DRAFT

NIST Security Working Group (WG) Agenda

May 4, 2011

Time: 2:00pm ET
Duration: 1 hour.
USA Toll Free Number: 866-819-5964
Passcode: 5576521

The purpose of this meeting is to discuss the feedback we have received so far, and some potential tasks that NIST has identified. The feedback is summarized below, and can be found with attribution at: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity/2011-04-20_Feedback_on_Rebooting.doc.

Feedback
Coordinate and work with CSA, FedRAMP and NIST 800-53.
What is our deliverable?
Cloud Security Profiles for Federal Industry (for a certain set of best practices)
Analyzing Security Issues in each Cloud Layer for strategic (fixed) and tactical (deployed) environments.
establish a decision-making risk catalog for considering risks (look at ENISA risk assessment)
(Question): what is delivered from this group – will it help to bridge the way for the federal agencies that have security concerns about moving their three apps to the cloud in 18 months?
encompassing portable (which I also read as mobile) environments is important.
As a developer for 800-53, a CSA long time member, I would like to build urgency because our calendar is way before the end of the fiscal year.
FIPS 200 has a brief statement for the 17 security related areas and requires selection of controls based on the SP 800-53 baselines.
1. we have an option to dig deeper technologically in terms of standards that enter into the NIST primary charge of portability, interoperability and security for cloud-based IT. **2.** Security at scale and for portable environments has got to be a focus. **3.** being able to identify each and every user - at least for non- automated processes. Who is allowed to initiate the backup of all files from your workstation or portable device to the federal cloud, for example, or to some service contracted by the government?

Additionally, the following are possible activities:

1. Rewrite charter, FYI, NIST will do this.
2. Relate the group's activity to the top 20 security concerns.
3. Write a security section for each of the business use cases from the Business Use Case WG.
4. Write a security section for the reference arch document from the Reference Architecture WG.
5. Inventory of security standards related to cloud computing.
6. Perform a security analysis of selected cloud standards: OCCI, CDMI, OVF.

7. Generate a prioritized list of documents that security/cloud folks should read (or know about).
8. Stray thought: create an inventory of existing guest operating system hardening guidelines that seem to apply in a virtualized setting. Collect as guidance for IaaS cloud providers/subscribers.

The meeting information will be available at: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity.

The conference call will use the web conf tool at: http://webconf.soaphub.org/conf/room/cc_security

Disclaimer: Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.