

## **NIST Cloud Computing Security Workgroup (NCC-SWG) Meeting Minutes**

Time: 06/15/2011 2:00-3:00 PM EST

Online at [http://webconf.soaphub.org/conf/room/cc\\_security](http://webconf.soaphub.org/conf/room/cc_security)

NCC-SWG's TWIKI page is at <http://collaborate.nist.gov/twiki-cloudcomputing/bin/view/CloudComputing/CloudSecurity>

### **General discussion:**

There was a question raised if the goal of WG changed (from a person who has not attended the meetings for a while). The answer is yes. The redefined goal is stated in the agenda, the impediment list document, and in the charter on Twiki site.

There was a question raised about the goal of FedRAMP. The answer is to seek feedback from NIST staff more involved in that effort. Based on already published FedRAMP documents, control list similar to 800-53 is not very helpful. Filling in the gaps and making it more actionable could be what should be done. WG members involved in R3 and R4 can provide pointers to the appropriate works.

### **Impediment specific:**

Picked up from where we left in the last meeting...

#### **3.7 Need to assess Trustworthiness of Cloud Operators**

There was a general agreement about the scope. Carlo Espiritu volunteered to provide comments for this impediment.

#### **3.8 Business continuity and disaster recovery**

A question was raised that NIST/FedRAMP might have covered this. Provide pointers to Guidelines for Secure Use of Cloud Computing by Federal Departments and Agencies (if published), Contingency Planning and to 800-144, Section 4.8 Availability.

#### **4.1 Lack of visibility for customers**

#### **4.2 Lack of control for customers**

These two impediments were discussed together since they were related and very important for cloud computing adoption. There was an emphasis on preventive controls over passive monitoring and auditing. Ulrich Lang volunteered to provide comments on both impediments.

#### **4.3 Limited Data Protection**

There was discussion about the name confusion that in many countries data protection relates specifically to PII. Consensus was that data protection was broader than PII. It is suggested to use Data Security. But the agreement was to wait until content was provided. Then the right name might bubble up. Michael Berman and Nadeem Bukhari volunteered to provide comments for this impediment.

#### **4.4 Risk of Account Hijack**

No comments.

#### **4.5 Identity Authentication and Management (IAM) not Deployed**

Has SAJACC covered this? The answer is that SAJACC is detailed. Here, it should be discussed broadly. Most WG members didn't like the name and suggested Identity Access and Management (IAM) and Authorization or something similar.

#### **4.6 Risk from Multi-tenancy**

No comments.

#### **4.7 Risk of Network Based Denial of Service (new)**

Concern was raised about the scope. If cloud related, it is in scope. If network infrastructure related, it is out of scope. It was advised to refer to Cloud Computing Reference Architecture, where the cloud carrier role is defined. Bill Butler and Mike Nelson volunteered to provide comments for this impediment.

Don brought up some topic as potential impediment candidates:

- Trust relationships between clouds
- Lack of Threat Taxonomy for Cloud

Don also proposed to add records retention in 3.2.