

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

Time: 05/18/2011 2:00-3:00 PM EST

Online at http://webconf.soaphub.org/conf/room/cc_security

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

Threads of discussions

1. Discuss and contribute to the new formulation of the deliverables, which is based on the feedback received.
 - Goal: Mitigate security impediments that may prevent adoption of cloud computing by Federal agencies.
 - Main Deliverable: A document, the "Security Impediments and Mitigations List". The document will contain a prioritized list of security impediments and. For each impediment, either a pointer to work that mitigates the impediment, or a description of approaches for mitigation.
 - a) This document will be the primary contribution to the roadmap.
 - b) Take a more strategic approach to address these concerns.
 - Other Deliverables: Security sections for the Reference Architecture document, the Business Use Cases, and the Standards WG roadmap document.
 - Deadlines for the deliverables.
 - a) First Draft: June 15th, 2011
 - b) Subsequent versions approximately every 2 weeks as appropriate
 - c) Final Draft: September 30th, 2011
 - Security Impediments and Mitigations List.
 - a. Review the feedback from the WG's mail list and address the issues rose to the impediments.
 - b. Split the impediments into two sections: Process Oriented and Focused Technical.
 - c. Some pointers are provided for the impediments. Feedbacks and contributions are welcomed from the participants for identifying more impediments and mitigations.
 - d. Suggestions and Questions.

- Some impediments need to be more clearly defined or narrowed down. Such as data protection from what?
- What is 3rd party auditing? An independent third party organization with certificated skills and motivation to provide assessment report based on standards controls like 800-53.
- Possible additional controls to NIST 800-53 for areas like virtualization and hypervisor, etc.
- Avoid re-inventing wheels. Our WG is collaborating and aligning with others groups, such as FedRAMP, etc.
- How to define Continuous Monitoring? Does it include the automated data-feeds into CyberScope? NIST has not finalized the definition of “Continuous Monitoring”.
- How is this document affecting the private Cloud providers, whom has data center outside the country? Compliance and requirements.
- More advanced draft.
- 800-53 Revision 4.
- Anything in the document to reflect the contractual difficult? NIST does not provide advice on the formation of the contracts.

-

Action Items

- Send feedbacks to the work group.
- Working on more structural draft and send out to the group.