# TSA 1.2 2011 Plan

## EGI CSIRT Plan

EGI CSIRT incident response sub-task will continue to coordinate and handle security incident reported to EGI CSIRT; It is now agreed that EGI CSIRT and EGI SVG take joint effort to assess security vulnerabilities and other operational security risks:

1. If needed, to produce an updated security incident handling process as part of MS412 PM15 operational Security Procedures by **August 2011**;
2. Continue to develop and improve CSIRT operational security procedure. To complete the critical operational security handling procedure by **31st January 2011**; To complete the EGI CSIRT/SVG internal detailed procedure for handling critical software vulnerabilities by **31st March 2011**;
3. Continue to improve EGI sites' security patch management through
   - Security Dashboard (see below for more detail)
   - Security Metrics, this will allow management to have a high level view on site security posture. CSIRT is collecting input on this. We do not anticipate this work will complete by end of 2011; but some of the work will be used in the security dashboard development
   - Encourage EGI sites to deploy Pakiti locally
4. A ticket system (RTIR) for security incident coordination is being setup by CSIRT; it will be used by CSIRT to cooridnate security incident across EGI infrastructure; It will be ready for EGI CSIRT by **30th April 2011**

Security drill sub-task will design and set-up realistic simulations of computer security incident scenarios – security service challenge (SSC):

5. Some improvement of the security challlange frame will be completed by **7th April 2011**. Up to 5 NGIs will participate the first phrase of NGIs SSC4 run. By **30th June 2011** development of SSC framework will complete, which will allow us to scale up the challenge so that more NGIs can participate;
6. To have a cross-NGIs security challenge to check and/or improve the overall coordination capability of EGI CSIRT. The challenge will simulate a security incident affecting many sites at once; This will complete by **30th June 2011**;
7. Integrate other experiment Job-submission frameworks such as CMS will be studied, but it will not be completed by end of 2011;

Security monitoring sub-task will continue to develop and enhance CSIRT security monitoring framework such as Nagios and Pakiti

8. Security Dashboard Development: CSIRT is currently working with OTAG and operation dashboard developers to implement and integrate a Security Dashboard into the operation dashboard; the security dashboard will allow sites, NGIs and CSIRTs to access security alerts in a controlled manner
   - Complete requirment analysis by **28th Feb. 2011**
   - The first prototype will be ready for testing by EGI CSIRT by **30th June 2011**
   - The first release will be available by **31st Dec. 2011**;
9. The improvements and feature enhancement of Nagios and Pakiti will continue, which include to add statitic function; to improve user interface; to add automatic alerting and to visualize security monitoring data etc. Some of the work will be used by the security dashboard (complete by 31st Dec 2011), other will be used by the security metrics (early 2012);

Security training and dissemination sub-task plans to organize a security training at next EGI technical forum sometime **September 2011**;

EGI CSIRT will also carry out some backgroud research work in the area of security in the cloud/virtulaziation environment and IPV6 security.

## EGI Software Vunerability Group (SVG) Plan

EGI software vulnerability group will continue handling vulnerabilities reported to the EGI SVG group. It will ensure issues reported to the group are investigated and assessed in a timely manner:

1. Produce an updated vulnerability handling process as part of MS412 PM15 operational Security Procedures by **August 2011**;
2. Collaborate with Members of the University of Wisconsin / Universitat Autònoma de Barcelona Middleware Security and Testing Group to produce a plan for Vulnerability Assessment of Grid Middleware used in the EGI infrastructure using their techniques; It is a cross-project activity. What EGI SVG is doing is helping with the plan to ensure that prioritization is carried out appropriately, and of course ensuring that any vulnerabilities found are handled according to our process.
   - A meeting is planned on **27th January 2011**;
   - An assessment plan is currently being written, and this should define which software is to be assessed and when they will be done. It is anticipated to complete the plan by **30th April 2011**;
3. Improve smooth running and efficiency of the issue handling process, including automation of some aspects of the issue handling using the EGI RT tracker; outcome of this activities will also be input for MS412, which is due August 2011

4. Collaborate on Vulnerability prevention, including advising on checking for common vulnerability types in the certification process, developer education, and the usage of safe libraries for carrying out common actions;