**OSG Year6 Security Area Work Plan**

# Strategy

OSG Security team’s main objective is to maintain operational security, which enables the computing and the science results on the OSG. In year6, we will shift some of our focus to key issues in identity management area. Improvements in this area will help our operational security as well as usability of OSG. We will also keep our focus on operational security items such as incident response, vulnerability assessment, security policies, and tools. Our strategy is that when operational emergencies arise, we will quickly shift effort and tend to these issues so that we won’t sacrifice operational security for improvements in other areas. Whereas, at routine work hours, we will focus on our planned project activities as described in Section 4.1. It will be a balancing act between operational needs and planned projects; we plan to have a close collaboration with OSG project management and executive team to achieve this.

# Requirements

This functional area gets its requirements from OSG stakeholders and users, OSG management, and OSG staff.

# Tactics and Changes in our Methods

There are two important changes from prior practice that we propose to implement in year6 in how we perform this function:

1. Based on our findings from Year5, we will lessen the time we devote to security test and controls. We will increase the frequency of some controls (from 6 months to a year or two years) which will help us greatly saving some time. We will most focus on the controls that are identified as problematic in Year5. Controls that we consistently rank high will have a lesser frequency.
2. We will ask Operations teams’ help over processing some of the security tickets when appropriate. Some security tickets have an operational aspect that can be handled by GOC staff. We will explore this during the year.
3. We will record and capture security requests/problems/troubles/etc in OSG ticketing system whenever appropriate. In previous years, we had trouble tracking issues via individual email accounts. Towards the end of year5, we prompted our users to open a GOC ticket as well as emailing the security team members individually. This will not only provide better coordination across the security team members, but also speed up processing a ticket (multiple team members can respond) and allow us to track our overall work items better.

# High-level Goals

## Projects (with Date targets)

1. Finalized Year 6 work plan for Security Area – Aug 30
2. Identity Management
   1. Work Plan agreed by OSG Management and Security team – Sept 30
   2. Set up a testbed to implement and demo various solutions
      1. Integrate OSG RA with Globus Online or TeraGrid Registration portal ; decide which one is more promising – February 30
      2. Create a test setup to integrate a VO with CILogon CA – Feb 30
      3. Create a test instance of Shib Server at FNAL and integrate booth BNL and FNAL IdPs with CILogon CA – August 30
      4. Evaluate the results from testbeds. Determine prototypes worth putting into production – Sept 30, 2013
      5. Implement chosen prototypes and move them into production – June 2013
   3. Conduct Security Controls and Tests
      1. Start executing identified controls – March 2012
      2. Complete the controls assessment – July 2012

## Ongoing Tasks

|  |  |  |
| --- | --- | --- |
|  | Activity | Measure |
| 1 | Incident response and vulnerability assessment | Time spent on closing and responding to incidents; number of tickets |
| 2 | Troubleshooting; processing security tickets including user requests, change requests from stakeholders, technical problems | Time spent on closing and responding to tickets; number of tickets |
| 3 | Supporting OSG RA in processing certificate requests | Time spent on closing and responding to tickets; number of tickets |
| 4 | Preparing CA releases (IGTF), modifying OSG software as the changes in releases require | Number of releases per year and amount of time spent dealing with changes in releases |
| 5 | Security Policy work with IGTF, TAGPMA, JSPG and EGI | To-be-determined |
| 6 | Security Test and Controls | Number of controls completed |
| 7 | Weekly Security Team Meeting to review work items |  |
| 8 | Weekly reporting to OSG-Production |  |
| 9 | Monthly reporting to OSG-ET |  |
| 10 | Quarterly reporting to Area Coordinator meeting |  |

# Staffing Plan

* Mine Altunay – 80% (leadership, oversight, reporting, operations, identity management)
* Anand Padmanabhan – 100% (Operations and software changes necessitated by operational changes)
* TBD 100% (Operations, identity management)
* Jim Basney – 35% (identity management)
* Adam Slagell – 15% (risk assessment)
* Alain Deximo 10% (OSG Registration Authority)

# Risks and Concerns

1. Biggest risk to the work plan is the unforeseen security work such as security incidents, vulnerabilities, high-level trouble tickets, and operational changes. Among operational changes we are most worried about the migration to openSSL 1.0 and its implications over the VDT software. There are yet no OSG sites which has switched to the RHEL6 which includes openssl v6.0 and we do not expect them to switch for another year or so. However, we should do some investigative work in the meantime to understand the impact of the change.