EUROPEAN COMMISSION
ENTERPRISE AND INDUSTRY DIRECTORATE-GENERAL

Space, security and GMES
GMES Bureau

GC-GMES-2011/16

ROADMAP FOR THE GMES SECURITY POLICY

In Regulation 911/2010 on the European Earth monitoring programme (GMES) and its initial operations (2011 to 2013), the EU Parliament and the Council tasked the Commission with the responsibility *«of the implementation of the GMES security policy, assisted by the Committee. For that purpose, a specific configuration of the Committee (the 'Security Board') should be set up.* »

A first meeting of the Security Board is planned in June. This document describes a roadmap for the GMES security policy and its implementation.

In view of the preparation of the 1st Security Board, the members of the GMES Committee (GC) are invited to exchange views on this roadmap, and to discuss the following questions:

- Ø Do you agree with the proposed roadmap?
- Ø Do you agree with the prioritisation of issues to be discussed by the Security Board?
- Ø What are your expectations for a risk assessment exercise?

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.
Office: BREY 9/215. Telephone: direct line (32-2) 2961.183. Fax: (32-2) 2920.767.
E-mail: clement.williamson@ec.europa.eu

1. INTRODUCTION

With the GIO regulation, GMES is becoming operational. As part of the overall implementation of the GMES programme, security is an important concern. Together with the setting up of operational services, and preparing the post-2013 period, it is necessary to put in place several procedures and mechanisms, notably for what concerns security. The GMES system, or system of systems, is broad and complex, and it is still partially in a definition phase. GMES is developed in coherence with GEO/GEOSS principles and the INSPIRE directive and should respect the data policies of contributing missions. GMES is composed of various components for which governance aspects (e.g. ownership, responsibilities of operators, national or international jurisdictions) are various and sometimes remain to be defined. The role and responsibility of the European Commission may vary from one component to the other. Nevertheless with regards to the security aspects of GMES components, the Commission, assisted by the Security Board, should ensure the overall coordination[1].

Particular attention will have to be dedicated to security aspects of GMES data policy. The GMES data policy has the objectives of a *«full and open access to information produced by GMES services and data collected through GMES infrastructures, subject to relevant international agreements, security restrictions (...)»*. It is important to ensure that GMES does not distribute information that could endanger the security of the Union, its Member States and its citizens to non authorized users. By potentially restraining the dissemination of information, the GMES security policy has important implications for the GMES data policy.

In 2010, the Council Security Committee (CSC) adopted recommendations on the security of GMES. They consist of 15 recommendations about: the principles, the governance, the responsibilities, the GMES data, the GMES infrastructures, and the integration of existing capabilities.

The GIO regulation states the need to implement GMES consistently with other European programmes, and in particular the European Global Navigation Satellite System (GNSS). While there are significant differences in terms of security for the two programmes, it is felt important to take full advantage of the experience already acquired, in particular for what concern methods and procedures developed with the GNSS Security Board.

Taking into account the elements above, it is proposed to start the implementation of the GMES Security policy under the GIO through:

1) a definition of the GMES security policy;

2) a dedicated risk assessment exercise;

3) the definition of governance, management and implementation modes.

The Security Board established by the GIO regulation and composed of Member States representatives, will have the role to assist the European Commission in this process.

---

[1] cf. GIO Regulation N°911/2010: «The Commission should be responsible for the implementation of the GMES security policy, assisted by the Committee. For that purpose, a specific configuration of the Committee (the 'Security Board') should be set up. »

2. GMES SECURITY POLICY

In addition to the normal obligations for the Commission linked to its role of coordinator of the GMES programme, the following elements of the security policy can be found in the GIO regulation:

- GMES information should be fully and openly accessible, without prejudice to relevant security restrictions (…) – Art.9(2);
- Adopt (…) specific measures on restricting access to the information produced by the GMES services and to data collected through the GMES dedicated infrastructure, including individual measures taking into account the sensitivity of the information and data in question – Recital 11 and Art.13(1);
- (…) ensure the control and integrity of the system within the GMES space component dedicated programme – Art. 13(2);
- (…) control the access to, and handling of, technologies that provide security to the GMES space component dedicated programme – Art. 13(2);
- (…) contributing to the sustainability and continuity of the provision of GMES data and information – Art. 9(1);
- (…) ensure authenticity, traceability and data integrity – Art. 5(3);
- (..) ensure the attainment of the GMES information and data policy objective (…) while providing for the necessary protection of the information produced by the GMES services and of data collected through the GMES dedicated infrastructure – Art. 9(2);

Starting from these elements, it could be worth translating the GMES Security policy into a list of high-level objectives.

A non-exhaustive list of high level objectives of the GMES Security policy (to be discussed by the Security Board) could be:

(1) Prevent the misuse of any data potentially harmful to the EU and its Member States and their citizens;

(2) Prevent unauthorized access to data/information (e.g. leading to breach to any legal restrictions such as national space laws or licences from contributing elements);

(3) Ensure integrity of data/information, including traceability and authenticity;

(4) Ensure continuity of services;

(5) Allow a permanent monitoring / dynamic management of security issues;

(6) Protect GMES users and personnel involved;

(7) Protect the GMES infrastructures.

Most of these objectives are interconnected and need regular updating.

3. RISK ASSESSMENT

The GMES Security policy should be based on an assessment of the threats and vulnerabilities of the system. The evaluation of risks should be done component by

component at the appropriate level of detail taking into account, among other parameters, the different responsibilities of the involved partners. In parallel, risk mitigation measures have to be proposed and assessed.

As an example, for well established contributing missions, it could be acceptable to receive certain guarantees from the operators/owners that appropriate security measures are implemented while, for other elements, an in-depth risk analysis will need to be performed. As new threats can rapidly emerge and as the system will continuously evolve, the overall risk assessment has to be performed regularly.

3.1. Threat and Vulnerability analysis

The risk assessment is a combination of likelihood of threats occurring and their potential impacts. It starts with a threat and vulnerability analysis based on a definition of the overall system and each component.

An important part of the risk is driven by the potential harmfulness of the data. By analogy with several existing comparable infrastructures, it is felt that this potential is rather limited for most of the components of the system. Thus, it is important in this exercise to distinguish between the different sources of data (e.g. Sentinel satellites, in-situ components, contributing missions, services…).

3.2. Definition of possible mitigation measures and their cost

Following the risk assessment exercise, possible mitigation measures have to be considered, for example taking the form of recommendations (e.g. to impose limitation in the data dissemination, or to accept the risk without specific mitigation measure). Recommendations should also take into account risks which can warrant risk treatment that is not justifiable on economic grounds, e.g. severe (high negative consequence) but rare (low likelihood) risks or secondary risks implied by the mitigation measure itself[2].

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived. The costs and efforts implied by possible mitigation measures will have to be carefully analysed, including as to who would cover the respective additional costs.

4. GMES SECURITY GOVERNANCE, MANAGEMENT AND IMPLEMENTATION PLAN

Following the risk assessment exercise, a chain of responsibility should to be established for the different elements of the system taking into account their specificities.

On this basis, a GMES Security management and implementation plan could be drafted to deal with different security measures to be implemented. It could include:

- the definition of the GMES Security Policy;
- a description of the GMES Security governance, methods and processes;

[2] Cf. ISO 31000 Risk management — Principles and guidelines

- a list of reference documents;
- other relevant elements following discussion by the Security Board.

5. CONCLUSIONS AND TIMING

GMES is a complex system whose ownership and responsibilities are shared and still under definition. The Commission, advised by the Security Board, plans to initiate a risk assessment of the system and each of its components together with the relevant partners involved. The Security Board should also discuss the goals for an overall GMES Security policy and the methods and governance of its implementation.

Ø First meeting of the GMES Security Board (June 2011):

The purpose of this meeting will be to discuss the most urgent items of a security policy: a risk assessment based on an analysis of threats and vulnerabilities. Pragmatically, this work should be carried out initially in relation to the space component and the services entering into the operational phase (i.e. Land and Emergency). For the space component, the process should start with the Sentinels given that they are specifically developed for GMES.

However, such a prioritisation should not loose sight of the need to agree on a set of (high level) security objectives (beyond what is stated in existing documents like the GMES regulation, the Council Security Committee recommendations[3], or relevant ESA documents[4]) and the need to define a more precise mandate for the Security Board, its working method and documents expected to be developed. An outline for a tentative agenda for the first meeting of the security board is annexed to this roadmap.

To support these discussions, a first set of draft **working documents** will be circulated in advance to the meeting planned in June:

- an overall planning for GMES and the implementation of the Security policy;
- a draft GMES Security Management Plan describing the Security policy, methods and processes, chains of responsibilities and reference/subsequent documents;
- an initial draft of the risk assessment of the GMES space infrastructures, excluding the contributing missions, i.e. the Sentinel satellites and the ground segments (characterisation, initial threat and vulnerability exercise, security measures in place…);
- a basic description of the initial GMES Land monitoring service (from a security point of view);
- a basic description of the initial GMES Emergency management service (from a security point of view)

Ø Second meeting of the GMES Security Board (autumn 2011):

[3] Note 5213/10 from the Council Security Committee experts' sub-area for GMES data security to the CSC: Recommendations on GMES data security policy.

[4] Such as the Joint Principles for a Sentinel Data Policy - ESA/PB-EO(2009)98

This meeting will offer the opportunity to progress on the elements discussed during the first meeting and to start dealing with the other elements of the system like the in-situ component, contributing missions, services still in the development phase or other possible transversal infrastructures (e.g. for archiving, communication, data distribution…).

Ø Further work of the GMES Security Board (end 2011- mid 2012):

Provisional security inputs to the GMES data policy should be provided by the end of 2011 to be integrated in the wider GMES data policy foreseen for 2012 (delegated act).

***

Contact:
Clément Williamson, Telephone:(32-2) 2961.183,
clement.williamson@ec.europa.eu

1st meeting of the GMES Security Board
June 2011
Outline of the draft agenda

- Adoption of Rules of procedure
- Discussions on the role and working methods of the Security Board and on the GMES Security policy
- Overall planning for GMES and the implementation of the Security policy
- Risk assessment of the Sentinels
- Risk assessment of the Emergency management service
- Risk assessment of the Land monitoring service