

CHAPTER IV

Security Management



Section Q

POLICY ON CHEMICAL, BIOLOGICAL, RADIOACTIVE AND NUCLEAR THREATS AND ATTACKS

Promulgation Date: 23 January 2019

A. Introduction

1. Chemical, Biological, Radiological, and Nuclear (CBRN) events are actions or occurrences that may lead to the release or dispersal of hazardous materials that put individuals or groups at significant risk. CBRN events are of serious health, safety and security concern to United Nations personnel¹.
2. The release of hazardous materials in a CBRN event can be non-deliberate, such as those caused by industrial accidents, disease, natural disasters, or discovery of remnants of war. The release can also be deliberate, with the goal of causing injury, death, disruption, or fear. This policy only addresses the deliberate release of CBRN agents, in line with the current distinction made between safety (non-deliberate events) and security (deliberate events) in the United Nations Security Management System (UNSMS)². Safety risk management³ should provide the framework for the prevention and mitigation of safety-related events resulting from a non-deliberate release of CBRN agents.
3. The characteristics and effects of CBRN agents are unfamiliar to most people. The threats associated with CBRN attacks create anxiety and fear due to their nature and impact. The Guidelines entitled Operational Considerations for Unintended Toxic Chemical Weapons Exposure⁴ provide basic information on chemical warfare agents and other chemicals used as weapons and on basic first aid and operational reaction in the event of exposure. Similar information regarding biological, radiological and nuclear events, which are extraordinarily rare, is available in open sources.⁵ Care should be taken when using open sources, as not all CBRN open source material is authoritative.
4. Nothing in this policy contradicts existing relevant emergency response frameworks including, among others, those coordination frameworks to which the United Nations system organizations, Host Governments, Member States, regional organization and other international organizations such as the OPCW have already agreed.

B. Purpose

5. This policy outlines the principles of the UNSMS for managing CBRN threats or the consequences of a CBRN attack in areas where United Nations personnel operate in order to ensure a coordinated and efficient approach, in collaboration with Member States and other intergovernmental organizations.

¹ All individuals as defined in Chapter III of the *Security Policy Manual* on “Applicability of the United Nations Security Management System.”

² *Security Risk Management Manual*

³ For example, Occupational Health and Safety (OSH)

⁴ *Security Management Operations Manual*.

⁵ See “[Chemical, Biological, Radiological and Nuclear Response: Introductory Guidance](#)”, International Committee of the Red Cross (ICRC); “[Nuclear, Radiological, Biological and Chemical events – in Brief](#)” (ICRC)

6. This policy aims to assist the Designated Official (DO), the Security Management Team (SMT), and United Nations security professionals, as well as programme managers, in carrying out their security management responsibilities to minimize the risks to the United Nations while operating under a CBRN threat or to manage the consequences of a CBRN attack, in line with the Framework of Accountability⁶.

C. Applicability

7. The policy is applicable to all UNSMS organizations as well as all individuals defined in Chapter III of the *Security Policy Manual* (“Applicability of the United Nations Security Management System”). All references to the United Nations herein refer to the United Nations and United Nations system organizations forming part of the UNSMS.

D. Definitions

8. The components of CBRN are defined as:
 - i. Chemical: naturally occurring or man-made toxic substances used in everyday life, industry and medicine, or for law-enforcement/military purposes;
 - ii. Biological: naturally occurring or genetically altered microorganisms (viruses, fungi and bacteria) and toxins (poisonous chemicals produced by biological organisms);
 - iii. Radiological: radioactive materials occurring naturally, as by-products of industrial processes or manufactured for use in industry or medical therapy;
 - iv. Nuclear: radioactive materials generated by nuclear fission or fusion, such as those associated with an operating nuclear power plant or with the detonation of a nuclear weapon.
9. CBRN attacks may be conducted by States, Non-State Armed Groups, criminal groups, or individuals.
10. CBRN attacks may result in hazardous conditions in the operating environment such as the contamination of air, water, or earth with harmful chemicals, residual biological agents, radioactive material, or irradiated materials from a nuclear explosion, such as radioactive fallout in the atmosphere or radioactive water or other substances.

⁶ Please refer to *Security Policy Manual* Chapter II, B.

E. Principles

11. The primary responsibility for the security and protection of United Nations personnel and assets from CBRN threats and for consequence management of CBRN attacks affecting said personnel and assets rests with the Host Government.
12. The CBRN threats and responses are sensitive by nature and must consider host nation capabilities, perceptions of governments, local authorities, as well as the perceptions of the general public. During armed conflict, parties to the conflict may note the nature and scale of UNSMS actions, and they may have conflicting perceptions of those actions. It is therefore important, wherever possible, to anticipate and prepare for scenarios as part of security planning and to consider the consequences of possible actions.
13. Where the risk is unacceptable (very likely and critical impact or compared with programme criticality), risk avoidance is required, so United Nations Security Management System (UNSMS) organizations will not undertake or continue operations in an environment where CBRN attacks are occurring or have occurred. Appropriately-trained and equipped personnel from entities with mandates to operate in environments with CBRN hazards may undertake or continue operations after an attack⁷ if such training and equipment lower the likelihood and/or impact so that the risk is acceptable.
14. The threat of CBRN attacks is addressed at the field level through the SRM process. Recognising that these types of threats are highly technical and require appropriate expertise, the DO is encouraged to seek expert resources primarily from specialised UNSMS organisations, Member States (as feasible in the local context), other international organizations. Subject matter experts will be essential to identifying appropriate security management measures and to preparing specific scenarios and responses as part of security planning⁸.
15. In responding to a CBRN event, the primary objective is to reduce the risk of injury from exposure. The three key steps to take are:
 - (a) To avoid exposure, especially inhalation of CBRN agents or material
 - (b) Remove agents from exposed skin, hair and clothing by decontamination
 - (c) Seek medical attention
16. Security Risk Management Measures (SRMM) identified to manage CBRN risks may require specialized training and the acquisition of equipment that can be considered sensitive by some host governments. No measure should be selected if it cannot be realistically implemented, nor equipment acquired if prohibited by local restrictions. These measures should be regularly reviewed by the DO to ensure continued relevance.

⁷ Organizations such as the Organization for the Prohibition of Chemical Weapons (OPCW) and the International Atomic Energy Agency (IAEA).

⁸ *Security Policy Manual*, Chapter IV, Section B: “Security Planning”

F. Roles and Responsibilities

17. The SMT members, and the most senior security professional directly supporting the DO⁹ are responsible for ensuring that CBRN events are considered and managed through the Security Risk Management (SRM) process. The SRM process requires that the DO and the most senior security professional directly supporting the DO maintain close liaison with Host Government authorities in all aspects of security management, including on CBRN threats, on behalf of the United Nations, and to consult, as necessary, with the Under-Secretary-General for Safety and Security in implementing this policy.
18. When finding that Host Government support or capacity to respond is inadequate, the DO must report this to the Under-Secretary-General for Safety and Security to request strategic interventions at the appropriate level. It is preferable to acquire required CBRN technical advice from UNSMS organizations¹⁰, however, commercial providers and the direct hire of experts as staff or consultants may be optimal in certain circumstances. The DO is responsible for consulting with the Under-Secretary-General for Safety and Security when deciding which approach will best meet the requirement for CBRN expertise in a timely manner.
19. The most senior security professional directly supporting the DO is responsible for reaching out to relevant expertise within the United Nations system or acquiring such expertise from commercial providers to ensure that CBRN threats are properly analysed, reviewed and that the SRMM are adapted. These measures could include alternate work modalities, relevant awareness programmes for personnel, planning for consequence mitigation of assessed, specific CBRN risk scenarios. In cooperation with relevant experts, security planning, as deemed feasible according to specific contexts, might include the development of awareness information products such as signs and handbooks, prepositioning decontamination kits, post-exposure antidote/medication, and acquisition or deployment of early warning tools in a range of settings, possibly to complement evacuation or shelter-in-place plans or procedures.

G. Training Requirements

20. This policy and relevant training on decision-making in the CBRN threat context shall be included in the security training for DOs, SMT members, security professionals, and managers in the United Nations system organizations posted in SRM areas with identified CBRN threats who have responsibility and

⁹ This is usually the Principal/Chief or Security Adviser (P/C/SA) or his or her 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 there is no assigned international professional security advisor).

¹⁰ Organizations such as the Organization for the Prohibition of Chemical Weapons (OPCW) and the International Atomic Energy Agency (IAEA).

accountability for security management in line with the Framework of Accountability for the UNSMS.

21. Training relevant to specific CBRN security risks and specified as SRMM will be provided to UNSMS personnel by relevant organizations such as the OPCW, the IAEA, the WHO, or if so determined by these UN expert entities, commercial providers, as *ad hoc* training, as modules integrated into regular security training courses, or as otherwise deemed appropriated by the DO and SMT.
22. Technical guidance on risk management will be made available to personnel in relevant SRM areas by specialized organizations¹¹ within the scope of their mandates or through commercial providers, if necessary; however, its purpose will be for the generalist security official to gain an understanding of CBRN threats and possible mitigation measures.

H. Final Provisions

23. This policy is to be distributed to all United Nations personnel.
24. This policy enters into effect on 1 June 2019.

¹¹ i.e. OPCW, IAEA, WHO