fleet" mobile phones or to local landlines);
    f. A dedicated UNSMS support focal point from the mobile phone provider;
    g. A bulk SMS function, where a local SMS number can be used for the automated dispatch of security broadcasts via SMS by the SOC;
    h. Monthly invoicing to be done per UNSMS organization, for each of their subscriptions;
    i. Pre-agreed voice, SMS and data rates (including roaming charges) for those identified users who are permitted to use the service beyond the standardized UNSMS fleet contract flat rates.

G. Standards for the use of VHF/UHF radio networks as SCS

24. The use of VHF/UHF radio networks as SCS should follow the three scenarios indicated in paragraph 10. In the Scenarios A and B, VHF/UHF radio networks can be used as backup SCS. In Scenario C, they can be used as primary SCS.

VHF/UHF radio network standards

25. Where new VHF radio networks or extensions to existing VHF radio networks are being installed, these are required to *provide analogue VHF user access onto a VHF backbone.* The VHF backbone (the repeater network itself) can be either analogue or digital equipment, but the user access should be analogue.



26. The VHF networks used as SCS must include two basic user features:
    a. Have a basic ”Push to Talk" feature, where users can easily reach all other users in the UN security communications network; and
    b. Support the current standard user equipment features such as "call ID broadcast", remote stunning of radios by the network operators using the current SelV functionality.

27. Newly installed common VHF security communications networks – and those being upgraded – are to be compatible with any and all analogue VHF user equipment (mobile radios and handhelds) and with digital VHF user equipment, to be programmed in analogue mode, and to support the two basic features specified in paragraph 26.

28. This standard for the supporting backbone configuration (repeater network) is an "open" architecture which can be based on either:
    a. Legacy analogue VHF repeater systems, or
    b. Digital repeater systems (DMR, Mototrbo, dPMR or TETRA) where in all cases, the user access should be analogue, supporting the basic features outlined above.

    TETRA systems are only to be used when the SCS is based on an existing UN mission’s TETRA digital network and where no other alternative is possible.

29. The choice of the configuration for the VHF SCS systems will depend on local conditions, systems already deployed, and input from the UNSMS SCS supporting agencies, as long as they fall within the above standards.

30. While the use of VHF for short distance radio networks is preferred, in locations where VHF licenses are unavailable or restricted, UHF networks can be supported, based on the same standard VHF architecture. In this case the term "VHF" can be replaced by "UHF" in the above guidelines.

31. For any operation where additional guidance is required, the TESS team will provide support and advice.

32. This VHF/UHF SCS standard only applies to the common SCS and does not restrict specific UNSMS organizations from using different standards for their internal communication needs.

H. Standards for the use of satellite phones as SCS

33. The use of satellite phones as SCS follows the three scenarios indicated above. In Scenarios A, B and C, satellite phones can be used as backup SCS for key UN personnel, and can be used as primary or backup SCS for offices and vehicles.

I. Training

34. The TESS team will work in collaboration with the Security Training Working Group to make recommendations to the Inter-Agency Security Management Network on the content and format of specific awareness or training packages for security personnel and other personnel involved in the use, design, implementation and support of Security Communications Systems. Where possible and needed, the TESS team will contribute to the design and content of the relevant awareness and training packages.

J. Final provisions

35. These guidelines supersede the UNDSS Communiques dated 30 July 2018 and 29 April 2019 which provided guidance on SCS.

Annexes to the SMOM Guidelines on Security Communications Systems– Release 1 - Draft Version 8.0 (31-Dec-2020)

Annex A: Background on TESS and {TESS+} 3

Annex B: Template TOR for Security Operations Centres 6

Annex C: Template TOR for Security Operations Centre Assistants 9

A. Introduction 9

B. Typical duties and responsibilities for a SOC Assistant 9

C. Competencies 10

D. Required skills and experience 11

Annex D – Guidance for operational areas without the physical presence of a Security Operations Centre 12

A. Background 12

B. Overall approach 12

C. Recommendations 12

Annex E – Guidelines for the technical evaluation of a mobile telephone network's suitability as a security communications systems tool 15

A. Introduction 15

B. Background 15

C. Responsibilities 16

D. Process 16

E. Information gathering 16

F. Analysis 22

G. Conclusion/recommendation 24

Annex F – Guidelines on the role of the ICT Working Group in support of a Security Communications System 25

A. Introduction 25

B. Governance 25

C. Roles and Responsibilities 25

D. Terms of Reference: Tasks related to supporting the SCS 25

Annex G – Standard Operating Procedures for Movement Monitoring 27

A. Introduction 27

B. Definitions 27

C. Roles and Responsibilities 29

D. Means of communications 30

E. Prior to departure 31

F. During mission movement 31

G. Arrival at final destination 31

H. Incident handling 31
I. Daily reporting 32
Annex H – Standard Operating Procedures for Communications Checks 36
A. Introduction 36
B. Responsibilities 36
C. Frequency 37
D. Equipment and networks check 37
E. Reporting 37
F. Notes related to headcount 38
Annex I – Guidance for the maintenance of a radio-based security communications system 39
A. Introduction 39
A. Roles and Responsibilities 39
B. Planning 39
C. Implementation 40

Annex A: Background on TESS and {TESS+}

A. Historical Background

1. Interagency standards for the United Nations Security Management System (UNSMS) security communications systems (SCS) were initially established in the late 1990s by UNSECOORD and an informal interagency technical working group, consisting of UNHCR, UNICEF, DPKO and WFP. These standards were expanded and formalized into the Minimum Operational Security Standards (MOSS) as outlined in the Field Security Handbook of 2006, which preceded the *Security Policy Manual* and the *Security Management Operations Manual*.

2. In 2009, reference was made to the standards within the MOSS Policy as part of the *Security Policy Manual*. At that time, guidance was provided by the Working Group on Emergency Telecommunications.

3. With subsequent amendments to security policies and the revision of the Security Risk Management Policy, which took into account MOSS and Security Risk Management measures, specific responsibilities for security communications were not identified nor provided to any entity.

B. The TESS Project

4. As of May 2018, at the request of the Inter-Agency Security Management Network (IASMN), which is chaired by UNDSS, and the Emergency Telecommunications Cluster (ETC), which is chaired by WFP, a new interagency collaborative project, called Telecoms Security Standards (known as TESS), was created to re-standardize the SCS for both existing and future purposes.

5. Coordinated by WFP, TESS works in collaboration with all UNSMS entities (represented through the IASMN), in consultation with NGOs (represented through the ETC), individual communications and security experts, the private and public sector.

C. The conversion of TESS to {TESS+}

6. In January 2020, the IASMN and ETC endorsed the conversion, as of July 2020, of the TESS project into {TESS+}, a permanent and institutionalized support service to the UNSMS and NGO community, with a mandate, budget, service deliverable and governance structure similar to TESS.

7. In the overall *Security Management Operations Manual* SCS guidance and procedures, the terms “TESS” and “{TESS+}” are used interchangeably and refer to both TESS as a project and {TESS+} as an institutionalized service.

D. The TESS and {TESS+} mandate

8. In July 2018, UNDSS issued a communiqué, endorsed by the ETC and the IASMN, noting that TESS has been mandated to provide clear recommendations on the

standardization of future UNSMS security communications systems (connectivity, applications and procedures) and to inform UNSMS decision makers and stakeholders to streamline their field investments for future security telecommunications services.

9. In January 2020, the IASMN agreed to extend the mandate to {TESS+} as a permanent, institutionalized service, which was also endorsed by the ETC. Beyond its mandate for longer term standardization on SCS systems, TESS and {TESS+} aim to provide active field support, guiding and assisting the UNSMS in establishing pragmatic and cost effective SCS solutions. This includes:

    a. Assessing (remotely or on-site) field SCS systems and making pragmatic recommendations;
    b. Providing on-site or remote guidance and support to field operations in the identification, deployment and operation of appropriate SCS connectivity solutions (including the identification of the primary and backup SCS), applications and procedures;
    c. Providing direct advice and support, to the local ICT Working Group (ICTWG), and to the most senior security professional, the Security Cell and the Security Management Team (SMT);
    d. Providing field support resources, where needed, to assist in implementing SCS recommendations, and critical upgrades and technical support.

10. As such, TESS is the primary global focal point for guidance and support on SCS in the UNSMS, working closely with Communications/ICT technical personnel of UNSMS organizations in addition to security personnel of the UNSMS and NGO stakeholders. At the country level, UNSMS entities are strongly encouraged to adopt, implement and use the TESS recommendations and guidance.

E. The TESS and {TESS+} governance structure

11. The overall final responsibility and accountability for TESS and {TESS+} lays with the TESS/{TESS+} Senior Programme Manager, who also acts as the main coordinator and facilitator.

12. The core of the TESS governance structure is the TESS Interagency Steering Group (TESS IA SG), which assembles the five main technical SCS field service providers (UNICEF, UNHCR, OICT/DOS, WFP and ETC), as well as the key business client stakeholders (UNDSS, ETC [representing NGOs] and the IASMN).

13. The TESS IA SG, in consultation with the TESS Technical Working Groups (representing all TESS IA SG stakeholders) and with *ad hoc* advice from the TESS online community, defines the higher-level project or service direction, technical SCS architectures, and priorities.

14. The TESS core project team is the “operational arm” of TESS, consisting of subject matter experts. The core project team is responsible for the field assessments, field support and coordination of all technical tests, and input to other processes, such as the design of training and manuals, and input into commercial contracts.

15. In the field, the TESS core project team works closely with the UNSMS stakeholders (on the security side), the ICTWGs and the regional/headquarters ICT personnel from UNSMS organizations. This collaborative team is generally referred to as "the TESS team".

Annex B: Template TOR for Security Operations Centres

A. Introduction

Within the changing context, applicability and implementation of newly available technologies, security communications systems (SCS) have changed from the traditional radio-only systems, supported by radio rooms and staffed by radio operators, into Security Operations Centres (SOCs), staffed by SOC Assistants. Accordingly, their evolving role and activities have been recognized and require a standardized terms of reference (TOR), for SOCs and SOC Assistants.

This annex provides a template TOR for SOCs. Each operational area can customize this template to address specific limitations and requirements.

B. Definition and objective of a SOC

A SOC is a shared resource, which is established on the basis of a need identified through the Security Risk Management (SRM) process.

The purpose of a SOC is to monitor, facilitate and coordinate the data and voice communications and applications using the SCS, within one or more operational areas they are covering, in order to support the safety and security of United Nations Security Management System (UNSMS) personnel[1], premises, assets and operations.

Where SOCs are established[2], UNSMS personnel must always be able to contact the SOC and be contactable by the SOC, independent of their location within the operational area covered by the SOC. Where the SOC does not operate on a 24/7 basis, an alternative must be available either though a remote SOC or a security professional must be contactable (as outlined in Annex D).

Within the "Saving Lives Together" framework[3], in line with the *Security Policy Manual* and local Memoranda of Understanding (MoUs), the SOC may also support security communications for personnel of NGOs and UN implementing partners. For those locations with limited UN presence, which are covered by smaller SOCs but have a large presence of NGOs or UN implementing partners, the cost for personnel and equipment for this SOC may need to be addressed in a local MOU including a Standard Operating Procedure (SOP) to clarify the services, modalities and to manage the expectations.

C. Typical duties and responsibilities for a SOC

Within the assigned operational area(s) and according to local SOPs, SOCs are typically responsible for the following duties within their operational area:

[1] See *UNSMS Security Policy Manual*, Chapter III: "Applicability of the UNSMS".
[2] If no SOC, or no 24/7 SOC, is established within an operational area, it is the responsibility of the most senior security professional to ensure there is a 24/7 emergency contact number for UNSMS personnel (and where appropriate, for eligible dependents of UNSMS personnel, NGO and implementing partners' personnel). See also annex D.
[3] "Saving Lives Together" is the framework of security cooperation between the UNSMS and NGOs, both national and international. See *UNSMS Security Policy Manual*, Chapter II, Section F: Saving Lives Together.

- Support the UNSMS on the daily operations of the SCS;
- Receive, transmit or relay security and safety messages and information on behalf of the Designated Official/Senior security personnel via all identified means of communications;
- On receipt of notifications of security incidents or observations of security incidents through public media, escalate these through the appropriate and defined channels for follow-up and support;
- Notify the most senior security professional[4] of any security incident and the respective UNSMS organization or NGO security focal points when their personnel are involved in a security incident;
- Based on the local SOPs, contact external security services, to support UNSMS and NGO personnel who are involved in security incidents;
- Maintain records and logs of communications and actions taken to support security incident management;
- Maintain accurate and up-to-date contact and residence details of all UNSMS personnel, including wardens (and, if applicable, contact details of NGO and implementing partners), and contact details of premises and vehicles;
- Always maintain the necessary confidentiality of individuals, and in accordance with host government data protection regulations and recommendations provided by the most senior security professional;
- When determined by the Designated Official /Area Security Coordinator /Senior Security Professional (as applicable), through the appropriate SCS, support and facilitate headcounts of all UNSMS personnel, collated in a timely and accurate manner in accordance with instructions or an established SOP;
- Maintain the contact details of the respective emergency services, support structures of host government and local authorities, private security services/contractors, and UNSMS/NGO response teams; be in a position to direct personnel to the nearest support structure during times of security incidents;
- Using the SCS, monitor the movement of missions, as per SOPs in the operational area;
- Verify the operational status of the SCS, via "communications checks", to ensure that personnel can use or access the SCS and that the SCS is functioning properly;
- Perform other duties as directed by the most senior security professional.

D. Organization, reporting lines and budgeting of a SOC

In the SRM process that determines the need for a SOC, two important factors must be considered for the operation of the SOC in the operational area:

a. Hours of operation;
b. Location: SOCs can be physically located within the operational area or can operate and support remotely from another operational area.

[4] This is usually the UNDSS Principal or Chief Security Adviser (P/CSA) or a Security Adviser (SA), including their officer-in-charge ad interim. Where a P/C/SA is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services, Country Security Focal Point (CSFP) or Local Security Assistant, if necessary, in designated areas where no international professional security adviser has been assigned or is present.

A SOC is staffed by SOC Assistants, functionally reporting to the most senior security professional in their operational area. In so far as is possible, a SOC, including its personnel, are administratively managed directly by UNDSS. In the case UNDSS does not have that capacity or capability, SOCs and SOC Assistants can be administratively managed through one of the UNSMS organizations present in the operational area.

The funding of a SOC should be covered through the Locally Cost-Shared Security Budget[5] .

E. Additional provisions on training and tools

SCS technologies evolve rapidly, including the current development and deployment of more advanced SCS applications or security information management platforms. The UNSMS recognizes the continuous emergence of new socio-technical pathways in terms of information/data management and the ongoing evaluation of applicable systems.

Therefore, SOC Assistants must receive the necessary operational guidance and the required training provided by the appropriate technical experts. This will ensure that SOC Assistants adequately master the technical skills required to operate the evolving SCS connectivity and application tools selected by the UNSMS in the operational area, so they can carry out all the duties and responsibilities correctly and appropriately. This must also include SOPs and training components related to supporting gender-based security incidents, the initial actions and response to these, and handling of sensitive information cognizant of confidentiality requirements.

[5] See *UNSMS Security Policy Manual*, "Chapter VI – Section B: Locally Cost-Shared Security Budget.

Annex C: Template TOR for Security Operations Centre Assistants

A. Introduction

A Security Operations Centre (SOC) is a cost-shared resource, established to support the safety and security of personnel, premises, assets and operations working for various organizations covered by the United Nations Security Management System (UNSMS). The SOC monitors, facilitates and coordinates the communications of data and voice messages using the security communications system (SCS), within one or more operational areas. Additionally, responsibilities can include maintaining administrative data supporting security communications, such as aggregating contact data for UNSMS personnel, offices, vehicles and emergency services.

This position will be supporting key functions and operations of the United Nations. The role of a SOC Assistant can be challenging and unpredictable as they may be required to respond and assist callers in need of immediate assistance. They will have the responsibility to pass key information and instructions in a timely and calm manner to UNSMS personnel and others, as required. At times, the work will be fast paced and intense, but highly rewarding as the Assistants will be part of a response and support team which contributes to the work of the United Nations. The selected candidate will gain valuable experience and skills while working with people from a broad range of cultures and professional backgrounds.

Under the overall supervision of the most senior security professional[6] in the operational area, the SOC Assistant is responsible for supporting the UNSMS with the daily operations of the SCS.

This annex provides a template Terms of Reference for SOC Assistants. Each operational area can customize this template to address specific limitations and requirements.

B. Typical duties and responsibilities for a SOC Assistant

Operational:

- Receives, transmits or relays security and safety messages and information on behalf of the Designated Official/Area Security Coordinator/Senior Security Personnel (as applicable) via all identified means of communication to personnel;
- On receipt of notifications of security and safety incidents, escalates these via the appropriate and defined channels for follow-up and support;
- Using the SCS, monitors the movement of field missions, as defined by the Security Risk Management (SRM) process and appropriate local standard operating procedures (SOPs);

[6] This is usually the UNDSS Principal or Chief Security Adviser (P/CSA) or a Security Adviser (SA), including their officer-in-charge ad interim. Where a P/C/SA is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services, Country Security Focal Point or Local Security Assistant (if necessary) in countries or Security Risk Management Areas where no international professional security adviser has been assigned or is present.

- Based on the local SOPs facilitates the provision of immediate support to the UNSMS and NGO personnel involved in security or safety incidents: alerts the response and support functions through the appropriate and defined channels, gives the necessary feedback and input to the personnel involved in the incidents, maintains the communication link to personnel, acts in an overall supportive role. Records all information and communications related to these incidents;
- Notifies the respective UNSMS organization or NGOs security focal points when their personnel are involved in a security or safety incident;
- Monitors the usage of the SCS and ensures it is used according to established SOPs; guide personnel on appropriate behaviour when using the SCS;
- Verifies the operational status of the SCS to ensure that personnel can use or access the SCS and that the SCS is functioning properly. Reports any anomalies to the appropriate authority for further action or guidance;
- Undertakes personnel headcount in accordance with instructions from the Designated Official /Area Security Coordinator /Senior Security Professional (as applicable), or an established SOP in a timely and accurate manner.

Administrative:

- Maintains the contact and residence details of all UNSMS personnel and their eligible dependents (and if applicable contact details of NGOs and implementing partners), and the contact details of premises and vehicles;
- Maintains the UN warden lists;
- Maintains the contact details of the response team emergency services and support structures of host government, local authorities and contracted private security companies; direct personnel to the nearest one during times of security or safety incidents;
- Maintains records and logs of actions and communications undertaken to support security or safety incidents or any other critical communications;
- Prepares and submits reports, as directed by the most senior security professional.

Other:

- Perform other duties, as directed by the most senior security professional.

C. Competencies

- Commits to the ideals of the United Nations Charter and the Organization's core values and possesses the UN core competencies;
- Displays cultural, gender, religion, race, nationality and age sensitivity and adaptability;
- Knowledge management and learning:
    - Shares knowledge and experience;
    - Provides helpful feedback and advice to others in the office;
- Operational effectiveness:

  - Demonstrates excellent knowledge of security and incident protocols;
  - Shows operational resilience;

- Self-management:
  - Focuses on results for the client;
  - Consistently approaches work with energy and a positive, constructive attitude;
  - Remains patient, in control, calm, resilient, emphatic and good humoured, even when under high pressure or managing complex incidents;
  - Responds positively to critical feedback and differing points of views;

- Teamwork
  - Proven interpersonal skills and the ability to work and cooperate in a multi-cultural, multi-ethnic environment with sensitivity and respect for diversity;

- Communication
  - Proven and sustained communication (verbal and written) skills in the official UN language(s) and the local language(s) used at the duty station;
  - Proven listening skills, including ability to understand different accents.

D. Required skills and experience

Education:
- Completion of secondary school. Relevant training and experience can be considered as an alternate to a degree.

Experience:
- Work experience related to operational communications and direct interaction with a broad range of clients;
- Prior working experience within the UN system, an international NGO, or another international organization is desirable.

Language requirements:
- Excellent command (written and spoken) of the working UN language(s) used for official communications in the operational area is essential;
- Knowledge of local language(s) used in the operational area is essential;
- Working knowledge of English is desirable.

Other skills and requirements:
- Computer skills and information management/processing experience;
- Good understanding of computer-based tools such as MS Office Suite and other computer-based, web and smartphone applications;
- Experience with radio, satellite and web-based communications is an asset.

Annex D – Guidance for operational areas without the physical presence of a Security Operations Centre

A. Background

1. It is recognized that providing a dedicated common Security Operations Centre (SOC) service in each operational area presents challenges where there is insufficient local capacity or representation of United Nations Security Management System (UNSMS) organizations. Actual scenarios include smaller operational areas (OA)[7] within a larger country operation or designated area, or smaller country operations.
2. These scenarios require the UNSMS to seek alternatives to cater for the typical duties and responsibilities of a SOC outlined in Annex B, without the need to establish a local or physical SOC presence/service.

B. Overall approach

3. The overall approach is to provide a baseline for SOC services, as defined in Annex B, for those OAs where a dedicated local SOC is not deemed cost effective or required.
4. The Security Risk Management (SRM) process will identify what SOC or remote SOC (RSOC) capabilities are needed, including those OAs where there is no capacity or sufficient UNSMS presence to justify a dedicated local common UNSMS SOC.
5. In the cases where a local common UNSMS SOC is not required or deemed cost effective, SOC services will have to be provided using alternate means. The simplest approach would be to upgrade an existing "radio room" of a UN agency, fund or programme (AFP) to a minimum agreed SOC standard (noted in Annex B), in which case this AFP SOC would take on the roles and responsibilities of a UNSMS SOC[8] scaled to the local OA requirements. Alternatively, an approach could be used where a designated regional or RSOC could be used as the OA's SOC providing remote communications and coordination within the local OA for both routine and emergency situations. As a last resort, an individual(s), for example security professionals (Local Security Assistants or agency Security Focal Points), can provide a minimal baseline local SOC service on behalf of the UNSMS.
6. The actual requirements, services and cost effectiveness to establish a local SOC, RSOC or to use the services of an individual security professional will be identified through the SRM process. Whatever the modality, the SOC-equivalent services must support all services as defined in the SOC TOR outlined in Annex B.

C. Recommendations

7. The structures available for provision of SOC services in OAs without a dedicated local common UNSMS SOC include:

[7] An operational area in this context can be defined as the Designated Area, Security Area or Security Risk Management Area.
[8] The UNSMS SOC is generally run by UNDSS, whereas the AFP SOC is run by a United Nations agency, fund or programme.

a. **AFP SOCs**: A single AFP to voluntarily take on the responsibility for establishing and maintaining its SOC, providing the services equal to those defined for common SOCs, as defined in Annex B, or;

b. **RSOCs**: Establish a remote SOC (RSOC) service to cover the OA, or;

c. **Individual services**: An individual (or individuals), for example security professionals (Local Security Assistant or UNSMS organization Security Focal Points), who provide(s) a minimal baseline local service on behalf of the UNSMS.

AFP SOC

8. Where no formal SOC or RSOC is established, and where an AFP has sufficient local capacity, this AFP may agree to take on the responsibility to provide common UNSMS services throughout the OA, as per the TORs for common SOC defined in Annex B.
9. When using an existing AFP SOC resource as the common UNSMS SOC, the AFP must have both the capacity and capabilities to provide the standard SOC services as defined in Annex B.
10. While the AFP SOC will administratively report to the AFP, the SOC will functionally report to the most senior security professional[9] in the operational area.
11. Any additional costs involved in the upgrade and maintenance of the expanded AFP SOC, as a common UNSMS SOC, will be covered by the Locally Cost-Shared Security Budget.
12. Based on the local security conditions, as for any common UNSMS SOC, the AFP SOC should be able to expand staffing and services in case of emergencies. Costs for this expansion should also be catered for by the Locally Cost-Shared Security Budget.
13. Due diligence should be taken to ensure that, as much as possible, SOC Assistants' grades and contractual status are aligned for all AFP and UNSMS SOCs.

RSOCs

14. Where there is no local UNSMS or AFP SOC capacity, the SMT should consider using an RSOC service. This allows for the majority of the local SOC services to be provided through a RSOC, e.g. centralized in the capital city or in regional hub. In this case, the RSOC would take on the responsibility for local SOC services in the OA.

Individual(s) providing SOC services

15. Should it not be feasible to establish a local UNSMS SOC, AFP SOC nor a RSOC – which may be typical for smaller OAs - the most basic routine services can also be

[9] This is usually the UNDSS Principal or Chief Security Adviser (P/CSA) or a Security Adviser (SA), including their officer-in-charge ad interim. Where a P/C/SA is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services, Country Security Focal Point (CSFP) or Local Security Assistant (if necessary) in countries or Security Management Areas where no international professional security adviser has been assigned or is present.

provided by an individual or small group, for example an AFP Country Security Focal Point and/or UNDSS security personnel.

16. Similarly, while under routine conditions, SOC services can be provided by a local UNSMS SOC, AFP SOC or RSOC for agreed coverage times but during e.g. silent hours on nights and weekends, these services can be provided by local security personnel/Duty Officer as agreed through the SRM process. It should be considered that in an emergency, these SOC or RSOC services may need to be augmented with additional capacity.

Annex E – Guidelines for the technical evaluation of a mobile telephone network's suitability as a security communications systems tool

A. Introduction

1. The United Nations Security Management System (UNSMS) is shifting part of its security communications system (SCS) onto third party infrastructures, especially mobile telephone services. To evaluate the technical capabilities and the capacity of mobile telephone services provided by mobile network operators (MNOs) in an operational area, and their suitability as an SCS for the UNSMS, a uniform and robust process must be applied.
2. This document provides guidelines to the local ICT Working Group (ICTWG) on how to undertake such a technical evaluation and, thereafter, categorize and establish the technical suitability of these services. This chapter outlines the key questions and considerations, which can be collected locally, as initial input for the evaluation of the local mobile networks' suitability as an SCS tool. The TESS team will then assist the ICTWG and UNSMS either remotely or locally, in selecting the most technically suitable mobile network operators to support the appropriate SCS scenario (see below) for each operational area.
3. These guidelines only cover the technical evaluation on the use of a mobile telephone network as an SCS tool.
4. After the technical evaluation is completed, considered and endorsed by the Designated Official (DO)/Security Management Team (SMT), it is recommended a formal procurement process is followed, taking into account the selection qualifiers as specified in the *Security Management Operations Manual* ("Guidelines on Security Communications Systems" Section 23), to select the MNO(s) to be used as common SCS service provider(s).
5. These guidelines only apply to the common UNSMS SCS and do not restrict UNSMS organizations from using different standards for their internal communications needs, as long as these do not compromise the SCS.

B. Background

6. Currently, the majority of UNSMS operations already rely on mobile phone services provided in the operational areas, by one or more MNO for operational communications and often, formally or informally, for security communications.
7. Standards for the use of mobile phone services as an SCS are described in the *UNSMS Security Management Operations Manual* ("Guidelines on Security Communications Systems"), categorizing service levels and the MNOs' suitability as an SCS into three scenarios. These standard scenarios describe the overall suitability of mobile services in a country or operational area, and how those services fit into the SCS:

    - **Scenario A:** Full availability of public mobile phone networks for security telecommunications.

- **Scenario B:** Public mobile phone networks are available, but prone to downtime.
- **Scenario C:** Reliable public mobile phone networks are unavailable in the operational area.

8. The MNOs' service quality in any country is dynamic and changes over time. It is, therefore, important to regularly assess the updated status in the country and individual operational areas. An assessment of the MNO status may also be required on demand if, for example, considerable changes take place in an operational area, such as the establishment of a new UNSMS operation, changes in the security situation, or a new MNO providing services.

C. Responsibilities

9. **ICTWG:** Coordinate the activities required to conduct the initial assessment on the suitability of MNO services as an SCS, as input to the TESS team's final recommendations.
10. **TESS team:** Support the ICTWG and UNSMS locally or remotely with guidance, tools, analysis and recommendations to conduct the evaluation process in a structured and uniform manner. TESS will assist in providing the UNSMS with the final technical recommendations.
11. **The most senior security official:** In conjunction with the security cell**,** proposes SRM Measures to the DO/SMT based on the technical guidance from the ICTWG and TESS Team.
12. **The Designated Official:** Endorses the technical recommendations and tasks the Operations Management Team to follow the formal procurement procedures to select the appropriate MNO(s) for each operational area.

CI. Process

13. The process described below adopts a pragmatic approach for an objective technical categorization of the MNO(s) services under evaluation. The process features three steps: information gathering, analysis and conclusions/recommendations.

CII. Information gathering

14. The evaluation process draws information from four groups of sources:
    a. MNO representatives;
    b. Current users of the services within the UNSMS;
    c. Publicly available information;
    d. Non-public information.
15. In general, there will be some overlap with regard to the questions asked to the four groups so that information given can be compared and corroborated. For example, if information from four different sources generally matches, there is a higher likelihood this represents the actual situation than if one or more had differing information. The sections below describe some of the key areas of information that must be sought from each of the groups.

E.1. MNO representatives

16. It is recommended to include representatives from both the technical side and the business side of the UNSMS organizations. The MNO representatives interviewed must be at sufficiently senior positions to be able to provide the information needed.
17. Coverage and availability
    a. Are the operational areas covered by mobile services? Define services as two groups: voice/SMS (2G minimum) and data (3G/4G/5G).
    b. What is their average uptime? What is their (spare) capacity to catch traffic peak?
    c. Which data services are provided (2G/3G/4G) in different areas: major cities, towns and villages, along major and minor roads including outlying operational areas, for example, those close to borders?
    d. Technical support capability (which will have an operational impact):
        i. Where are the MNOs' technical support staff based - in the capital or in each operational area?
        ii. Is support provided by in-house personnel or is this outsourced to subcontractor(s)?
    e. Do their services face regular, planned outages, for example, due to the security situation, electric power supply or other reasons?
    f. Are any services and applications blocked by default (e.g. WhatsApp, other social media)?
    g. Average number of users per site/cell?
18. Redundancy
    a. What is the risk that mobile networks become unavailable, in case of conflict / natural disaster, when they are needed the most? How resilient are these networks (internally in-country and its international gateway) and the individual network nodes? Does the operator have business continuity/recovery plans? What equipment does it have on standby (e.g. "Cells on Wheels") and intervention procedures (SOPs)?
    b. What is the configuration of the backbone (microwave, fibre) and what is the redundancy built in (e.g. two separate physical links, ring configuration, etc.)? Is the backbone owned by the MNO, a third-party commercial provider, or the government? What is the general quality of the backbone?
    c. Configuration of the international gateway and redundancy:
        i. Are there multiple, physically separated links? Which technology is used (fibre, microwave, VSAT, etc.)?
        ii. Are the links routed through different countries or different providers? Who owns the links?
    d. Does the MNO own or lease the Base Transceiver Station (BTS) sites? Are they shared with other MNOs or other private or public services? Is the power supply to the sites redundant? How long can they run without primary power supply? What physical security measures are implemented at the site?

e. What is the primary and backup power supply for backbone core elements (reliance on public grid)? How long can the backbone operate without the primary power source power? What are the typical physical security measures of the backbone installations?

19. Structure and governance

a. What is the ownership structure of the company (local or multinational or combination)? Does the government, or entities closely related to the government, have any controlling or management role of the MNO?

b. Does the government, regulator or armed forces have the authority and/or a mechanism to switch off all or part of the mobile services? How often has this happened in the past years? Under which circumstances? Can/will these circumstances re-occur?

c. Does the MNO have formal key performance indicators with the government or regulator, for example related to uptime and disaster recovery?

d. Is there an independent regulator (See also the ITU Regulatory Tracker)? How mature is the regulator and market?

e. Is the mobile network used for critical public and financial services, e.g. police, armed forces, emergency services, mobile banking, mobile money? Does the MNO offer "privileged access" to the network?

20. Miscellaneous

a. Is telephone number portability available in the country (i.e. a user can take their mobile number when shifting to another provider)?

b. Is international roaming allowed / generally available? Is internal (national) roaming allowed/activated?

c. What is the strategy and plans for improvements and expansion?

d. Is the MNO using technology that is compatible with widely used hardware, i.e. based on the global mobile phone standards (GSM, UMTS, LTE)? If not, what technology is used?

e. Who provides the backbone equipment (BTS and switching) for the MNO? Is the provider(s) and the quality of the equipment from a large international company (e.g. Ericsson, Huawei, Nokia)?

f. Is the MNO receptive to making a competitive UN fleet contract (as per SMOM guidelines)?

E.2 Users of the services within the UNSMS

21. It is recommended to interview personnel in key roles who rely on the mobile telephone services and have extensive experience using them in the different operational areas: security professionals, technical personnel, senior staff and field personnel. The information provided by these personnel may corroborate with the statements provided by the MNO(s). The assessment team's own experience with the MNO services could be included.

22. Coverage and availability:

a. Perceived mobile network coverage and problem areas;

b. Perceived availability/reliability;

c. Voice and data (speed) services quality;

d. Are there instances when services are shut down or not available? If so, how often and how long?

23. Redundancy

a. Any issues faced with the services: network or partial service (e.g. not working, slow data rate, difficulties making calls)?

24. Customer support quality

a. How do the users perceive the customer support service quality? How easily accessible are these services?

25. Miscellaneous

a. Which means of SCS and operational communications are most often used, i.e. the *de facto* primary means of communications?

b. How are users using the mobile telephone services? Do they have private/official mobile phone, SIM cards and credit? One SIM card or multiple (for the latter, using multi-SIM phones or multiple phones)?

E.3 Publicly available information

26. There is a wealth of information on MNOs and their services available on the Internet. The MNOs' own websites provide useful information, though these may not be fully up-to-date or objective. There are also independent and open source entities that collect such information as coverage, availability, and service level for mobile networks globally. These would be valuable sources of neutral and objective information. One such source is ITU, primarily its ICT Tracker and global coverage map. In addition, public news services and technology media (magazines) are other sources that can provide information about the mobile services market in the country.

27. Coverage and availability:

a. Stated and actual coverage and capacity (2G/3G/4G/LTE);

b. Availability of services.

28. Redundancy: local backbone and international connectivity.

29. Technology upgrades and changes planned and implemented.

30. Structure and governance

a. Is the mobile phone service market controlled by an independent (to the government) regulator?

b. Recent and/or upcoming changes in regulations related to the mobile market.

31. Miscellaneous

a. Status of the MNO business itself, i.e. is it strong financially?
b. Security situation in the country and individual operational areas, as covered in the SRM.

E.4 Non-public sources

32. TESS has access, through agreements with several private entities, to relevant information that is not publicly available, for example Facebook, GSMA and Ookla. This includes measured service quality levels (e.g. data speed and quality), coverage maps, and usage patterns.

F. Analysis

33. Analysing the gathered information to reach a conclusion is far from an exact science but requires a fair amount of experience and judgement. Nevertheless, based on statistics and TESS' own experience in 60+ countries, the vast majority of countries belong under Scenario B (Failover). With the experience TESS has gained, it is uniquely positioned to support the local team with the analysis through guidance and advice.

34. It can be useful to start with the information provided by the mobile operators themselves and compare this with other sources. It is especially useful to compare statements on service level, availability and coverage made by the operators against the more practical perspective from the various types of users.

35. To further structure the evaluation, the criteria used to evaluate the MNO service has been split into "critical" and "supporting" factors. Any of the critical factors on its own has the potential to decide whether a service is categorized as B or C.

F.1 Critical factors

Redundancy in the network infrastructure

36. This factor looks at the redundancy that a market or provider has built into its infrastructure, i.e. how robust is it when affected by external events. A Scenario B service will have redundancy built-in for the internal backbone, and a link to an international network and for their sites, both for power and security. For example, its internal (in-country) network infrastructure consists of two separate and independent communications links (two sets of microwave links, a fibre link and microwave, or two separate fibre links). In general, these links would be configured as a ring for further redundancy. If there is no built-in redundancy, the conclusion is to rate it as Scenario C.

37. The same requirement applies to a link the provider has to the international network (Internet). A provider within Scenario B would have two or more, full capacity, physically separated international gateways, linked to the international network. Typically, these links would also be routed through different countries and/or connect to different international backbones. Scenario C services would typically have only one full capacity link and possibly a low capacity backup (VSAT) or no backup.

38. The telecommunications sites hosting the equipment and the supporting services provided there (security and power) has a big impact on the reliability of the service. A Scenario B mobile phone operator typically maintains on-site security and redundant power supply. The power supply can consist of grid power and a backup battery module. Other combinations include a generator and batteries/UPS and, possibly, solar panels. The battery backup would be sufficient to keep the services running until technical support personnel can reach the site. If the sites do not have a backup system (batteries) and only rely on an unstable grid or a generator, this may

indicate that it belongs in Scenario C. However, an isolated site being in Scenario C does not automatically place the entire network/MNO in Scenario C.

Ability and likelihood of the government interfering

39. In Scenario B (Failover), the government is shutting down all or part of the services only during certain events, e.g. elections, security incidents. These incidents occur once a year or less, without regularity, and the duration is generally short (up to several hours), where only some of the services are affected. To be categorized as C, the shutdowns would have to take place regularly throughout the year and/or when even minor events occur. In addition, all services would be shut down (voice, SMS and data) and across large areas or the entire country.

40. If an independent regulator is in place, the likelihood of the government interfering is lower. However, this will also depend on many other factors, like the mandate the regulator has been given. Another indication is assessing the frequency of the shutdowns now, compared to the past.

Coverage area and availability of services

41. For Scenario B countries, coverage is typically available in cities, town and villages, in addition to the main road axis. There may also be coverage along smaller roads but with gaps. In Scenario C, coverage is typically limited to major cities and towns, with minimal coverage outside these population centres. For the UNSMS, the priority must be consistent coverage where offices are located, where operations take place, and the roads between these.

42. For a service to be categorized as B it must, at a minimum, have an average availability of service of 95%. That is equivalent to about one hour of downtime per day. However, the service could have less availability than that intermittently. If there is regular downtime, for example due to the generator being turned off to save fuel during the night, the service would belong in Scenario C.

F.2 Supporting factors

43. Although these supporting factors alone cannot inform whether an MNO service is Scenario B or C, it can provide guidance on situations where services are borderline between the two scenarios.

Customer support

44. For a Scenario B, the MNO should have a dedicated customer support representative. This role must be capable of representing the UN in all the key functions of the MNO, e.g. managing subscriptions, propagating new demands, resolving service issues. In addition to being able to raise issues through a focal point, the MNO must have internal processes capable of resolving the cases.

Level of service provided: 2G/3G/4G

45. Considering that 3G deployments accelerated in the first half of the 2000s, the current lack of 3G, or better, services could indicate an immature mobile phone services market. This is particularly true if this deficiency also exists in larger towns and cities.

Technology used and suppliers

46. If the suppliers of the MNO infrastructure are not an internationally recognized brand, this could affect service reliability. Users will most likely also raise issues regarding low service availability and quality and provide negative feedback on its reliability.

G. Conclusion/recommendation

47. The final technical recommendation on the use of a mobile telephone systems as an SCS tool should be specific for each operational area.

48. After the initial analysis is completed and the services are categorized by the local team, the final recommendations and guidance will be provided by the TESS team, either remotely or through a mission.

Annex F – Guidelines on the role of the ICT Working Group in support of a Security Communications System

A. Introduction

1. These guidelines apply to all countries where the United Nations Security Management System (UNSMS) has established an ICT Working Group (ICTWG), which can be a valuable resource for the system. If no ICTWG is established, this function will be supported by the TESS team.
2. This document provides the guidelines on how the ICTWG can contribute to support the UNSMS through the security communications system (SCS).

B. Governance

3. The ICTWG is a working group established under the Operations Management Team with both telecommunications and IT expertise, supported by the regional technical expertise from the different UNSMS organizations. Depending on the size and complexity of the UNSMS operation, and thus the SCS, it might be more efficient and sustainable to separate the responsibility for IT and telecommunications in two sub-working groups.
4. According to policy, the Designated Official may decide to invite the chair of the ICTWG as a subject matter specialist when discussing matters related to ICT in the Security Management Team (SMT). Moreover, as they are supporting the Security Risk Management (SRM) processes, members of the ICTWG may be asked to attend and contribute to the work of the Security Cell.

C. Roles and Responsibilities

5. **UNDSS senior security professional / Security Cell:** Works closely with the ICTWG to determine the appropriate SCS supporting the UNSMS in an operational area.
6. **ICT Working Group:** The local focal point for technical support and advice on the SCS to UNDSS, the Security Cell and the SMT. They coordinate with the TESS team, as required.
7. **TESS team:** Provides guidance and support to the ICTWG and supports assessments to determine the appropriate SCS, as required, based on global SCS standards**.**
8. Operations Management Team: Tasks ICTWG on behalf of the SMT and, as required, identifies related budgetary requirements and contractual agreements based on the ICTWG's technical guidance.

D. Terms of Reference: Tasks related to supporting the SCS

9. The ICTWG has an advisory role and an operations and support role.
10. *Advisory Role*
    a. Provides technical advice on UNSMS standards and technical solutions.
    b. Supports the UNSMS to identify the appropriate SCS as part of the security risk management measures.

11. *Operations and Support Role*

a. Coordinates the development, implementation, support and management of UNSMS standards for the SCS, including, but not limited to, common radio callsigns and selective calls standard; common frequency list for radio communications; radio configuration setting (codeplugs); and equipment installation standards. Local standards must be aligned with global and relevant UNSMS standards.

b. Liaises and coordinates with local authorities to facilitate licensing, permissions to operate and import of telecom equipment for the UNSMS organizations.

c. Undertakes assessments of MNO and communications services to determine the most suitable provider to support the SCS for the UNSMS.

d. Coordinates the establishment and implementation of an annual SCS technical maintenance plan, including the preparation and submission of the annual maintenance budget, supervision of the actual support work, and the monitoring of the expenditures.

Annex G – Standard Operating Procedures for Movement Monitoring

A. Introduction

1. Movement monitoring procedures are essential to keep track of United Nations Security Management System (UNSMS) personnel on mission / when travelling, facilitating quick interventions or preventative measures in case of security or safety incidents.
2. The movement monitoring procedures allow Security Operations Centres (SOCs) or the most senior UNDSS security professional[10] and UNSMS organization security professional assigned to that area to contact (or be contactable by) all UNSMS personnel at any given time, so that the required assistance can be directed to the correct (or last reported) location immediately.
3. These procedures are applicable for all movements in which UNSMS personnel or UNSMS transport vehicles are involved, whether movement monitoring by the SOC is done manually using the security communications system (SCS) or automatically by means of a vehicle tracking system (VTS).
4. This annex provides a standard procedure (SOP) for the monitoring of common UNSMS movements for all personnel involved in the conduct and monitoring of field operations. Each operational area can develop their own SOP to address specific operational requirements.
5. This SOP applies to common movement monitoring procedures supported by the SOC for the UNSMS and does not prevent individual UNSMS organizations from having additional internal mechanisms for monitoring the movement of their own personnel, as long as these do not conflict or compromise the common movement monitoring.
6. This SOP should be distributed to all stakeholders involved with movement monitoring.

B. Definitions

7. **Mission**: The combination of UNSMS transport vehicles and UNSMS personnel involved in a movement.
8. **Movement**: "Movements", as supported by this SOP, are
   (a) Field missions between the confined areas of large cities, towns, villages or specific smaller operational areas (such as "camps") where UNSMS organizations have established their operational bases or premises;
   (b) As determined by the Security Risk Management (SRM) process, missions within these confined areas.
9. **Transport vehicle**: Type of transportation used in the mission (e.g. motor vehicles, - car, truck, bus, motorcycle, boat, barge, train, aircraft- airplanes, helicopter).

[10] This is usually the UNDSS Principal or Chief Security Adviser (P/CSA) or a Security Adviser (SA), including their officer-in-charge ad interim. Where a P/C/SA is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services, Country Security Focal Point or Local Security Assistant, if necessary, in designated areas where no international professional security adviser has been assigned or is present.

10. **Manual movement monitoring:** The mission reports its location regularly by contacting the SOCs via the SCS.
11. **Automated movement monitoring:** The mission reports its location automatically, at predefined intervals, to a centralize monitoring tool in the SOC via a VTS device. This device can be installed in the transport vehicles (hard wired or as a portable device) or carried by a member of the mission (portable devices).
12. **Primary Monitoring SOC**: The SOC responsible for monitoring the mission. This is usually the UN common SOC at the departure location, but this could also be another SOC designated to monitor the mission.
13. **Secondary Monitoring SOC:** If the mission is travelling to a destination where another UN common SOC is operational, that SOC is designated as the "Secondary Monitoring SOC". In this scenario, this SOC is to be on standby to assume the monitoring responsibilities if requested by the Primary Monitoring SOC or if the Primary Monitoring SOC is not reachable by the mission.
14. **Mission Monitoring Sheet:** A movement monitoring log that contains all the information about the mission and all communications with the mission. This can be an electronic database, spreadsheet or, as a last resort, on a hardcopy sheet. An example of a Mission Monitoring Sheet is attached as Appendix 1 to this annex. A dedicated Mission Monitoring Sheet is created for each individual mission and contains at least the following information:

Basic mission information

a. A mission identifier (e.g. key mission name, or description);
b. Planned date and time of departure and arrival;
c. Departure and destination point, and, if applicable, planned stops;
d. Name for each UNSMS organization's mission member (and the name of their organization), and other passengers in the UNSMS organizations' vehicles[11];
e. Name of the Mission Team Leader and the Mission Communications Lead;
f. Mode of movement reporting: manual or automated (using VTS);
g. Transport vehicle type and identifiers (license plate or other unique identifier) and the organization for each transport vehicle used in the mission;
h. Details of the communications installed in each transport vehicle in the mission, including (as applicable) HF/VHF radio callsign and selcall, satphone number. In case automated VTS is used, the unique identification number of the VTS device for each transport vehicle or carried by UNSMS personnel;
i. Contact information of all individual UNSMS mission members (including driver(s)) if they have personal communications equipment (such as VHF radio

[11] NGO Implementing and Operational Partners of the United Nations and its Agencies, Funds and Programmes; Government counterparts, or any Third-Party Contractors vehicles participating in a UNSMS movement will be included in the movement monitoring by the Organizations' name; vehicle registration; and number of passengers onboard. Should NGO Implementing and Operational Partner staff, Government counterparts, or Third-Party Contractors be traveling inside a UNSMS vehicle, the participants full name and organization should be recorded in the movement monitoring form and the required Waiver of Liability Form should be signed by the individual third party prior to departure.

callsigns, mobile telephone numbers, individual satphone numbers or mobile phone messaging contact details);

j. For non-UNSMS organizations' vehicles travelling in a convoy with UNSMS vehicles, only the vehicle identifier, the number of passengers and their organization's name is required;

k. For manual monitoring: reporting schedule, i.e. frequency (e.g. every 30 or 60 minutes) or agreed waypoints;

l. When required, confirmed mission order and any reference for security clearances required by the local authorities.

Mission movement data

a. Confirmed time of departure;

b. Details of each communication (confirmed contact or attempted call) with the mission, including time and basic content of the call;

c. If manual movement monitoring is used, time and position of the mission as reported

d. Time and location for any stops during the mission, taking into account known communication blackspots or areas of security concerns;

e. Details of any incidents or accidents including actions taken;

f. Confirmed time and location of arrival.

15. **Mission Team Leader:** A mission member in charge of the mission. The Mission Team Leader should be a UNSMS personnel.

16. **Mission Communications Lead:** The mission member responsible for operating the communications systems and reporting to the SOC during the mission.

C. Roles and Responsibilities

SOC Assistants

17. Monitor regularly (at least daily) the TRIP page on UNSMIN and all information provided by mission leaders on upcoming missions.

18. Verify that all information required for movement monitoring (see above for "basic mission information") is obtained and is registered in the Mission Monitoring Sheet.

19. Prior to and during the mission, the SOC will notify the Mission Team Leader of the latest security information or incidents on the planned route, e.g. specify locations where incidents have recently occurred and which the mission should avoid.

20. In conjunction with the TRIP clearance, give the final "go-ahead" for missions to depart and report missions departing without the official "go-ahead" to the most senior security professional.

21. Follow up with the missions' position and arrival reporting. If position reporting (in the case of manual movement reporting) or reporting on arrival was not done on time, escalate as necessary.

22. Record all communications (or "calls"), whether successful or not, position reports (in the case of manual movement reporting), and key messages related to the missions in the Mission Monitoring Sheet.
23. Close and archive the Mission Monitoring Sheet when a mission has confirmed its arrival at the pre-determined destination.
24. Facilitate initial support and information to the mission in case of need (e.g. contact police or medical support) as per local SOP.
25. If a Secondary Monitoring SOC is used for the movement monitoring, verify that the Secondary Monitoring SOC has all data related to the mission movement prior to the operational handover and, at any given time, can take over the mission monitoring. This also applies in reverse where the Secondary Monitoring SOC is handing the movement monitoring back to the Primary Monitoring SOC.
26. Immediately report any incidents or accidents to the most senior security professional.
27. Prepare a daily movement summary report (including reports of non-compliance). An example of a field movement summary report is provided further below.

Mission Team Leader

28. Provide all basic mission information (see above) to the Primary Monitoring SOC prior to the mission's departure.
29. Appoint one member of the mission as the Mission Communications Lead and one as an alternate. The role of the Mission Communications Lead should not be assigned to the Mission Team Leader or to the driver.

Mission Communications Lead

30. Verify that all required means of SCS communications, as per the SRM, are available for the mission and are tested before departure.
31. For manual movement reports, provide the SOC with regular movement reports and incidents as per instructions from the Mission Team Leader.
32. Follow the Mission Team Leader's instructions and assume all communication tasks agreed with the Mission Team Leader.
33. Be familiar with the use of any means of SCS communications available, understand how to contact the Primary (and if applicable, also the Secondary) Monitoring SOC.

D. Means of communications

34. Movement monitoring will be done by means of the SCS established in the operational area(s) where the mission is taking place. This typically requires the mission to have, at a minimum, two means of communications available to the Mission Team Leader (and the Mission Communications Lead). If the mission is moving across multiple operational areas, it is paramount that the Mission Communications Lead verifies the means of communications for these operational areas.

E. Prior to departure

35. At the start of the day, the SOC checks which missions were approved (received security clearance through TRIP) and prepare to monitor their movements. At the end of each shift, the SOC Assistants perform a proper handover of the missions' list and status of all active missions, to the next shift.

36. It is the responsibility of the Mission Team Leader to provide the basic mission information and mission movement data to the Primary Monitoring SOC prior to the mission's departure and, preferably, in writing:

37. The Mission Team Leader is responsible to make sure all means of communications required for the mission are tested and operational:

    a. For voice communications (e.g. radio, mobile phone or satphone), a test call has to be made to the SOC;

    b. For automated mission monitoring, it has to be verified if the VTS location for the vehicle is properly visible and updated on the monitoring screen in the SOC.

    c. If any of the communications systems are not operational, the Team Leader must rectify the issue, or an alternative means of communications must be obtained and reported to the SOC.

38. The mission commences when the SOC gives the clearance to depart.

F. During mission movement

39. The Mission Communications Lead is responsible to ensure field movement information is communicated to the monitoring SOC, whether manual or automated.

40. For manual monitoring only: The field movement information needs to have, as a minimum, the following information: identification of the mission, location references (a GPS location or a pre-defined waypoint), and the status of the mission.

41. Report planned and non-planned stops and incidents to the monitoring SOC as soon as possible. The actual transmission of the field movement information is made by the Mission Communications Lead, or alternate.

G. Arrival at final destination

42. Whether manual and automated movement monitoring is used, on safe arrival at the final destination, an "arrival call" is made to the Primary Monitoring SOC, alternatively to the Secondary Monitoring SOC if the Primary SOC is not reachable. In the latter case, the Secondary Monitoring SOC will be responsible for informing the Primary SOC of the arrival of the mission.

H. Incident handling

Non-reporting

43. For manual movement monitoring: If the mission has not reported according to the schedule noted on the Mission Monitoring Sheet, the SOC provides a time buffer (typically 30 minutes, or as per local SOP) to cater for the delay. The delay can be due to the mission being in a situation where they cannot communicate or are occupied with other tasks. For automated monitoring: The absence of an updated location can be due to unavailability of the GPS signal or connectivity.

44. After this time buffer has expired, the SOC will actively try to contact the mission or the mission members via all necessary means of communications.

45. If, after a specific period (typically one hour after non-reporting, as defined by the SRM), all attempts to reach the mission have failed, the SOC must escalate this to the UNDSS security professional on duty.

Reporting and recording incidents

46. If the mission is involved in any minor incidents or any delay in their mission (e.g. traffic jam, flat tire, delay at a checkpoint), the mission must inform the SOC of the new expected time of arrival if the delay is more than 30 minutes.

47. In case of serious incidents, involving personnel or transport vehicles from the mission, the mission must immediately report to the SOC the basic information: when, what, where (location), who (is involved) and how (what actions or support are needed). The location can be an easily identifiable geographic location, waypoint or GPS coordinates. In the case of serious incidents, the SOC must immediately inform the UNDSS security professional on duty, who in turn will notify the relevant organizational focal points.

48. The SOC records all incident details pertaining to a mission movement recorded in the Mission Monitoring Sheet.

I. Daily reporting

49. The SOC summarizes the daily mission movement monitoring in a daily summary report, as required. An example of a Daily Mission Monitoring Summary Report is provided in Appendix 2 to this annex.

Annex G – Appendix 1: Example Mission Monitoring Sheet

(Only provided as example for the format and data needed. The actual form can be an Excel spreadsheet or in a database.)

Mission Monitoring Sheet								Date:
Mission identifier:				Mode of transportation:			Transport ID:	
Primary SCS:		Backup SCS:		Monitor mode (VTS/Man):			Monitor interval:	

Contact info (Primary)

	Name	Organisation	TRIP	Mobile Phone nr	Satphone nr	VHF callsign
Mission lead						
Communications Lead						
Alternate comms lead						
Driver						

Mission details

Itinerary	From:	To:		Via:
	Est. Date/Time	Est. Date/Time		Est. Date/Time:
Purpose:				
Remarks:				

Movement monitoring details

	Time	Location	SCS used	Name SOC assist.	Message/Location/Issues/Remarks
Dept. check:					
Departure:					
Contact 1:					
Contact 2:					
Contact 3:					
Contact 4:					
Contact 5:					
Contact 6:					
Contact 7:					
Contact 8:					
Contact 9:					
Contact 10:					
Contact 11:					
Contact 12:					
Contact 13:					
Contact 14:					
Contact 15:					
Contact 16:					
Contact 17:					
Contact 18:					
Contact 19:					
Contact 20:					
Arrival:					

Transport details

Type	Transport ID	SCS installed	Organisation	Official/Rented	Remarks

Contact info (Secondary)

Name	Organisation	Role	VHF callsign	TRIP	Mobile Phone nr	SatPhone nr	Transport ID

The example Excel spreadsheet file, with explanations for each field, and a sample filled sheet can be found on UNSMIN.

Annex G – Appendix 2: Daily Mission Monitoring Summary Report

(Only provided as example for the format and data needed. The actual form can be an Excel spreadsheet or in a database.)

Daily Mission Monitoring Summary Report			**Date:**
Missions overview:			
Total monitored	**Initiated today**	**Closed**	**Open**
Incidents overview:			
Reporting non-compliant	**Comms check non-compliance**	**Road crash**	**Other (Details below)**
Incidents details:			
Mission ID	**Incident type**	**Description**	
Monitoring details:			
SCS Usage		**Monitoring mode**	
Mobile	%	Automatic VTS	%
SatPhone	%	Manual	%
Radio (VHF/UHF/HF)	%		
Messaging (SMS/IM)	%		
Other	%		
Prepared by:		**Date/Time:**	

The actual example Excel spreadsheet, with explanations for each field, and a sample filled sheet can be found on UNSMIN.

Annex H – Standard Operating Procedures for Communications Checks

A. Introduction

1. Within an operational area[12], communications checks are performed to:
   a. Verify the proper functioning and use of a security communications system (SCS);
   b. Verify users have the tools, in working order, required to access the SCS;
   c. Verify users are capable of using the tools and understand the procedures;
   d. Verify the contact list of users of the SCS is up to date.
2. The purpose of a communications check is different from that of a headcount, even though both can be combined into one exercise. A communications check focuses on the technical functioning of a particular SCS, while a headcount is used to establish who is present, and their status, in a particular location.
3. The SCS in a United Nations Security Management System (UNSMS) operational area generally consists of a primary means of communications and at least one backup. A communications check tests one specific SCS (e.g. mobile phone network, radio network, satellite network, electronic messaging).
4. This annex provides a standard operating procedure (SOP) to undertake communications checks. Each operational area can further develop this SOP to address specific operational requirements.
5. This SOP only applies to the common UNSMS SCS and does not restrict UNSMS organizations from using different standards for their internal communications needs, as long as it does not compromise the SCS.
6. These SOPs should be distributed to all stakeholders involved with communications checks.

B. Responsibilities

7. **Designated Official:** Supported by the Security Management Team (SMT) and the most senior security professional; decides whether a communications check is required on a regular or ad hoc basis.
8. **Common UNSMS SOC:** Announce, initiate and manage the communications check, including recording who responds; follow up with those who do not respond; prepare and share reports with the assigned authority (typically the most senior security professional). Ensure the UNSMS personnel list (with contact details) is up to date.
9. **Individual users:** Are responsible for responding to the communication checks using the SCS method to be tested. If users are unable to respond as required, or experience any issues, they will notify the SOC as soon as possible via alternative means (e.g. email).

[12] An operational area in this context can be defined as the Area, Security Area or Security Risk Management Area.

10. **The UNDSS Principal/Chief/Security Adviser:** Review, report and distribute outcome of the communications checks to the Designated Official, SMT (and NGOs if applicable). Ensure any issues reported during the check are followed up and resolved in the SMT.
11. **Representatives of UNSMS organizations at the country level:** Ensure their personnel participate in the communications check.

C. Frequency

12. The frequency of communications checks depends on a number of factors, as determined in the Security Risk Management (SRM) process:
    a. The current or expected security situation. In low risk areas, one communications check per one or two months is sufficient. In very high-risk areas, a communications check can be undertaken on a more regular basis, based on the Area SRM.
    b. The choice and reliability of the SCS connectivity systems. For example, if the primary SCS is the mobile phone system, and the secondary SCS is a VHF network, both can be tested once a month. But if, due to external events, the mobile phone system would become more unreliable, the frequency of the VHF network should be increased.

D. Equipment and networks check

13. Make available up to date UNSMS personnel contact lists (including e.g. VHF call signs if applicable) before the communications check is initiated. Following the communications check, based on the outcome, UNSMS organizations resolve any discrepancies and update the SOC.

14. Depending on the number of personnel in the operational area, communications checks can be done in one go or be spread over several time slots (split up per group of UNSMS organizations). It is recommended that users initiate the call to the SOC, rather than the SOC calling each user one by one.

15. Prior to the actual communications check the SOC sends a reminder to all users, specifying the date, time, means of communications, contact details of the SOC, what is expected from them. This could be done via the UNSMS Organization Security Focal Points.

16. During the actual communications check, each individual user calls the SOC by means of the appropriate communications tool and identifies themselves (name or callsign). The SOC operator records the personnel check in a dedicated spreadsheet or database for reporting purposes.

17. At the end of the agreed time slot, the SOC will attempt to contact, by any means available, those users who have not called in for the communications check.

E. Reporting

18. The SOC records who responded (or did not respond) to the communications check:

a. Attended: User called in during the communications check;

b. Not attended – verified: User did not call in during the communications check, but the SOC was able to contact them, after the check;

c. Not attended – not verified: User did not call in during the communications check, and the SOC was unable to contact them. In this instance, the individual UNSMS organization will be notified by the SOC informing that there has been no contact from the individual concerned.

19. Reports on response rates and reasons for non-compliance are shared with SMT via the most senior security professional for their appropriate follow-up.

F. Notes related to headcount

20. A headcount is a similar process but used to verify the presence of UNSMS personnel in the operational area (or e.g. at home or base after curfew hours). In headcounts, UNSMS personnel can use ANY means of communications that are part of the SCS, including phone calls, instant messaging, and radio.

21. If using text messaging or a social media application like WhatsApp, the SOC must verify reception of user response by transmitting a confirmation message to the user.

22. The locally established SOP will define the process of how personnel unable to be accounted for during the headcount process will be contacted to ensure that the status of all personnel can be established in a reasonable amount of time.

Annex I – Guidance for the maintenance of a radio-based security communications system

A. Introduction

1. In many operations, the United Nations Security Management System (UNSMS) owns and relies on a common radio-based infrastructure (typically VHF/UHF networks) as a part of its primary or backup security communications system (SCS). Regular and preventive maintenance of this infrastructure is paramount in order to keep this vital part of the SCS fully operational.
2. This guidance applies to the maintenance of the SCS radio-based infrastructure itself (such as the VHF/UHF repeaters) as well as the radio equipment installed in the Security Operations Centres (SOCs), used to access the SCS infrastructure. This maintenance support can also be extended to the radio equipment used by the individual UNSMS organizations to access the radio-based SCS system, typically handheld radios and radio equipment installed in cars and offices. The maintenance visits are however not meant to support/maintain the communications equipment used for internal (operational) communications by the individual UNSMS organizations, which remains the responsibility of each UNSMS organization.
3. This guidance only applies to the common UN SCS and does not restrict UNSMS organizations from using different standards for their internal communication needs, as long as they do not compromise the SCS.

A. Roles and Responsibilities

4. **Designated Official (DO):** Supported by the Security Management Team, to formally endorse the maintenance plan and the accompanying Locally Cost-Shared Security Budget (LCSSB) to implement it.
5. **ICT Working Group (ICTWG):** Has the overall responsibility, in coordination with the country UNSMS and the individual UNSMS organizations, for preparing a maintenance plan, its budget and coordinating its implementation and subsequent reporting through a local Standard Operating Procedure (SOP). If the maintenance is provided by a local commercial contractor, the ICTWG still supervises this contracted service at a technical level.
6. **Country UNSMS:** Review the maintenance plan and its associated costs and local SOPs as input for the DO's endorsement.
7. **TESS team:** If required, provides additional guidance and technical advice to the ICTWG on the maintenance of a radio-based SCS.

B. Planning

Scope

8. To maintain a radio-based SCS, at least two preventive maintenance visits must be conducted each year to each operational area where radio-based UNSMS SCS installations are used.
9. The maintenance visits are primarily aimed to support the common UNSMS SCS infrastructure.

10. If decided by the DO, this maintenance support can also be extended to the radio equipment used by the individual UNSMS organizations to access the radio-based SCS system.

Activities

11. **Common UNSMS SCS infrastructure**: Maintenance will be provided to the common UN SCS infrastructure, which includes all installations deployed to support radio-based SCS (such as VHF/UHF repeater sites) and in common UNSMS SOCs, to ensure installations meet SCS standards and that they perform as expected. Basic issues can be resolved during the maintenance missions. Problems which cannot be resolved during a routine maintenance mission will be flagged in the "back-to-office" report and dealt with in a follow-up technical support mission.
12. **Optional: Radio equipment of UNSMS organizations accessing the SCS**: This maintenance includes checking the radio installations in vehicles and offices, as well as staff's equipment (such as handheld radios). Basic issues can be resolved during the maintenance missions while more significant problems will be reported back to the specific UNSMS organization.
13. **Training**: Both end user and SOC Assistants' training/refresher courses and the training of the local technical personnel to maintain SCS radio equipment are important activities that support efficient operations and use of the SCS, and should be included into the SCS maintenance missions.
14. All the above-mentioned activities, and the time/budget required to deliver them, must be taken into account when preparing the maintenance plan and be included in the SCS maintenance budget of the LCSSB.

Budget

15. Most maintenance activities have an associated cost. Funds must be made available for the implementation of the maintenance plan through the LCSSB, independent from who does the actual maintenance: a dedicated technical team, an outsourced contractor or technicians from a UNSMS organization.
16. The yearly LCSSB budget to implement the maintenance plan has two components:
    a. **Staffing resources**: Costs related to the staffing needed for the maintenance and the associated costs including internal travel and DSA, considering the staffing can be made available by the ICTWG, UNDSS, an individual UNSMS organization or a commercial contractor.
    b. **Spare parts, consumables**: This includes cost related to spare parts required to repair faulty equipment and components. These are consumables that regularly need to be replaced, such as protective tape, backup batteries, and connectors. Major upgrades or equipment replacement are typically not included in a maintenance budget.
17. In addition, the one-time cost for the appropriate technical toolkits also has to be budgeted.

C. Implementation

Checklists

18. The TESS team can provide standard checklists templates to ensure consistency in the implementation of the maintenance of the SCS radio-based infrastructure. These can be adapted by the ICTWG to cater for all equipment to be maintained. The checklists should include visual inspection, functional testing and performance checks

Maintenance visits

19. Maintenance visits must be scheduled in advance so that all equipment is accessible for the inspection and maintenance. Routine maintenance work will be undertaken while on-site. If major repairs cannot be done during the scheduled visit, these must be recorded and included in the back-to-office reports and addressed in subsequent maintenance visits.
20. If maintenance support is also provided to radio equipment used by individual UNSMS organizations to access the common SCS, the technical support team will need all information from the UNSMS organizations in each location regarding the nature of support required. This will allow the team to allocate the necessary time to address all the issues.

Local SOP

21. The ICTWG, in close collaboration with the country UNSMS and country UNSMS organizations, documents the actual maintenance plan and reporting procedures, in a local SOP, to be reviewed and approved by the country UNSMS.

D. Reporting

22. It is recommended to keep a maintenance log for each operational area, including the sites visited, i.e. SOCs and repeaters, and maintenance support provided to UNSMS organisations' equipment accessing the common SCS infrastructure.
23. A "back-to-office" report is required after each maintenance visit summarizing the issues observed, key actions performed and open issues still to be resolved. This should also include the maintenance of UNSMS organizations' user equipment used to access the SCS. The "back-to-office" report would include the following information, at minimum:
    a. Date and duration of the mission;
    b. Locations visited;
    c. Participants of the mission;
    d. Planned and executed maintenance tasks;
    e. Any pending issues unresolved during the maintenance visit and what is required to resolve them, including the associated cost.
24. A yearly maintenance report should summarize:
    a. All maintenance missions, actions taken, issues resolved and pending;
    b. An annual expenditure report and a budget proposal for the next year's maintenance budget, including the cost to resolve any pending issues;