

DRAFT

Cloud Computing Security Impediments and Mitigations List

v04

June 13, 2011

Table of Contents

1. Overview ..... 1
2. <impediment-name> (as short as possible while being descriptive) ..... 2
3. Process Oriented ..... 3
3.1 Confusion about Application of 800-53-style Controls, and Compliance ..... 3
3.2 Lack of Cloud Audit Assurance and Log Sensitivity Management..... 3
3.3 Need Clear Certification and Accreditation Guidelines ..... 4
3.4 Need Clear E-discovery Guidelines ..... 4
3.5 Need Clear Privacy Guidelines..... 4
3.6 Need Clarity on Security Control Roles and Responsibilities..... 5
3.7 Need to Assess Trustworthiness of Cloud Operators ..... 5
3.8 Business continuity and disaster recovery..... 5
4. Focused Technical..... 6
4.1 Lack of visibility for customers ..... 6
4.2 Lack of control for customers ..... 6
4.3 Limited Data Protection..... 6
4.4 Risk of Account Hijack ..... 6
4.5 Identity Authentication and Management (IAM) not Deployed ..... 7
4.6 Risk from Multi-tenancy ..... 8
4.7 Risk of Network Based Denial of Service (new) ..... 9
5. References ..... 10

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.

1. Overview

This working document records a list of security issues that appear to be obstacles to the adoption of cloud computing by Federal agencies, and possible mitigations. The issues listed here have been added by members of the NIST security working group, or by NIST, and do not necessarily represent consensus by the group. The working group's charter and meeting notes can be found at: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity.<sup>1</sup>

Goal of the Security Working Group: Mitigate security impediments that may prevent adoption of cloud computing by Federal agencies.

<sup>1</sup> The online charter is being updated for consistency with this document.

# DRAFT

**Main Deliverable of the Security Working Group:** A mature version of this working document, the "Cloud Computing Security Impediments and Mitigations List". The working group and NIST will expand this document to 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.

## Schedule:

June 15, 2011 - first draft
subsequent versions approximately every 2 weeks as appropriate
Sep. 30, 2011 - final draft

**Approach:** The WG nominates impediments and mitigations as necessary, critiques existing impediments and mitigations, and provides rationale for each. NIST maintains and guides the writing of the impediments list. The next section provides a **template** for expressing an impediment and its associated mitigations. The purpose of this template is to help communicate impediments and related mitigations quickly without a lot of effort on the format itself, but with enough structure to remind authors of key aspects. Draft or incomplete impediment sections are expected: this is a working document.

Subsequent sections document security impediments that have been captured from feedback on the cc\_security@nist.gov email list and through discussions with the working group. They are divided into two groups: process oriented and focused technical.

## 2. <impediment-name> (*as short as possible while being descriptive*)

**Description:** *A paragraph-sized (or less) description of the impediment.*

**Importance:** *A sentence or paragraph-sized rationale for why we should care: why does this impediment matter?*

**Solution Maturity:** *An informal English-language summary of how close current techniques are to mitigating the impediment, and an estimate of how feasible mitigation is in the 12-month timeframe.*

### Mitigation 1: <mitigation-name>

*Text here should describe a mitigation of the impediment and how sufficient the mitigation is. The first part should take one of two forms:*

- 1. The text can be an English-language narrative of how to mitigate the impediment. This narrative might be similar in form to the text in a success scenario for a NIST SAJACC technical use case. E.g., see: <http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/UseCaseOpenAccount> .*

**OR**

- 2. The text can be a short synopsis of what others have done for this mitigation (perhaps a paragraph), along with a URL pointing to their public work. If the document identified is large, the text should include some navigation information, like page numbers or section names to help the reader quickly find the relevant material.*

**Sufficiency Comment:** *Informally characterize the effectiveness of this mitigation, and whether it depends on any other mitigations.*

### Mitigation 2: ...

# DRAFT

...

**Mitigation *n*:** ...

**Active WG Members:** *Names of WG members who are helping with this impediment and who wish to be identified.*

**References:** *We anticipate that different mitigations will share references, so this field will ultimately exist at the end of the document in its own section but may initially exist per-section.*

## 3. Process Oriented

The process-oriented issues rely on human-centered processes, procedures, and guidance for mitigation.

### 3.1 Confusion about Application of 800-53-style Controls, and Compliance

**Description:** Need for clarity on how 800-53-style control guides can work for the cloud.

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** FedRAMP

A list of security controls for a cloud system, with details similar to 800-53...

**Sufficiency Comment:** TBD.

**Active WG Members:** Ken Stavinoha, Michael Berman, othersTBD.

**References:** TBD, but clearly including the FedRAMP document URLs.

### 3.2 Lack of Cloud Audit Assurance and Log Sensitivity Management

**Description:** How to gain assurance that:

1. important events are monitored, and
2. sensitive/private audit logs are appropriately protected.

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** risk management framework

The NIST Risk Management Framework (SP800-37) provides guidance to federal system owners to take a risk-based approach to securing systems. This approach is operationally focused and is intended to facilitate the monitoring, documenting, and mitigation of threats on a regular if not near real time basis. Continuous monitoring is step 6 of SP800-37's 6-step risk management framework. While many vendors are seeking to offer automated vulnerability monitoring tools, it is important to realize that there is more to an effective continuous monitoring program than the automated tools. The FedRAMP program's Proposed Security Assessment and Authorization document (<https://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf>) describes an effective continuous monitoring program as one that includes:

- "Configuration management and control processes for information systems;
- Security impact analyses on proposed or actual changes to information systems and environments of operation;
- Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the defined continuous monitoring strategy;
- Security status reporting to appropriate officials; and

## DRAFT

- Active involvement by authorizing officials in the ongoing management of information system-related security risks."

**Sufficiency Comment:** TBD.

**Active WG Members:** Nadeem Bukhari, Fred Whiteside, othersTBD.

**References:**

CSA cloud audit work. Also, CSC has started the "Cloud Trust Protocol."

The FedRAMP document: <https://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf>

### 3.3 Need Clear Certification and Accreditation Guidelines

**Description:** How to certify and accredit cloud solutions with confidence.

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** audits and monitoring

3rd party audits + Continuous Monitoring, ...

**Sufficiency Comment:** TBD.

**Active WG Members:** Lisa Carnahan, othersTBD.

**References:** TBD.

### 3.4 Need Clear E-discovery Guidelines

**Description:** How to provide access to data in response to lawful authority while protecting customer privacy.

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** TBD.

**Sufficiency Comment:** TBD.

**Active WG Members:** Michael Berman, othersTBD.

**References:** TBD.

### 3.5 Need Clear Privacy Guidelines

**Description:** How to build confidence that cloud solutions provide privacy.

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** TBD.

**Sufficiency Comment:** TBD.

**Active WG Members:** Michele Drgon, othersTBD.

**References:** TBD.

## DRAFT

### 3.6 Need Clarity on Security Control Roles and Responsibilities

**Description:** Who (among cloud actors such as customer and provider) should be responsible for the implementation of required security controls listed in section 1.1? It seems that the actor most able to observe and configure specific a portion of a cloud implementation would be in the best place to implement a relevant control.

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** provider-subscriber guidelines.

Write roles and responsibilities definitions or guidelines for cloud provider and consumer/subscriber. Clarity about how responsibility for protection of information remains with a system owner but the terms of a contract between a system owner and a cloud provider can place an obligation on the provider to protect information.

**Sufficiency Comment:** TBD.

**Active WG Members:** Ken Stavinoha, othersTBD.

**References:** TBD.

### 3.7 Need to Assess Trustworthiness of Cloud Operators

**Description:** What is the basis for trusting the human cloud operators?

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** cloud provider human resources practices

Provider staff screening, hiring, training, monitoring, separation of duty, malicious insider.

**Sufficiency Comment:** TBD.

**Active WG Members:** TBD.

**References:** TBD.

### 3.8 Business continuity and disaster recovery

**Description:** How to maintain continuity of operations if cloud providers fail?

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** redundancy and backup

Redundant clouds? Non-cloud backup?

**Sufficiency Comment:** TBD.

**Active WG Members:** TBD.

**References:** TBD.

# DRAFT

## 4. Focused Technical

The focused technical issues are amenable to automated mitigation mechanisms.

### 4.1 Lack of visibility for customers

**Description:** How can customers observe their workloads to be aware of their health and general status?

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** audits and monitoring

TBD. 3rd party audits + Continuous Monitoring?

**Sufficiency Comment:** TBD.

**Active WG Members:** TBD.

**References:** TBD.

### 4.2 Lack of control for customers

**Description:** How can customers maintain effective control their workloads even though the protection mechanisms and even locations of workloads may not be known to customers?

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** audits and monitoring

TBD. 3rd party audits + Continuous Monitoring?

**Sufficiency Comment:** TBD.

**Active WG Members:** TBD.

**References:** TBD.

### 4.3 Limited Data Protection

**Description:** data protection (move in/out of cloud, assured deletion, loss/leakage, location).

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** encryption, etc.

TBD. encrypt data wherever practical; replication; off-cloud backup; disaster recovery.

**Sufficiency Comment:** TBD.

**Active WG Members:** TBD.

**References:** TBD.

### 4.4 Risk of Account Hijack

**Description:** Benefits of cloud computing include its easy accessibility. A customer can use cloud computing services anywhere he/she has Internet access. However, the Internet is full of threats such as phishing, pharming and spyware, whose purpose is to steal usernames and passwords

## DRAFT

(credentials). Facing this Internet security threat environment, customers adopting cloud computing are concerned about how user accounts are protected from hijack to avoid misuse.

**Importance:** Account hijacking is not new, but its potential is heightened in the context of cloud computing because:

- There are uncertainties due to increased complexity and dynamics in the infrastructure.
- There are new APIs/interfaces that are less battle-tested.
- A hijacked account may be used to steal information, manipulate data, and defraud others under the customer's identity.
- A hijacked account may be used to attack other tenants as an insider in the multi-tenancy environment.

**Solution Maturity:** Mitigations such as strong authentication, encrypted credentials, and secure APIs/interfaces have been used to protect user accounts from hijack. But, as pointed out in the Symantec Security Threat Report, the easiest vulnerability for attackers to exploit is our trust of friends and colleagues. Users tend to click the links and attachments in an email they received from a trusted source (perceived or real). Thus, these mitigations should complement proactive monitoring and auditing of unauthorized activities.

**Mitigation 1:** Strong authentication

- Enforce strong password usage and change passwords periodically.
- Use multi-factor authentication.
- Prompt users for their passwords during sessions especially when there are suspicious events.
- Allow logins coming only from a white listed address range.
- Use biometrics.

**Sufficiency Comment:** There is already a password proliferation, resulting in security compromising behavior and increased burden on help desk. Possible alleviations in cloud computing include integration with customers' exiting identity management processes and single sign-on (SSO).

**Mitigation 2:** Encrypted Credentials

- Provide a dedicated VPN.
- Use HTTPS and LDAPS.
- Enable secure cookies.
- Use strong cryptographic PKI keys.

**Sufficiency Comment:** The effectiveness of encrypted credentials depends largely on secure key management.

**Mitigation 3:** Secure APIs/interfaces

- Provide common security models for cloud APIs/interfaces (such as WS\*, WS-I, SAML for web services).
- Protect application security using secure APIs/interfaces (e.g., input validation/escaping/encoding against injection exploits such as SQL injection and cross site scripting).

**Sufficiency Comment:** Cloud APIs/interfaces are still evolving (all the way up to the level of cloud federation).

**Active WG Members:** Shilong Chu.

**References:** [09].

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

**Description:** how to manage identity management for a cloud and access rights.

# DRAFT

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** TBD

TBD.

**Sufficiency Comment:** TBD.

**Active WG Members:** TBD.

**References:** TBD.

## 4.6 Risk from Multi-tenancy

**Description:** Cloud computing provides the potential of cost saving through resource sharing. Different tenants use services on the same cloud simultaneously. As a result, there are warranted security concerns:

1. A tenant may have access to other tenants' virtual machines, network traffic, actual/residual data, etc.
2. A tenant may impact the normal operation of other tenants, steal their data, steal their identities, etc.

**Importance:** Although many network services and programs have simultaneously supported multiple tenants in the past, cloud computing elevates this concern because the resource sharing is pervasive, exposes many possibly-vulnerable interfaces, and potentially occurs at a very large scale. Thus, this is a new challenge and Federal agencies are not familiar with this kind of massive resource sharing and its security ramifications. The uncertainty may impede the adoption of cloud computing. The following mitigations address these concerns by ascertaining application separation and data encryption in cloud computing.

**Solution Maturity:** Physical separation is a mature enough practice even in traditional IT environments. Despite key management limitations, data encryption has been accepted in eCommerce and Federal IT systems. Application partitioning facilitates putting critical components in more secure environments, but its assurance of security needs to be further verified. Logical separation in cloud computing remains a general concern and its maturity will be vendor dependent in the near future. Based on their maturity levels, it is suggested to use physical separation or a combination of data encryption, application partitioning and logical separation (defense in depth) to address the risk of multi-tenancy. All mitigations should complement the identity management and access control best practices.

**Mitigation 1:** Data encryption

- Data in transit: Encrypt data using a one-time session key similar to how SSL/TLS works.
- Data at rest: Selectively encrypt sensitive data using NIST 140-2 validated algorithms.
  - Manage key separately from data with higher privileges and preferably accessible only through procedures/programs.
  - Change key periodically and data unencrypted and re-encrypted with the new key.
  - Compile and/or wrap the encryption procedure/program to hide additional data transformation or padding to make it even harder for a snooper to get the key.

**Sufficiency Comment:** By itself, encryption is not sufficient to mitigate the risks from multi-tenancy. Encrypted data is not as vulnerable to disclosure as plaintext data but is still vulnerable to loss

## DRAFT

and possibly corruption. Key management must be performed correctly and at scale or the cryptography does not provide value. Performance may be affected.

### **Mitigation 2:** Application Partitioning

- Separate access control functionality from business processing functionality.
- Separate logic processing functionality from data access functionality.
- Separate user functionality from system management functionality.
- Aggregate functionalities with similar security requirements to run in the same virtual environment and take advantage of modern compartmentalized data centers (vLANs/sub-network zones with varying levels of security controls).

**Sufficiency Comment:** By itself, localization is not sufficient to mitigate the risks from multi-tenancy but it can localize the reach of security risks and hence reduce risks.

### **Mitigation 3:** Logical separation

- Support holistic logical separation of the resources at all the layers: computing (virtualization), networking (vSwitches and vLANs) and storage (logical separation of files with access controls).
- Secure the virtualization server (hypervisor isolation settings to limit accesses).
- Secure the virtual network by working hand-in-hand with the physical network security, especially man in the middle attacks.
- Harden the Virtual Machine (VM) so that the virtualization layer is not exposed to attack.

**Sufficiency Comment:** If logical separation is faithfully implemented it addresses much of the multi-tenancy impediment. The difficulty is in achieving assurance that an implementation is correct. Still a concern and vendor dependent.

### **Mitigation 4:** Physical separation

- Special virtual environments with physical separation can be provisioned to customers with special security requirements.
- This kind of special virtual environments can be provisioned in a cookie cutter way to respond to increasing demands.

**Sufficiency Comment:** Consider private cloud for even higher demand for separation/isolation.

**Active WG Members:** Shilong Chu, Lee Badger, others TBD.

**References:** [01] through [08] Inserted in section 5.

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

**Description:** Because cloud customers depend on functional networks to access their resources, and because networks are often not under the control of customers, there is a risk that the cloud may not be reachable.

**Importance:** TBD.

**Solution Maturity:** TBD.

**Mitigation 1:** redundant paths to a cloud, private cloud, etc.

TBD.

**Sufficiency Comment:** TBD.

# DRAFT

**Active WG Members:** TBD.

**References:** TBD.

## 5. References

- [01] Draft Cloud Computing Synopsis and Recommendations -  
<http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf>
- [02] Proposed Security Assessment & Authorization for U.S. Government Cloud Computing -  
<http://www.cio.gov/pages.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP>
- [03] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 -  
<https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf>
- [04] Top Threats to Cloud Computing V1.0 -  
<https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>
- [05] SaaS, PaaS, and IaaS: a Security Checklist for Cloud Models -  
<http://www.csoonline.com/article/print/660065>
- [06] Cloud – 10 Risks with Cloud IT Foundation Tier - [https://www.owasp.org/index.php/Cloud-10\\_Risks\\_with\\_Cloud\\_IT\\_Foundation\\_Tier](https://www.owasp.org/index.php/Cloud-10_Risks_with_Cloud_IT_Foundation_Tier)
- [07] Edward L. Haletky, “VMware vSphere and Virtual Infrastructure Security”, Prentice Hall, 2009, ISBN-13: 978-0-137-15800-3.
- [08] Cloud Computing and Security – A Natural Match -  
[http://www.trustedcomputinggroup.org/files/resource\\_files/1F4DEE3D-1A4B-B294-D0AD0742BA449E07/Cloud%20Computing%20and%20Security%20Whitepaper\\_July29.2010.pdf](http://www.trustedcomputinggroup.org/files/resource_files/1F4DEE3D-1A4B-B294-D0AD0742BA449E07/Cloud%20Computing%20and%20Security%20Whitepaper_July29.2010.pdf).
- [09] Symantec Internet Security Threat Report, Trends for 2010, Volume 16, April 2011.