EUROPEAN COMMISSION
ENTERPRISE AND INDUSTRY DIRECTORATE-GENERAL

Space, security and GMES
GMES Bureau

SB-GMES-2012/11

GMES Data Policy workshop – GMES Security Board

12 – 13 January 2012

Security restrictions applicable to the data policy for the Emergency Management Service

The preliminary security aspects of the Emergency Management Service (EMS) has been prepared and discussed at the first Security Board which took place on 30 June 2011.

In the meantime, the reflection on a GMES data and information policy has made substantial progress, including the dissemination rules of products generated by GMES services. Moreover, the workflow and the activation mechanism of the Emergency Management Service has been refined in the context of the GMES Initial Operations.

This document is aimed at compiling all recent achievements and at updating the criteria for security restrictions that might be applicable to the Emergency Management Service in the frame of the GMES Data Policy. It will be used as a basis for discussion at the occasion of two events taking place back-to-back on 13 January 2012: (i) Security session of the GMES Data Policy workshop, and (ii) GMES Security Board.

This document is presented to the GMES Data Policy workshop and the GMES Security Board for discussion.

Table of Contents

1. BACKGROUND 3

2. POSSIBLE SECURITY ISSUES OF THE EMS 3

3. GOVERNANCE OF THE EMERGENCY MANAGEMENT SERVICE 4

4. LIST OF AUTHORISED USERS 5

5. ACTIVATION CRITERIA 5

5.1. STANDARD TRIGGERING CRITERIA FOR EMERGENCY SITUATIONS INSIDE AND OUTSIDE EUROPE– RUSH MODE 5

5.2. STANDARD TRIGGERING CRITERIA FOR EMERGENCY SITUATIONS INSIDE AND OUTSIDE EUROPE – NON-RUSH MODE 6

5.3. POTENTIAL SECURITY CRITERIA FOR EMERGENCY SITUATIONS OUTSIDE EUROPE – RUSH AND NON-RUSH MODES 6

6. CONTROL OF THE DIFFERENT PRODUCTION PHASES OF THE SERVICE 7

6.1. ACCESS TO VERY HIGH RESOLUTION DATA 7

6.2. GENERATION OF PRODUCTS 7

7. DISSEMINATION PRINCIPLES 8

8. WAY FORWARD 9

1. BACKGROUND

The GMES data policy, based on a full and open access principle, is subject to security restrictions. To ensure this objective, the Commission may adopt, by means of delegated acts, measures defining criteria for those restrictions (Article 9 of the GMES Regulation). On the basis of those criteria, the Commission shall adopt specific measures, in accordance with the examination procedure, i.e. involving the GMES Committee in its Security Board configuration (Article 13 of the Regulation).

This document is aiming at compiling all recent achievements and at updating the criteria for security restrictions that might be applicable to the Emergency Management Service in the frame of the GMES Data Policy.

2. POSSIBLE SECURITY ISSUES OF THE EMS

The Security aspects of the Emergency Management service[1] submitted to the Security Board in June 2011 identified four areas of sensitivity:

a. Actors involved on the activation / service cycle
b. Input satellite data
c. Content of service outputs / products
d. Dissemination

Areas	Potential sensitivity issues	Security response
a/ Actors involved in the activation / service cycle	– origin of the demand (user identification) – authority in charge of the acceptance or rejection of the activation – criteria for decision-making, including geographical area of interest (complex crisis area with civil unrest, local political stability at risk, military operations, critical infrastructure) – operators in charge of the interpretation and preparation of maps	– list of authorised users – governance of the service – activation criteria – governance of the service
b/ Input satellite data (GMES Contributing Missions)	– GCM data identified as sensitive (eg VHR data over sensitive area) – In very few cases, Sentinel data	– "shutter control" – exert control on the service steps
c/ Content of service outputs / products (maps, vector layer…etc)	– age of the map, timeliness (near real time) – accuracy, scale – some risk maps (e.g. dam bursting)	– exert control on the different production steps of the service
d/ Dissemination	– public overreaction – misuse of maps	– dissemination restrictions

[1] Security aspects of the Emergency Management Service, SB-GMES-2011/05, 30 June 2011

3. GOVERNANCE OF THE EMERGENCY MANAGEMENT SERVICE

The service is civilian in nature, uses civilian capacities and has civilian purposes. It can encompass natural and man-made disasters, including environmental and technological disasters as well as complex crises where it will support the operations of humanitarian or civil protection actors in line with the humanitarian principles. The service is global in scope.

Pursuant to Regulation (EU) 911/2010 on GMES and its initial operations, the objective of GMES Emergency Management Service is to provide users (mainly Civil Protection and humanitarian aid communities) with information in support to their relief operations, in particular in relation to different types of disasters, including meteorological hazards (including storms, fires and floods), geophysical hazards (including earthquakes, tsunamis, volcanic eruptions and landslides), deliberate and accidental man-made disasters and humanitarian disasters. The service will include rush mapping activities (disaster response) and non-rush mapping activities (preparedness and recovery).

Responsibilities are shared between DG ENTR (overall coordination), DG ECHO (role of operational coordination incl. interface with the users and authorisation of the activations based on a set of criteria) and DG JRC (role of technical support, contractual management and monitoring of activations). DG ECHO will ensure the interaction with Authorised Users, in particular national civil protection authorities, humanitarian aid actors and EEAS.

The activation of the service, for both rush and non-rush mapping activities, will be based on several basic principles:

i. Only Authorised Users (AUs) will be allowed to trigger the service. Since the GMES EMS is a service funded by the EU budget and managed by the EC, the AUs implicitly accept to share their information on activation and outputs of the Service with the EC;
ii. The first priority of the service should be to serve large scale national or cross-border disasters in Europe and large scale crises outside;
iii. A **single interface (ECHO European Emergency Response Centre/EERC)** is presently being defined for the activations by Authorised Users, including rush and non rush mode. ECHO/ERC will be in charge of the clearance of requests;
iv. The generation of products (operations) will be carried out by different service providers under service framework contracts;

The overall activation procedure and workflow of the service will be fully described in a User Manual which will include the content of the service, the authorised users, the criteria for selecting the user request in rush and non-rush mode, and the dissemination rules.

4. LIST OF AUTHORISED USERS

The list of Authorised Users may be:

(1) European users for disasters within Europe:

(a) National Focal Points (NFP) in Member States. The basic principle is that the requests placed by MS will be channelled through the national focal points: regional users will submit request through their NFP;

(b) National Focal Points from Countries participating to the Civil Protection Mechanism (Croatia, Iceland, Norway, Liechtenstein). Regional users will also submit request through their NFP;

(c) European Union Services, including Commission services (DG ECHO/EERC, DG HOME, …) and other European services (EEAS);

(d) Possibly other Implementing European Agencies.

(2) European users for disasters outside Europe:

(a) National Focal Points in Member States;

(b) National Focal Points from Countries participating to the Civil Protection Mechanism (Croatia, Iceland, Norway, Liechtenstein);

(c) European Union Services, including Commission services (DG ECHO/EERC, DG HOME, …) and other European services (EEAS). Delegations and Regional Offices would go through their Head Quarters.

(3) Non European users for crisis outside Europe:

(a) Any government affected by disaster may trigger the service through ECHO/EERC, provided that assistance has been formally requested through the Civil Protection Mechanism. If it is not the case, triggering is proposed to go through UN OCHA as a Focal Point;

(b) International Governmental Organisations and International non governmental organisations, such as from the UN-family, or the International Red Cross and Red Crescent Movement;

(c) National Non-Governmental Organisations will pass through AUs, preferably National focal Points but in exceptional cases also the UN FP.

5. ACTIVATION CRITERIA

5.1. Standard triggering criteria for emergency situations inside and outside Europe – rush mode

(1) Predefined types of events inside Europe where activation may be accepted (it will be up to NFP to decide on activations on their territory. In cross border events EERC may trigger in cooperation with the Civil Protection Mechanism). Generally this will be in:

(a) relatively large scale disasters;

(b) types of disasters compliant with EMS scope;

(c) cases where serious impact on lives with expected casualties is registered;

(d) cases where serious impact on property, nature, cultural heritage (civil protection mandate), critical infrastructure, environment and local economy can be expected;

(e) cases where several days will pass before the situation can be expected to return to normal.

(2) Predefined types of events outside Europe where activation may be accepted. Generally this will be in:

(d) relatively large scale disasters;

(e) types of disasters compliant with EMS scope;

(f) cases where serious impact on lives with expected casualties is registered;

(g) cases where serious impact on property, environment, cultural heritage; environment (civil protection mandate), critical infrastructure and local economy can be expected;

(h) cases where several days will pass before the situation can be expected to return to normal;

(i) cases where impact clearly exceeds capacities of local authorities to respond and rescue population and/or where lack of local GIS data hampers assistance efforts;

(j) certain disaster prone geographical areas based on existing scientific data (e.g. EM-DAT database of Centre for Research on the Epidemiology of Disasters);

5.2. Standard triggering criteria for emergency situations inside and outside Europe – non-rush mode

Most of the above criteria will apply. In addition for Disaster Risk Reduction, Prevention and Preparedness purposes, there will be various concerns about the need to have Reference maps on hotspot areas around the world. The scope of the non-rush service will be based on priorities to be finalised for the start of the EMS in 2012. These priorities may include a focus on Africa and on humanitarian requirements, e.g. on areas where the population is likely to be exposed to large scale emergencies and where identification and monitoring of IDP/Refugees is needed.

5.3. Potential security criteria for emergency situations outside Europe – rush and non-rush modes

Security criteria will be defined at the appropriate policy level. They will be used by DG ECHO/EERC in the evaluation of triggering request. DG ECHO/EERC may consult the relevant European service (e.g. European External Action Service) on a case by case basis if a potential security risk is identified. The security criteria may include:

(1) Type of events (e.g. complex crisis);

(2) Local political stability at risk;

(3) Ongoing of expected civil unrest;

(4) Impact on critical infrastructures;

(5) Existing or planned military operations.

6. CONTROL OF THE DIFFERENT PRODUCTION PHASES OF THE SERVICE

6.1. Access to Very High Resolution data

The emergency management service needs access to satellite data, mostly from GMES Contributing Missions (GCM) and to a limited extent from Sentinel missions. None of these satellite data are classified. For the latter, the access will be determined by the Sentinel data access policy to be formally adopted by the EC.

In the current design of the EMS service for the 2011-2013 period, it is not planned that service providers could be authorized to access classified space data.

For most of emergency situations, access to Very High Resolution satellite data is required, typically at a resolution below one meter. Additionally, the timeliness of the delivery is as well a key element for the quality of the service. These two parameters demonstrate the potential sensitivity of the primary data.

Access to European GMC data is subject to national shutter control mechanisms and to space laws. GMES will not supersede the existing national Regulations. EU Member States will continue to apply their national security regulations and data access policies. Access to non European satellite data providers will follow a similar scheme, whereby the owner of the satellite will apply the existing dissemination rules applicable by its national security authority.

Providing primary satellite data to users of the EMS may be allowed, depending on the security restrictions and the licensing conditions agreed between the satellite data provider and ESA in charge of the Data Access Portfolio in the framework of the Data Ware House.

In case of security concerns, the Commission may decide to:

– Shut down the activation;
– Limit/stop the dissemination of primary satellite data in the GMES framework.

6.2. Generation of products

There are four security concerns related to the information content of the maps:

(1) Geographical area of interest (e.g. covering complex crisis, critical infrastructure or areas with military operations);

(2) Timeliness and age of the map (higher sensitivity for most recent or near real time maps);

(3) Accuracy / scale : detailed or contextual maps (scale ranging from 1/5,000 to 1/25,000) may be considered as sensitive, depending on the area covered;

(4) Risk mapping (non rush mode): the potential impact caused by a disaster that could be induced by human intervention can be sensitive.

In the current design of the service for the 2011-2013 period, it is not planned that service providers could be authorized to produce classified information.

In case of security concerns, the Commission may decide to:

– Shut down the activation;
– Limit/stop the dissemination of products in the GMES framework;
– Classify the products.

7. DISSEMINATION PRINCIPLES

Several categories may be identified for the dissemination of GMES satellite data, maps and reports/information. The different level of dissemination will depend on the security restrictions that may be applicable in the frame of the GMES data and information policy. The dissemination categories could be :

(1) Relevant Commission services (ECHO/EERC, ENTR, JRC, …) and the EEAS;

(2) The Authorised User who triggered the service;

(3) The entire group of European Authorised Users for emergency situations inside Europe;

(4) The entire group of European and non European Authorised Users;

(5) General public.

The two main concerns in the dissemination are:

– the potential over-reaction of the public: over-reaction of the public may occur when disaster products can provoke an unexpected chain reaction. But such a situation would be exceptional, and can be overcome by an appropriate and anticipated analysis of the likely impact to the public.

– the misuse of products: products may be used for non peaceful applications by ill-disposed users. The misuse of maps can be prevented at two levels: (i) in the upstream decision process by cancelling the service activation, first at EU level with the rejection of the service activation and second at national level with the shutter control of satellite programming request; and (ii) at the service level with the restricted access to products, according to dissemination rules (e.g. products distributed to authorised users only).

Whatever the sensitivity of products, the dissemination will be done towards Commission Services and EEAS. Then the following may apply:

a. not sensitive products: full dissemination to all authorised users (groups 2, 3 and 4 above defined). The distribution to other categories of users, including sub-level emergency operators and the public, should remain under the responsibility of the authorised users;

b. sensitive products (classification is not considered here): dissemination limited to the Authorised User who triggered the service. If the crisis is located in Europe, further dissemination to neighbouring countries or to all NFPs may be decided by DG ECHO/EERC, pursuant to the Civil Protection Mechanism Regulation, without the possibility to redistribute the product. If the crisis is located outside Europe, dissemination can be considered to the Authorised User who triggered the service and to European NFP, without the possibility to redistribute the products.

Temporary or permanent restrictions might be decided depending on the level of sensitivity. At EU level, the dissemination of products is proposed to be in two steps: first step to categories (1) and (2) (relevant EC services and MS NFP activating the services) prior to the dissemination of products to other categories.

8. WAY FORWARD

The User Manual of procedures will cover all aspects related to the triggering of the service and to the workflow. It will be issued at the latest in March 2012.

The Delegated Acts related to the GMES data and information policy will include the security restrictions that may apply to the EMS service. However, security concerns are limited and are expected to be tackled through specific measures:

- the list of security criteria will be finalised by the European Commission after consultation with relevant European services (e.g. EEAS);
- the triggering acceptance or rejection will be under the full responsibility of the EC (DG ECHO/EERC) who should keep an overall control of the different production steps
- the User Manual will be prepared with a clear description of tasks and responsibilities for all actors involved in the service, including industrial service operators;
- existing national data dissemination policies and laws will apply for the access to VHR satellite data;
- the dissemination rules will be compliant with the Delegated Acts and the applicable security restrictions.

In case of unforeseen security threat, the situation will be monitored by the EC who will take the appropriate decisions on a case by case basis.