# Security Area Work Plan for the First Year of the OSG N5Y

## New Projects:

1. **Enhance site security; do what sites cannot do for themselves.** Provide sites with software tools and/or provided services to improve site Security. The OSG security team will find, produce, integrate, and provide usage guidance on a set of security tools that will enable sites to setup, manage, and monitor their resources security. In the past, we saw that sites have a big challenge discovering compromises and vulnerabilities. Following services or tools can be provided by the security: vulnerability scanner (Pakiti); remote port scanning service; tools to setup and monitor clusters; documentation and sample configuration documents for existing available tools; working with sites and software team on how to deliver and apply security updates in an efficient way.

Because this project has a very broad scope, we decided to take a step-by-step approach: we first select one sub-project (tool or service) and once we complete the sub-project, we will continue with new sub-projects all year long. We decided to start with Pakiti project. We will provide Pakiti as an rpm and help sites install and configure it as a local service. This means sites can scan their local clusters completely internally and discover vulnerabilities.

1. **Identity Management**
   1. **10% of non-LHC Users access OSG services using campus identities.** The biggest challenge ahead of this goal is to have the OSG sites agree to accept campus identity providers. Currently, there are no campus identity providers that carry an accreditation such as IGTF that OSG sites are familiar with. This causes additional difficulty and anxiety for the sites to accept campus identities. The security team will prepare a risk assessment of using campus identities, help OSG sites discuss the risks, when possible mitigate the risks, and if accepted, help sites accept the campus identities. CILogon CA service provides the mechanisms to convert campus identities into X.509 certificates. Initially, we will use CILogon CA to enable users to access grid resources with their campus ids. Therefore, we will include CILogon CA in the campus identities risk assessment. We will present the risk assessment at BNL, Indiana Univ, and other Tier2 university sites. This will allow the security team to understand OSG Members’ concerns and address them. This will also help accelerate smaller site’s (e.g. Tier2 and 3) acceptance of campus identities.
   2. **Complete the architecture and design of the new set of ID management services.**

We will architect and design the new ID management services that will keep up with stakeholder demands. In the first phase, we will design the services and changes necessary in OSG infrastructure to fully integrate campus identities (CILogon CA) with grid resources. In the second phase, we will architect ID services necessary to integrate campus identities (SAML) with non-grid resources such as web applications, twikis, docdb, and so on. In the third phase, we will architect the integration of identities across other collaborative computing projects such as XSEDE and EGI. This phase will design ID services that will allow users to utilize resources across different projects without gaining new identities.

## Ongoing Operational Work:

1. Incident response and vulnerability assessment
2. Troubleshooting; processing security tickets including user requests, change requests from stakeholders, and technical problems
3. XSEDE Operational Security Interface
4. Maintaining security scripts
5. Supporting OSG RA in processing certificate requests
6. Preparing CA releases (IGTF), modifying OSG software as the changes in releases require
7. Security Policy work with IGTF, TAGPMA, JSPG and EGI
8. Weekly meetings: security team meeting, production, area coordinators

## Metrics

1. Initial acknowledgement/response time to an incident, separated based on incident severity.
2. Initial acknowledgment/response time for high-level operational tickets assigned to the security team.
3. Time spent on security software maintenance tickets.
4. Number of CA bundle releases