Security Coordination Group (SCG)

|  |  |
| --- | --- |
| **Venue:** | Telecon |
| **Date and Time:** | Tuesday 2nd February 2011 at 11 CET |
| **Agenda:** | https://www.egi.eu/indico/conferenceDisplay.py?confId=571 |

Participants 2

MINUTES OF THE PREVIOUS MEETING 3

ITEMS OF BUSINESS 3

CSIRT report 3

SPG Report 4

SVG Report 4

EUGridPMA IGTF report 5

CSIRT with other Grids 5

D4.4 discussions 6

AOB 7

Actions 7

Date for Next Meeting 8

Report from SPG 10

Report from SVG 11

Report from CSIRT 12

Report from EUGridPMA IGTF 13

# Participants

|  |  |  |  |
| --- | --- | --- | --- |
| Name and Surname | Abbr. | Representing | Membership[[1]](#footnote-1) |
| Steven Newhouse | SN | EGI.eu Director and CTO | Member |
| David Kelsey | DK | EGI SPG Chair | Member |
| Linda Cornwall | LC | EGI SVG Chair | Member |
| David Groep | DG | EGI Representative in EUGridPMA | Member |
| Mingchao Ma | MM | EGI CSIRT Chair | Member |
| Michel Drescher | MD | EGI.eu Technical Manager | Observer |
| Tiziana Ferrari | TF | EGI.eu Chief Operations Officer | Observer |
| Damir Marinovic | DM | EGI.eu Policy Development Officer | In attendance |

# MINUTES OF THE PREVIOUS MEETING

The minutes of the last meeting held on 10th February 2010 were reviewed. No other additions/corrections were reported. The minutes were approved as a correct record of the proceedings.

# ITEMS OF BUSINESS

## CSIRT report

MM: At the moment CSIRT is developing a security dashboard and plans to make it available for sites and NGIs by the end of this year, in order for them to have overview of their security problems. Security dashboard will be part of central dashboard, but with the separate interface. CSIRT spends lot of time on noncritical security issues; it seems that communication channels do not fit the purpose. Non-critical security issues will be tracked by RT tickets; CSIRT will be acting as a second and third line support, we w providing solutions; this is only for noncritical security issues. For critical ones CSIRT will follow-up directly and react with a swift response. Introduction of security dashboard will help bring non-critical security operation in line with normal operation. I would like to consult with others, what groups to approach for discussion in order to implement a security dashboard as soon as possible?

TF: Noncritical vulnerabilities that ROD team and the NGIs encounter; they should be instructed how to provide a support on vulnerability issues. MM: This is really like any other alert, e.g. NAGIOS test. If there is an alert, site should look for solution, if there is no response, it should be escalated to COD and COD will follow up. Security monitoring can produce alert, if nothing happen after certain period of time, site will be suspended. TF: For example, open GGUS ticket that cannot be solved, one should send it to CSIRT. MM: Whenever we have identified the issue we will provide advisory, the real problem for us is how to follow up, we don’t have enough resources, providing solution is not a problem. It is a time consuming, and we don’t have means to check how to pursue them; NOC manager mailing list helps to certain extent. TF: This and issue of harmonising the existing procedures; it is indeed the correct approach. CSIRT should be contacted for specialized support by raising a ticket to CSIRT. If would be nice to see diagram with workflows. The other thing is first line support for critical issues; it is little bit more complicated.

SN: No objection from SCG, we agree to keep CSIRT role in separating out routine security follow up from the exceptional follow up.

## SPG Report

DK presented the latest SPG activities. Updated Grid Site Operations Policy is now in external consultation phase, while HEPiX Policy on Virtual Machine Image Endorsement Policy draft is now well under way; internal draft will be complete until next week. Whom to consult in policy discussion and consultation? It would be useful to create one integral mailing list, so called list of list on which we can send policy drafts for consultation.

SN: TCB, UCB and OMB mailing lists are primary communication channels for different areas. I have circulated the draft to EB; their role is more procedural than technical. DK: It would be good to consult as much interested parties as we can. Define the distribution mechanism for sending policy drafts and define what mailing lists that should be included in consultation; discuss the proposal in Lyon ***(action 03/01).***

TF: Is there a distinction between the infrastructure and any Resource Centre? DK: Difference is primarily that infrastructure is management thing of whole, collective club of a whole, not each RC. TF: In glossary no infrastructure was defined, only the term IT infrastructure; if we use IT definition for IT infrastructure, few statements from the Grid Site Operations Policy draft don’t seem to be correct and they are not clear. Revisit the glossary and define the term Infrastructure ***(action 03/02).***

## SVG Report

LC presented the SVG report. There is a new version of Issue handling document, i.e. revised after 1 year. No major changes to the process, main changes to the document are clarification of types of software, and how they are handled,

Vulnerability Assessments by UAB continuing. They still hadn’t issue the public and official report but informally I can say they didn’t find any vulnerabilities.

For the EGI TF, two SVG sessions are planned; one will be open session where the work of SVG will be presented, other session will be SVG F2F meeting.

## EUGridPMA IGTF report

DG: Next meeting of the EUGridPMA IGTF will be in the middle of September. Release 1.40 went relatively smoothly and the report was sent earlier to TF and MD.

TF: For release 1.40 there is still combining scenario, nothing has to be changed? DG: New probes are available, they don’t require changes, reliability of NAGIOS and CA packages TF: Do we still have a mixture configuration? DG: Yes. MD: Development of the probes and provision of CAs have to be co-scheduled and it always challenging. DG: With the new NAGIOS probes that will not be the case. MD: What about availability of the sites? DG: It will go up, better availability and synchronization. For the last 2 months probes were running TF: I think we should leave August as it is and in September have a talk with DG

DG: Today I will have an EGI-TERENA-IGTF meeting with Gergely Sipos in order to discuss how to improve TERENA services for EGI users.

## CSIRT with other Grids

SN: There is a need to discuss relationship between EGI and WLCG. There is confusion about the escalation procedure and role of WLCG officer in it.

MM: If there is security incident then EGI CSIRT has to deal with it. Is there better way for CSIRT to have vulnerabilities visible? SN: Both TF and myself are members of Management Board of WLCG, so it is visible for us. If it is done through informal channels, than it is hard to make it visible. Recent incident that took place at Canadian sites is a non-European; I would expect that CSIRT take a lead in collaboration of WSLCG for incidents happening within EGI. TF: One of the main reasons why we are signing MOU with external RiP is because the security is on the top of the list. If there is security breach we have established list of contacts. In the case of Canada, I don’t see them different than any other European country, they follow all procedures and by all means they are part of the infrastructure.

DK: What is happening with MoU between WLCG and EGI? SN: Still waiting for WLCG response, however the MoU is focusing on user communities rather than on resource provider aspect. WLCG close relationship with some of the sites, might make passing EGI a reasonable thing. DK: I think we should be aware if something is happening.

MM: Just take for example Canadian sites, at the moment Canadians are not sure how EGI come to play, but we have authority to ask them to provide them information. That’s the reason we should have a clear scope for CSIRT, we must have authority to ask for information, and they must provide us with necessary information, no matter whether they like it or not. External RiP MoU should make it clear what is relationship between sites covered by MoU ***(action 03/03).***

To put in place MoU between EGI and Canadian sites in order to clearly define our relationship ***(action 03/04).*** TF: In MoU for external RiPs, it is clearly written that sites have to be certified and have to be follow EGI procedures.

SN: Canada does have nationwide grid activity, there is a cross country federation called Compute Canada. I have some contacts within Compute Canada. I will try to get in touch Compute Canada CSIRT ***(action 03/05).***

DK: I saw that EGEE OSCT is listed as a member of TERENA? MM: EGI CSIRT should be there, it will replace EGI OSCT. Prior to EGI, EGEE OSCT was listed as a trusted CSIRT team. EGI CSIRT is getting in touch with TERENA to get it updated so that EGI CSIRT will be listed as a trusted CSIRT team on the website. Other two levels of trust are Accredited and certified, which are paid services. At the moment we don’t have any major problems with Canadians, we have a good working relationship, even though some of the info we asked is missing. SN: I would like to see prioritisation and focus of CSIRT resources to NGIs first.

## D4.4 discussions

SN read the full description of delivery D4.4 Security Risk Assessment of the EGI infrastructure. What was done in EGEE? LC: The previous EGEE "Overall Grid Security Risk Assessment", could be a starting point, although people were a bit weary at the end of EGEE and participation was limited, the list of threats is not a bad starting point. This is not something that is just a matter of sitting down and writing. It is something that requires more work and it involves getting a team together, considering what security threats there are and how we assess them. There are more general risks listed, there needs to be some sort of plan of action for how to deal with the most serious threats. There is a lot of work ahead of us if we want to do a good job. It will require lot of consultation, and participation of the SVG people; we need also to consult experts from other areas.

DK: What do we mean by vulnerabilities – risk or software vulnerabilities? I assume we are talking about new risks we come with by moving to virtualisation; so it is risk assessment. SN: I would prefer focusing on higher level, than on lower level technology things. Yes, it includes, virtualisation and what implication does it have. DK: It is important to agree on the scope – high level risks. SN: SPG, SVG and CSIRT do their job regardless of technology snapshot of current risk. There is also defined process how to deal with them. TF: OMB wiki page provides overview of existing procedures including security ones. DK: We need EGI risk database. Who should own it? SVG should own it and maintaining it on regular bases. SN: PM 19 is end of the November so we need mature draft at the beginning of the November. Linda agreed to draft ToC until end of August ***(action 03/06).***

DK: WLCG is also working on security risk assessment. Maybe we could share resources since we are working on the similar list of high-level risks. SN: Agreed.

## AOB

There were no additional points raised.

# Actions

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Resp. | Description | Status[[2]](#footnote-2) |
| 01/02 | LC | To prepare a poster for the User Forum explaining the responsibilities for the various security policy groups within EGI | CLOSED |
| 02/01 | SN | Find out whether it is possible to have IPG meeting in Tapei, Taiwan | CLOSED |
| 02/02 | JW | Circulate to the SCG list EMI faults on common security libraries | OPEN |
| 02/03 | SN | Establish link with other software providers for the middleware security group | CLOSED |
| 03/01 | PDT, SN | Define the distribution mechanism for sending policy drafts and define what mailing lists that should be included in consultation; discuss the proposal in Lyon | NEW |
| 03/02 | DK, TF | Revisit the glossary and define the term Infrastructure | NEW |
| 03/03 | MM, TF | External RiP MoU should make it clear what is relationship between sites covered by MoU | NEW |
| 03/04 | TF | To put in place MoU between EGI and Canadian sites in order to clearly define our relationship | NEW |
| 03/05 | SN | Contact Compute Canada CSIRT | NEW |
| 03/06 | LC | Draft D4.4 ToC until end of August | NEW |
| 03/07 | SN | Schedule SCG meeting in early September before TF in Lyon | NEW |

# Date for Next Meeting

There being no further business, the meeting concluded at 12:00.

Schedule SCG meeting in early September before TF in Lyon ***(action 03/07).***

Minutes prepared by Damir Marinovic 03.08.2011.

Minutes Approved Group Chair Steven Newhouse

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

COPYRIGHT NOTICE

Copyright © EGI.eu. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/3.0/ or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

The work must be attributed by attaching the following reference to the copied elements: “Copyright © EGI.eu (www.egi.eu). Using this document in a way and/or for purposes not foreseen in the license, requires the prior written permission of the copyright holders. The information contained in this document represents the views of the copyright holders as of the date such views are published.

# Report from SPG

1) Several meetings have been held to make progress on current work:  
<https://wiki.egi.eu/wiki/SPG:Meetings>  
  
2) Updated Grid Site Operations Policy now in external consultation phase.  
New document called Service Operations Security Policy.  
<https://wiki.egi.eu/wiki/SPG:Drafts:Operations_Policy>  
<https://documents.egi.eu/document/669>  
  
3) Extended version of HEPiX Policy on Virtual Machine Image Endorsement now well under way.  
  
New document called Policy on the Endorsement and Operation of Virtual Machine Images  
<https://wiki.egi.eu/wiki/SPG:Drafts:Virtualisation_Policy>  
  
Internal draft due for completion next week.  
  
4) Work continues on the Security for Collaborating Infrastructures (SCI) security policy standards activity.  
e.g. <http://indico.cern.ch/conferenceDisplay.py?confId=140660>  
  
We are planning a face to face meeting in the USA in the Autumn.  
  
5) I attended (as did several others) the Federated Identity Workshop at CERN in June.  
<http://indico.cern.ch/conferenceDisplay.py?confId=129364>

# Report from SVG

Started having monthly EVO meetings - as we stated we would in the TOR.New version of Issue handling document, i.e. revised after 1 year. No major changes to the process, main changes to the document are:\* Clarification of types of software, and how they are handled\* Include specific SVG wiki, lists to send advisories to, which were not firmed up a year ago.\* Some notes and exceptions e.g. - For issues where other projects vulnerable - advisories not placed on web but just distributed within EGI as 'GREEN' - operational actions to mitigate.Issue handling: (Approx)13 new issues in last 5 months or so - since approx last meeting.7 advisories issued by SVG (1 critical, 2 High, 2 moderate, 2 Low)2 CSIRT advisories concerning issues reported to SVG.Vulnerability Assessments by UAB continuing - ARGUS assessed - report pending.2 SVG sessions planned for EGI TF:1 - open session - presentation on work1 - F2F

# Report from CSIRT

The following CSIRT report covers last 3 months CSIRT activities:  
  
- A cross EGI security service challenge (SSC5) has completed. In total 40 EGI sites participated. The final report will be made available at EGI TF

- MS412 - Operational Security Procedures is under external review. This is an overview of all currently approved operational procedures

- EGI CSIRT ToR has been approved

- CSIRT is updating the incident handling procedure, after more than a year of experience. Some clarification will be made, no major change.

- Security dashboard development is on track, plan to make it available to sites and NGIs by the end of this year. This will help bring non-critical security operation in line with normal operation

- 6 hours security training has been scheduled at EGI TF, most training topics and presenters have been finalized

- CSIRT will have a face to face meeting at EGI TF

# Report from EUGridPMA IGTF

- Release 1.40 went relatively smoothly (following a failure of 1.39). The report was sent earlier to Tiziana and Michel (see below)

- New developments in credential-managing and generating portals discussion is scheduled for Marrakech meeting

- Lots of new CAs will become accredited from the EUMedGrid Support project - HIAST already made it, DZ-eScience, JUnet, UAE Ankabut in progress, .eg scheduled

- Next release 1.41 due end of September (last Monday of the month)

1. Member, Observer, in Attendance [↑](#footnote-ref-1)
2. NEW, OPEN, CLOSED, REJECTED [↑](#footnote-ref-2)