UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION B

Security Level System (SLS)

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 08 April 2011

A. Introduction:

1. The Security Level System is a system for assigning a grade or level to areas where the United Nations operates in order to identify the overall level of danger in that area. The Security Level System is a tool for United Nations security professionals to:

   a. More accurately identify and measure the level of security threat that exists in a geographic location,

   b. Produce a Security Level (1-6) for that location, and

   c. Give an overall impression to staff and managers of how the security environment in one area/location compares with another.

B. Purpose:

2. The purpose of this policy is to outline the rationale for the Security Level System and the relevant roles and responsibilities associated with it.

C. Application/Scope:

3. The policy is applicable to all individuals covered by the United Nations Security Management System, as defined in Chapter III of the *Security Policy Manual* ("Applicability of United Nations Security Management System").

D. Conceptual Framework:

4. The Security Level System is an integral part of the Security Risk Management process and is designed to accurately describe the security environment that exists in an area or location ("Security Level Area") in which the United Nations operates.

5. The Security Level System is based on threat and not risk. The Security Level System describes the general, threat-based security environment. Because security measurers must be designed to solve specific security problems, the Security Level System is not used to make specific security decisions. The Security Level System objectively describes the threat environment and uses this objective evaluation to inform the Security Risk Assessment, from which security decisions are made.

6. A Security Level is determined using a Structured Threat Assessment. The Structured Threat Assessment evaluates five categories: Armed Conflict, Terrorism, Crime, Civil Unrest and Hazards. Each category is evaluated using a point system, and the combination of these separate evaluations automatically determines the Security Level. The Security Level indicates the level of danger that exists in the defined area or location on a scale of 1 to 6.

7. To be reliable, a Structured Threat Assessment must have a clearly defined geographical area of analysis. A Security Level Area should define the geographical scope of similar threats and hazards. It is rare for threats and hazards to be the same throughout an entire country, therefore most countries require more than one Security Level Area, although the number of Security Level Areas in a country should be kept to a manageable number.

8. The Structured Threat Assessment is updated anytime there is a significant change in the security environment, either an improvement or a worsening of the situation. The Security Level System provides security decision makers with a very important snapshot of the existing threat-based environment in the defined area or location in which they need to operate. All Structured Threat Assessments are conducted in the same way, so security decision makers receive the added value of being able to compare their locations with other locations in the world.

E. Security Levels

9. The SLS has 6 Levels, from 1 (least dangerous environment) to 6 (most dangerous environment). In addition to numbers, the Security Levels also have accompanying titles and colors as described in Annex A below.

F. Roles and Responsibilities in the Security Level System

10. All Chief Security Advisors, Security Advisors and Chief Security Officers, along with the Security Cell, are responsible for preparing the Structured Threat Assessment, including establishing Security Level Areas, using all applicable threat-related information.

11. The Designated Official approves Security Levels 1 to 5. The Secretary General, through the Under-Secretary-General for Safety and Security, approves Level 6. Upon approval, the Security Level is recorded in the Department of Safety and Security (DSS) database and automatically included in the DSS Travel Advisory.

12. The Security Level System must be a standing agenda item for all Security Management Team meetings, where the Designated Official, in consultation with the Security Management Team, either confirms the Structured Threat Assessment as it stands, or approves any modification to it due to changes in the security environment, as per paragraph 7 above.

13. The Headquarters of the Department of Safety and Security is responsible for validating all Structured Threat Assessments and resulting Security Levels.

G. Training Requirements

14. Requirements for Basic Security in the Field (BSITF) and Advanced Security in the Field (ASITF) are not linked to Security Levels. All United Nations personnel must successfully complete “Basic Security in the Field” (BSITF) training. United Nations personnel being assigned to, or visiting on official travel, any field

location[1], regardless of Security Level, must successfully complete "Advanced Security in the Field" (ASITF) training. BSITF and ASITF certificates are valid for three years, at which point staff members must recertify.

H. Security Clearance

15. Security clearance is required for all official travel to any location regardless of the Security Level[2]. The Designated Official has the delegated authority to grant security clearances for official travel to areas designated Security Level 1 to 5. The Under-Secretary General for Safety and Security may rescind this delegation as required. Security clearance authority for areas in which Security Level 6 is in effect is not delegated and will be granted only by the Under-Secretary General for Safety and Security on behalf of the Secretary-General.

16. As explained in detail in Chapter V of the *Security Policy Manual*, "Security Clearance Procedures and the Travel Request Information Process (TRIP)", TRIP allows for both "automatic" and "manual" processes for granting security clearances. If the security plan for a certain location requires security clearance only to track traveller numbers and movement, then Designated Officials have the option of setting "automatic" clearances in TRIP.

17. When the security plan requires control over the number of travellers in a specific location, Designated Officials can set the TRIP system so that all official travel into a specific area has to be cleared manually. Manual security clearance procedures can be established at any location in any Security Level if the Designated Official requires it, and it is highly recommended that all areas in Security Level 4 or higher have manual security clearance procedures.

I. Relocation and Evacuation:

18. The Security Level System does not deal with evacuation and relocation of staff or eligible family members. This issue is categorized as a risk management option and is considered after the Security Risk Assessment has been conducted. See *Security Policy Manual*, Chapter IV, Section D, "Relocation, Evacuation and Alternate Work Modalities - Measures to Avoid Risk" for the procedures on

[1] For the purpose of this policy, "field location" is any location not designated as an "H" (Headquarters) duty station under the mobility and hardship scheme established by the International Civil Service Commission (ICSC).

[2] The HLCM, at its 20th Session "endorsed the objective of requiring that all official travel be registered in TRIP, on the basis of full integration between TRIP and each organization's travel system, by the end of 2011" (CEB/2010/5). Until the end of 2011, if an organization's travel system is not integrated, official travel of its personnel from "H" duty station to "H" duty station, as defined by the mobility and hardship scheme established by the International Civil Service Commission (ICSC), will not require security clearance. [By the end of 2011, or when all travel systems are integrated, this footnote will be removed from the policy].

making relocation and evacuation decision, as well as for issuing “All Agency Communiqués” to this effect.

Annex A: Security Levels System overview

Security Level		Recommended Management Actions[3]	Authority	Level of Oversight
6	Extreme	• SMT meets at least weekly (at DO discretion) • Re-evaluation of staffing needs and security clearance based on the "Acceptable Risk Model" and the new "concept of operations" and security plan • External Security Clearance approved by USG/ DSS	Secretary-General[4] (as delegated)	
5	High	• SMT meets at least weekly (at DO discretion) • Re-evaluation of staffing needs based on the "Acceptable Risk Model" (Staff in non-critical posts relocated/evacuated) • Security clearance required	DO	USG/DSS (validation within 7 days)
4	Substantial	• SMT meets at least bi-weekly (at DO discretion) • Re-evaluation of staffing needs and security clearance based on the "Acceptable Risk Model" • No external conferences	DO	USG/DSS (validation within 7 days)
3	Moderate	• SMT meets at least monthly • External conferences must be authorized by DO	DO	Director DRO/DSS (validation within 7 days)
2	Low	• SMT meets at least twice a year • External conferences organizer must notify DO	DO	Director DRO/DSS (validation within 7 days)
1	Minimal	• SMT meets at least twice a year • TRIP entry for all official travel	DO	Director DRO/DSS

[3] Every SMT meeting must review the Structured Threat Assessment as part of the required validation of the Security Risk Assessment. A change in the Structured Threat Assessment launches the Security Risk Management process, the result of which will be specific and appropriate security management actions.

[4] Should the Secretary-General decide that a minimum number of staff may remain in a Level 6 location, the Executive Heads will decide whether their staff may operate in this environment.