

2005 Cyber-Security Summit Report

NSF Response

3.1.1 Issues and recommendations

In addition to the proposed language change, the group noted several issues about the requirement that needed to be clarified:

- The requirements are simply an extension of the business plan that is currently required of awardees. The initial reaction by many was that the requirements were an entirely new set of hurdles to overcome, but NSF program managers pointed out that a business plan is already a requirement, and these requirements would be treated in the same manner.
- The requirements are for Large Facilities and FFRDCs only, not for all NSF awardees
- The goal of the requirements are to goal is to engage the program manager in a dialogue with the PI, awardee, research office, and local organization security in order to put together a security program that is satisfactory.
- There was wide concern that they are not guidelines, but mandated set of requirements or checklist for compliance. The proposed language changes are intended to reflect this concern. Some issues that still need to be addressed:
 - How is the NSF to communicate back to awardee on guidelines and program requirements? Possible suggestions were outreach to PIs and contract offices.

Response: NSF is addressing these recommendations in this 2007 Summit. These recommendations heavily influenced the language that is now included in Cooperative Agreements.

- How should sites manage notification of security incidents back to NSF? There was consensus that not all incidents should require notification, in which case, some guidelines need to be provided which give thresholds for notification.

Suggested thresholds suggested were:

- When business continuity is affected or potentially affected
- Potential impact on community as a whole
- Likelihood of bad PR and political/reputation ramifications

Response: The NSF Large Facilities Security Working Group has discussed these topics and they are in agreement with the first two sub bullets. The group feels that the site cyber-security plan should address how the latter should be handled.

- There was also some concern about the confidentiality of information that is reported to the NSF. Many sites have legal confidentiality requirements, in addition to institutional privacy policies. It is not clear whether information provided to NSF becomes public information, or whether it is subject to FOIA requests. This issue should be clarified by NSF so that sites can properly comply with all requirements.

Response: The NSF Large Facilities Security Working Group is discussing and reviewing this and seeking input internally at NSF. Recommendations will be forthcoming.

3.2.3 Fundamental Recommendations

There are many approaches to increasing (or attempting to increase) the awareness about security issues. They are being discussed and addressed in a variety of other venues and activities. However, for the particular base community being addressed – scientists and researchers – the discussion seemed to come back to a set of approaches that might be the most effective;

- Ensure that applicable aspects of security are considered at the institutional level
 - In the deliberations and considerations of Institutional Review Boards and Human Subjects Committees and Research Compliance Committees
 - In employee job descriptions
 - In faculty, staff, and student orientation sessions
 - Along with other already-required compliance training

Response: This should be reflected in the cyber-security plan submitted to NSF from the awardee's institution/organization.

- Find and engage external organizations that have influence over and/or the respect of the research community:
 - Higher education Presidential associations
 - Professional organizations
 - Academies
 - Accreditation boards
 - NSF and other funding agencies
- Promote and leverage existing educational opportunities (listed above).

Response: NSF agrees with these two recommendations. We will be looking to knowledgeable organizations for assistance and coordination in this effort.

- Encourage NSF to be more aggressive in providing security awareness assistance (e.g., Guidelines for IT Security of NSF's Large Facilities).

Response: Draft Guidelines for IT Security of NSF's Large Facilities are currently being reviewed internally at NSF.

- Encourage institutions to include technology support (IT Security) in grant proposals, especially graduate students (future researchers).

Response: Noted. Awardees are encouraged to leverage the policies and practices already available to them at their institutions.

3.3.3. Key issues and recommendations

Realizing that *no one recommendation is going to be the silver bullet for site security*, a defense in depth, or layered security approach needs to be taken. Sites have to balance the limited monetary resources they have, along with their personnel resources, to choose what security measures can/should be applied. Because of the diversity of sites, even within the 20+ organizations represented, it was recognized that each individual site needs to evaluate what security measures are best for them. Sites with a strong control of host end systems may be able to focus on HIDS, whereas other sites may have to take a more network centric approach with NIDS or flow analysis. For each site it is very important to "Know thy network".

Regardless of the approach, the following items can be investigated. Keep in mind when reading these recommendations that sites are different with different needs. Most sites are not going to be able to do every one of these, so will have to choose which ones they are able to deploy.

- Intrusion detection systems were determined to be very useful, and sites not deploying them should evaluate utilizing them.
 - Flow tools are useful as a complement to an intrusion detection system and sites should start collecting and analyzing flows.
 - Syslog data is useful as a host intrusion detection system and sites should set up a centralized syslog server.
 - Data correlation from different sensors is proving to be a valuable tool (such as syslog and IDS data). There are a couple tools mentioned in the appendix that are worth looking into.
 - Sites need to have an Incident Response plan and procedure in place. This includes knowing ahead of time who is involved on the incident response team.
 - Sites should have an out of band communication method (i.e. encrypted email, Jabber servers) which was found very useful in incident response.
 - Sites need to know requirements and laws they fall under. Reporting needs, data collection procedures, legal aspects
 - Sites need to know their researchers and resources.
- Assists in incident response and prevents incidents.

Response: This recommendation is directed to the awardees. NSF concurs that these are best practices.

3.4.4 Recommendations

1. **User Awareness and Education.** Consistent with most areas of cybersecurity, the effort to keep owners and users of data aware of the threats, and methods to mitigate the threats, must be maintained and increased. Communication between major data centers to discuss, develop and update best practices should be encouraged.

Recommendation: Centers should publish minimum user best practices for data security and integrity, and encourage adherence to best practices.

Response: The TeraGrid is identified as a “best practice” in this area.

2. **Collaboration.** Opportunities for detailed discussions of how to determine user requirements (user survey?), how to find the balance between security and usability, and how to implement

measures to assure data security and integrity, should be sought. **Recommendation:** Organize a workshop(s) specific to data security and integrity, perhaps with NSF sponsorship.

Response: This is best addressed within the awardee community. The 2007 Summit partially meets this recommendation.

3. Data Security Service. One of the primary unanswered questions within this breakout dealt with determining and alerting users, by monitoring in an automated fashion (enterprise level), if data has been destroyed or modified. Services could be offered which enhance the level of security required by the user, at the discretion of the user – such as duplication, replication, access control, change detection, encryption, metadata security tracking, etc. Because of varying user needs, a method to categorize the level of security should be developed.

Recommendation: Explore the demand/difficulty in creation/enhancement of enterprise data security service.

Response: While this does not appear to be a recommendation directly pertinent to NSF, NSF agrees that it may be able to facilitate further discussion of this recommendation. It will be discussed further in the NSF Large Facilities Security Working Group.

4. Conclusions and Final Recommendations

The NSF sponsored 2005 Cybersecurity Summit was a valuable follow on to the 2004 Cybersecurity Summit. It continued the important work of raising security awareness for participating NSF sponsored sites and provided a valuable resource for security discussion and recommendations to the NSF and summit attendees. Results of the 2004 Cybersecurity Summit can already be seen in the attention to security issues in NSF program reviews that have occurred in January 2006. The committee believes the Cybersecurity Summit has and can continue to be a valuable resource to the NSF to provide a forum for security discussions and recommendations of particular interest to the NSF and the NSF community related to security issues surrounding NSF proposals, programs and projects. In addition to the recommendations spelled out in the breakout session sections above, the 2005 Cybersecurity Summit program committee recommends that NSF consider sponsoring a 2006 Cybersecurity Summit. A 2006 Cybersecurity Summit could be used to continue to raise security awareness for NSF sponsored program staff, point out existing work to the community that has solved a previously identified security problem set and/or NSF could identify a set of security issues of interest to be discussed and addressed at the next summit.

Response: The 2007 Summit is in response to this recommendation.