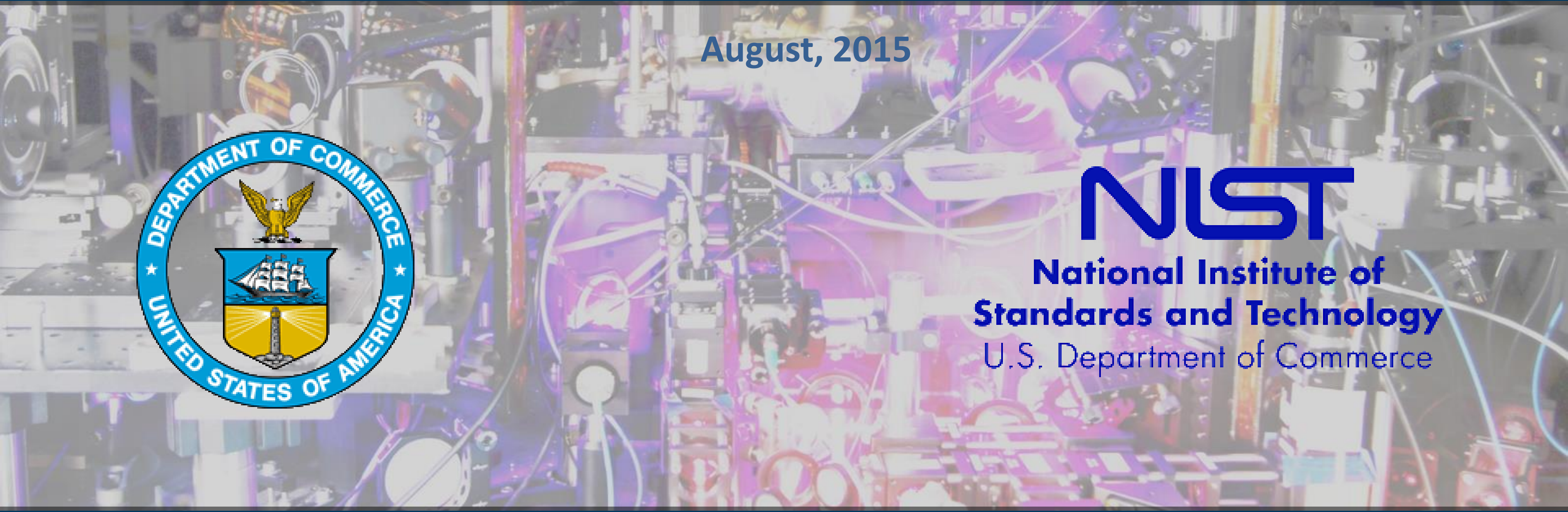
Cloud Assessments

Federal Computer Security Managers' Forum

John Connor, IT Security Specialist, OISM, NIST



August, 2015

National Institute of Standards and Technology
U.S. Department of Commerce

Background Photo - JILA strontium atomic clock (a joint institute of NIST and the University of Colorado Boulder)

National Institute of
Standards and Technology
U.S. Department of Commerce

“Certain commercial vendors are identified in this presentation for example purposes. 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 vendors identified are necessarily the best available for any given purpose.”

This presentation was created by NIST’s Office of the Chief Information Officer for informational purposes only and is not an official NIST publication.

Cloud Questions

Does my CSP use subcontractors ?

800-53, FIPS 199, FIPS 140-2 …

What are OMB requirements?

What is FedRAMP ?

Do I need to assess Social Media ?

What's a 3PAO ?

How do I scope controls ?

But they don't store the data …

My vendor says they are secure …

Who needs to be assessed ?

Are FedRAMP and FISMA the same, different ?

How to handle continuous monitoring ?

PCI / SSAE / HIPPA ?

IN THE NEWS - 2015

LastPass saw potentially millions of passwords accessed

CVS, Walgreens, others hit by credit card breach

Carphone Warehouse, phone store - 90,000 customers had encrypted credit card data stolen.

Anthem lost more than 80 million customer records - including SSN’s

UCLA Health hacked - 4.5 million records, including SSN’s, and medical data

IRS data breach led to hackers taking tax returns

Ashley-Madison - “The last truly secure space on the Internet”

Sony hasn't recovered from the hack yet

2 to look at in more detail…

OPM Breach (2014-2015)

Point 1:

In 2014, the Office of the Inspector General (OIG) urged the Office of Personnel Management (OPM) to shut down computer systems which were operating without a current security authorization. OIG specifically warned the breach of some of the systems could have “national security implications.”

In the audit report published 11/12/14, OIG found that 11 out of 47 computer systems operated by OPM did not have current security authorizations.

OIG recommended OPM, “consider shutting down systems that do not have a current and valid Authorization.” But OPM declined.

Point 2:

OPM didn’t know a breach had occurred until AFTER it had finished an “aggressive effort” in upgrading its cybersecurity systems, due to a previous breach.

What would have happened if they hadn’t made these security upgrades?

Hacking Team (July 2015)

Hacking Team, an Italian company that makes surveillance software used by governments to police the Internet was hacked.

All company information exposed.

Christian Pozzi, senior system and security engineer for the company:

The leaked security engineer's list of passwords:

UserName : Neo
Password : Passw0rd

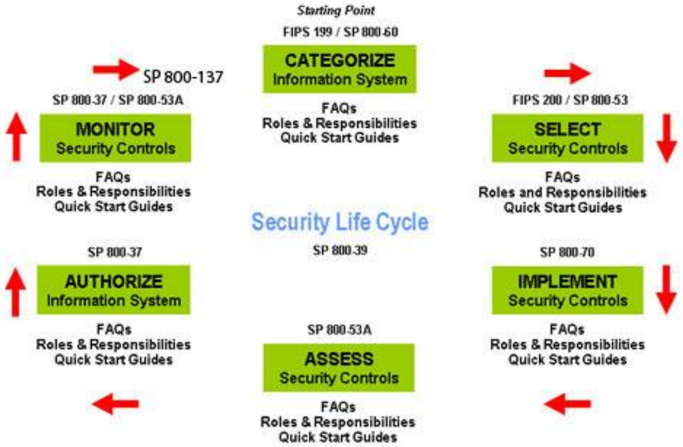
UserName : c.pozzi
Password : P4ssword

All information from various public news reports.

Let’s step back…

FISMA - Risk Management Framework

Assessment & Authorization, a core component of FISMA and implementation of the Risk Management Framework, ensures federal information system cyber security controls are continuously monitored and cyber security control status and risks are well understood by management and technical staff and managed in support of the organizations mission.



My answer:

To give the authorizing officials the knowledge and understanding of a given system so they can make informed decisions on the risks inherent in that system.

The head of each agency shall be responsible for:

> “Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of
>
> > “(i) information collected or maintained by or on behalf of the agency; and
> >
> > “(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Federal Information Security Management Act of 2002 (FISMA) section 3544. Federal agency responsibilities

See OMB Memo M-14-04 November 18, 2013
- Excellent FAQ on all aspects of FISMA, including cloud

What does this have to do with “The Cloud” ?

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

OMB Memo M-14-04 November 18, 2013
#25, 26, 27 & 48 specifically on 3rd part and cloud vendors

See NIST SP-135 for definition of “cloud”

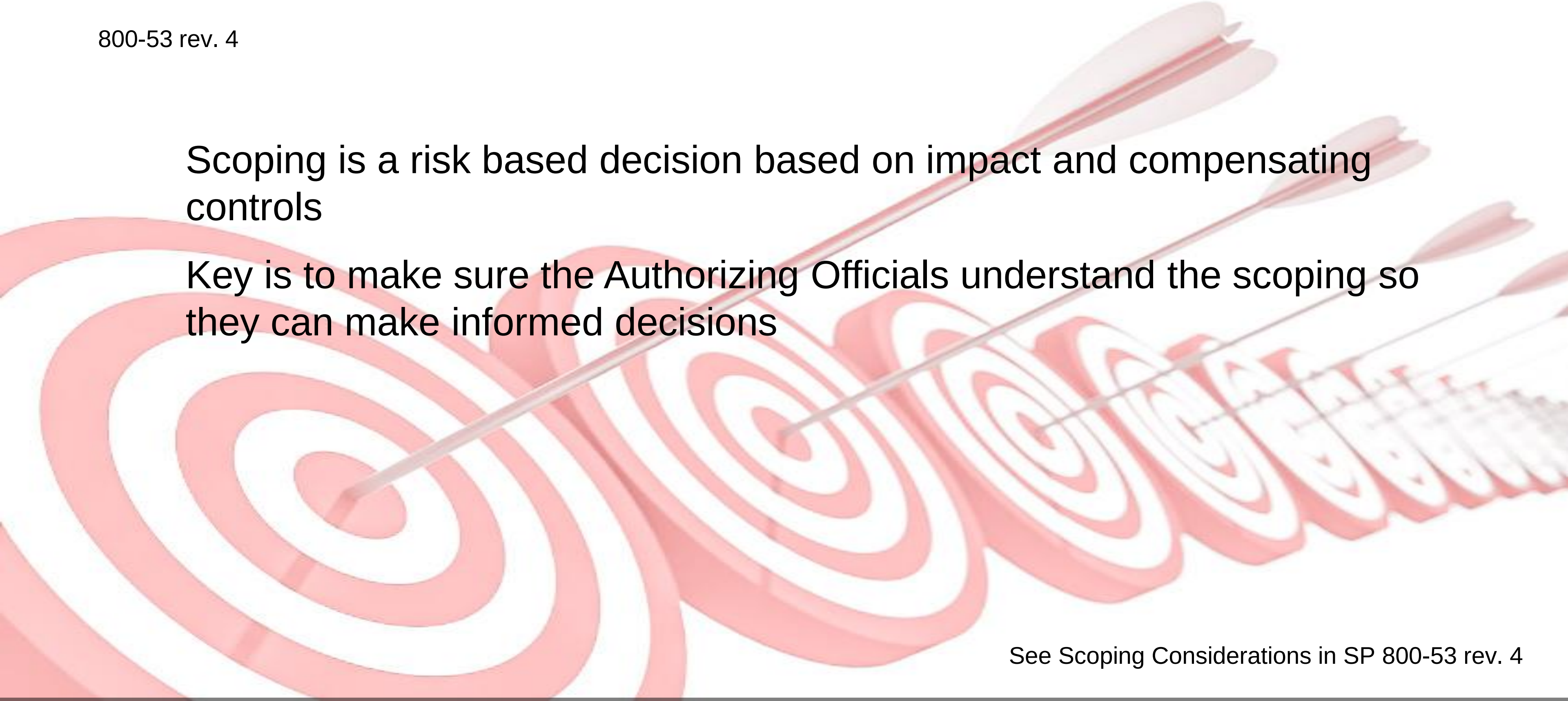
Any vendor who stores, accesses, CAN access, touches, manipulates etc… Government data MUST be *fully* assessed against all *applicable* controls.

Scoping Controls

The application of scoping considerations can eliminate unnecessary security controls from the initial security control baselines and help to ensure that organizations select *only* those controls that are needed to provide the appropriate level of protection for organizational information systems—protection based on the missions and business functions being supported by those systems and the environments in which the systems operate.

The scoping considerations listed in this section are exemplary and *not* intended to limit organizations in rendering risk-based decisions based on other organization-defined considerations with appropriate rationale.

800-53 rev. 4



Scoping is a risk based decision based on impact and compensating controls

Key is to make sure the Authorizing Officials understand the scoping so they can make informed decisions

See Scoping Considerations in SP 800-53 rev. 4

Assessing a "Cloud" Service Provider (CSP)

(applies to any 3rd party vendor)

Involves 2 parts:

1. Assessment of the CSP
   - Could involve multiple assessments

     CSP will often use subcontractors

     For example a SaaS CSP may use Amazon Web Services to host the data or May use Iron Mountain to store backups. Those providers must be assessed.

   - Could leverage other assessments

     Assessment could be conducted by the agency, leverage another agencies assessment, partially leverage non-FISMA assessments, leverage FedRAMP assessment.

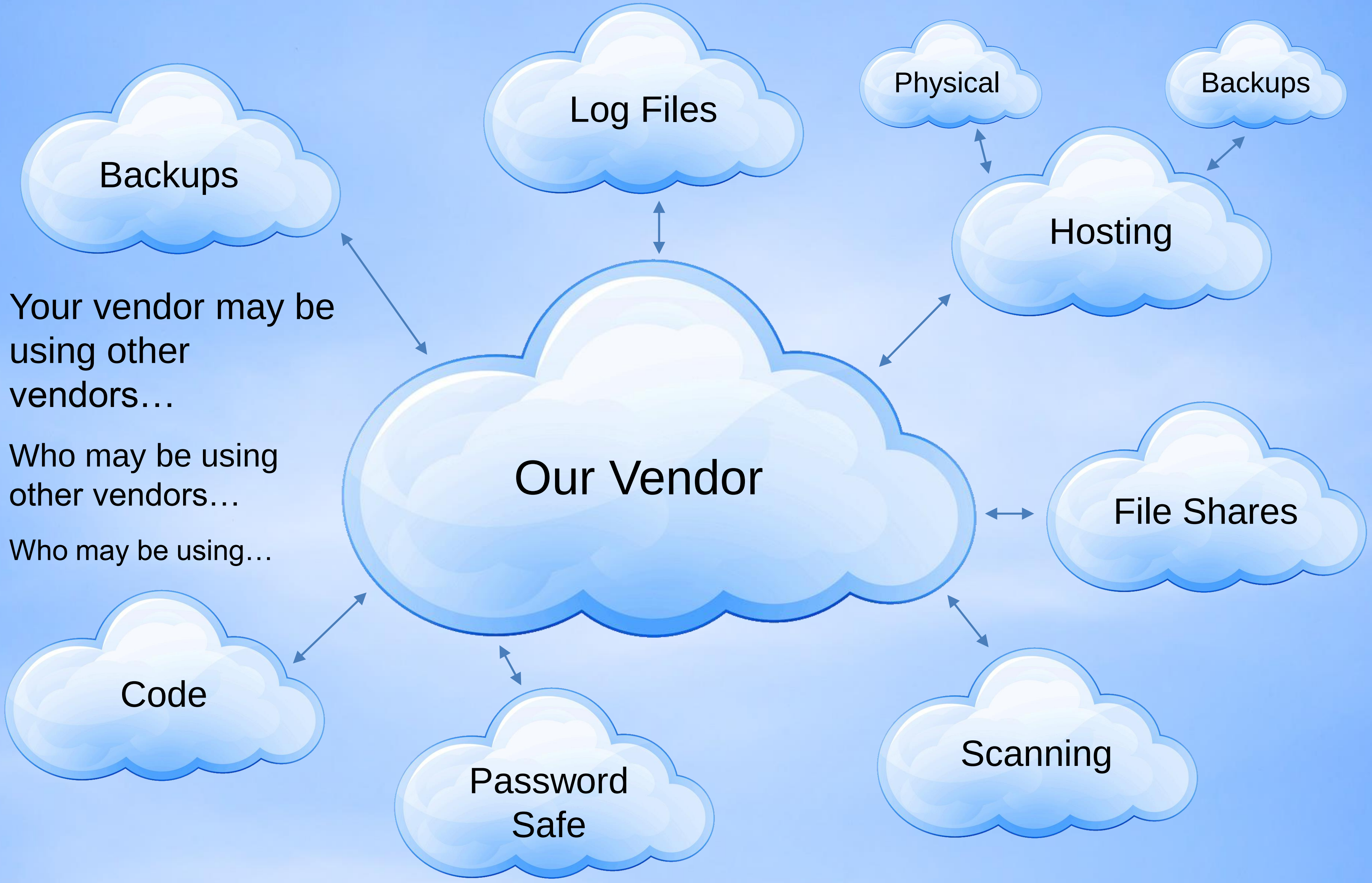
2. Assessment of agency specific controls

   There will **ALWAYS** be an agency specific implementation part

Your vendor may be using other vendors…

Who may be using other vendors…

Who may be using…



Different types of cloud assessments (example use cases)

Social Media

- Publically available, low criticality levels
- Confidentially not an issue, availability not a direct issue, integrity a concern

  Unauthorized modification of system information could be expected to have an adverse effect…
- Scope out of testing CSP, test agency specific implementation, document mitigations
- Still requires an assessment!

Enterprise Level (SaaS, PaaS, IaaS)

- Enterprise level, often moderate* criticality levels
- Full testing of CSP required
- Full testing of agency specific implementation
- Leverage FedRAMP, PCI, SAS 70/SSAE 16, HIPPA

Everything in between…

- Could have low impact levels, but not public and require login
- Could be a CSP that leveraged another PaaS and has limited access
- Must follow FISMA process to determine impact
- Finding balance of testing – 'Commensurate with the risk'

Software as-a-Service
END USERS
Enterprise Social Media
Marketing Demand Generation
Human Resources
Marketing Analytics
CRM
Vertical
Document Management
Finance & Accounting
Business Intelligence
Collaboration
Retail & E-Commerce
Platform as-a-Service
Infrastructure as-a-Service
DEVELOPERS & IT

Social Media

(Low, publically available material)

"The security controls selected for information systems are commensurate with the potential adverse impact on organizational operations and assets…"

SP 800-53 rev. 4

Social Media Scoping Example:

Social Media applications are third party-developed and externally hosted. Many controls have not been tested

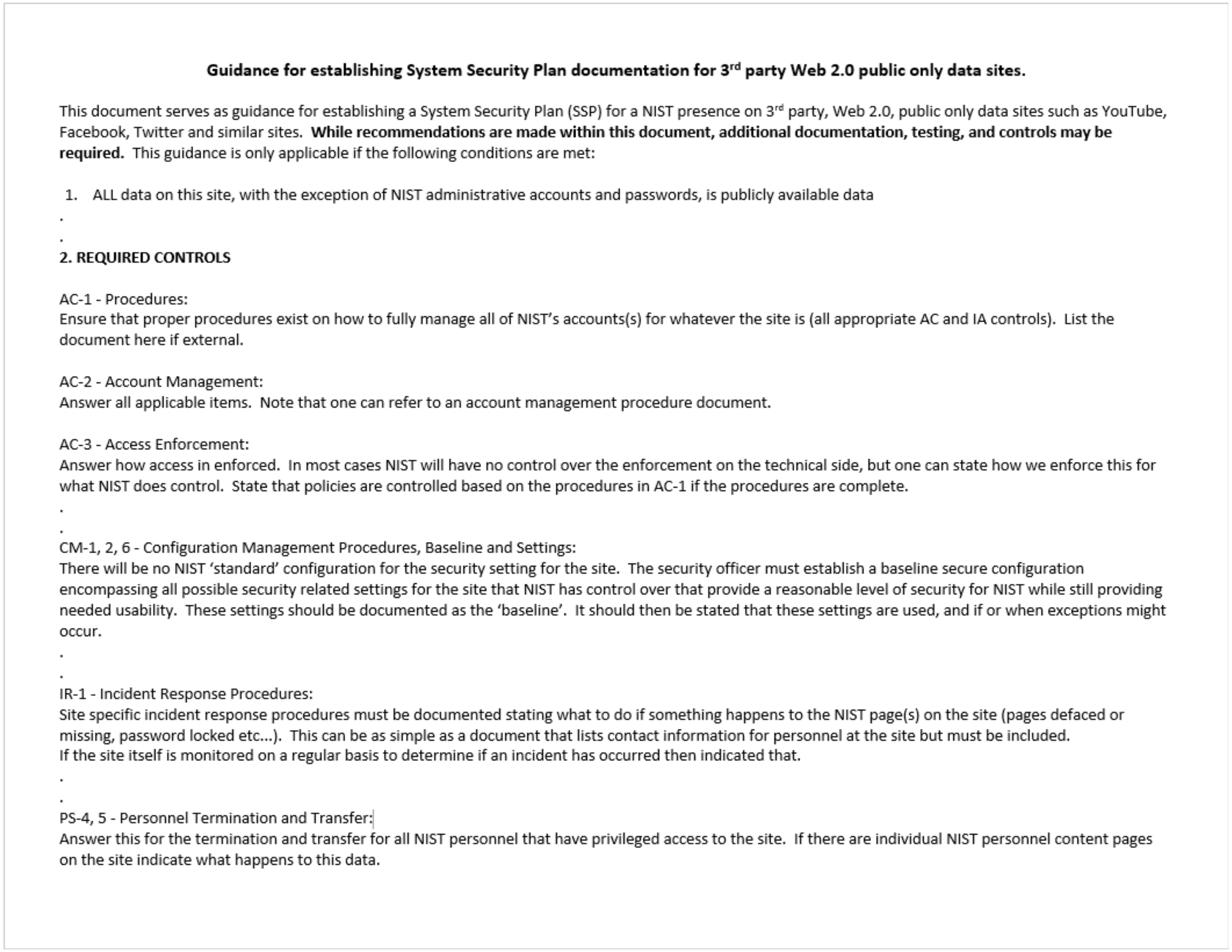
Lack of the ability to implement and test all NIST SP 800-53 controls could lead to undocumented security issues that could result in the compromise of the agency accounts on these applications.

This risk is accepted due to the following:

- All of the agency data associated with these applications that will be publicly available will be of low criticality level only.
- Account management, recommended security settings, and incident response procedures have been developed for these applications.

Social Media

Created scoping guidance for Social Media sites:



Guidance for establishing System Security Plan documentation for 3rd party Web 2.0 public only data sites.

This document serves as guidance for establishing a System Security Plan (SSP) for a NIST presence on 3rd party, Web 2.0, public only data sites such as YouTube, Facebook, Twitter and similar sites. **While recommendations are made within this document, additional documentation, testing, and controls may be required.** This guidance is only applicable if the following conditions are met:

1. ALL data on this site, with the exception of NIST administrative accounts and passwords, is publicly available data

.

.

2. REQUIRED CONTROLS

AC-1 - Procedures:
Ensure that proper procedures exist on how to fully manage all of NIST's accounts(s) for whatever the site is (all appropriate AC and IA controls). List the document here if external.

AC-2 - Account Management:
Answer all applicable items. Note that one can refer to an account management procedure document.

AC-3 - Access Enforcement:
Answer how access in enforced. In most cases NIST will have no control over the enforcement on the technical side, but one can state how we enforce this for what NIST does control. State that policies are controlled based on the procedures in AC-1 if the procedures are complete.

.

.

CM-1, 2, 6 - Configuration Management Procedures, Baseline and Settings:
There will be no NIST 'standard' configuration for the security setting for the site. The security officer must establish a baseline secure configuration encompassing all possible security related settings for the site that NIST has control over that provide a reasonable level of security for NIST while still providing needed usability. These settings should be documented as the 'baseline'. It should then be stated that these settings are used, and if or when exceptions might occur.

.

.

IR-1 - Incident Response Procedures:
Site specific incident response procedures must be documented stating what to do if something happens to the NIST page(s) on the site (pages defaced or missing, password locked etc…). This can be as simple as a document that lists contact information for personnel at the site but must be included.
If the site itself is monitored on a regular basis to determine if an incident has occurred then indicated that.

.

.

PS-4, 5 - Personnel Termination and Transfer:
Answer this for the termination and transfer for all NIST personnel that have privileged access to the site. If there are individual NIST personnel content pages on the site indicate what happens to this data.

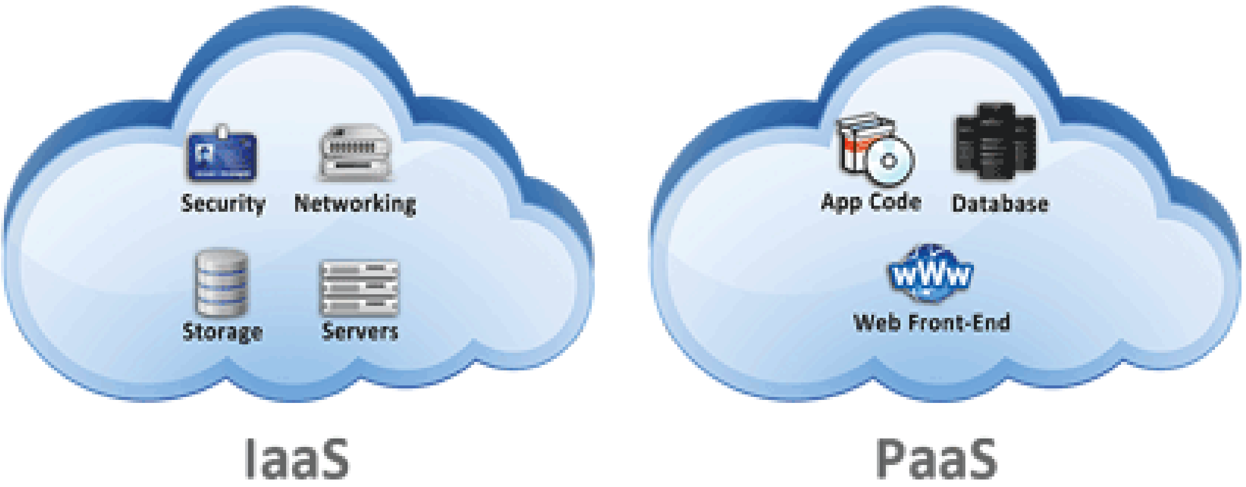
(excerpts only)

Platform/Infrastructure as a Service (P/IaaS)

Could still use other vendors…

Tend to be more knowledgeable about FISMA and FedRAMP then SaaS vendors

Tend to have independent assessments (though not always)



Leveraging other assessments

SSAE 16 (formerly SAS-70) (Statement on Standards for Attestation Engagements)
PCI (Payment Card Industry)
HIPPA (Health Insurance Portability and Accountability Act)
Sarbanes–Oxley
others… (will get into FedRAMP shortly)

- Do not encompass all FISMA (800-53)/FedRAMP controls
- Will not meet all requirements
- Some are pass/fail – no explanation of mitigating controls

For instance PCI only requires a 7 character password

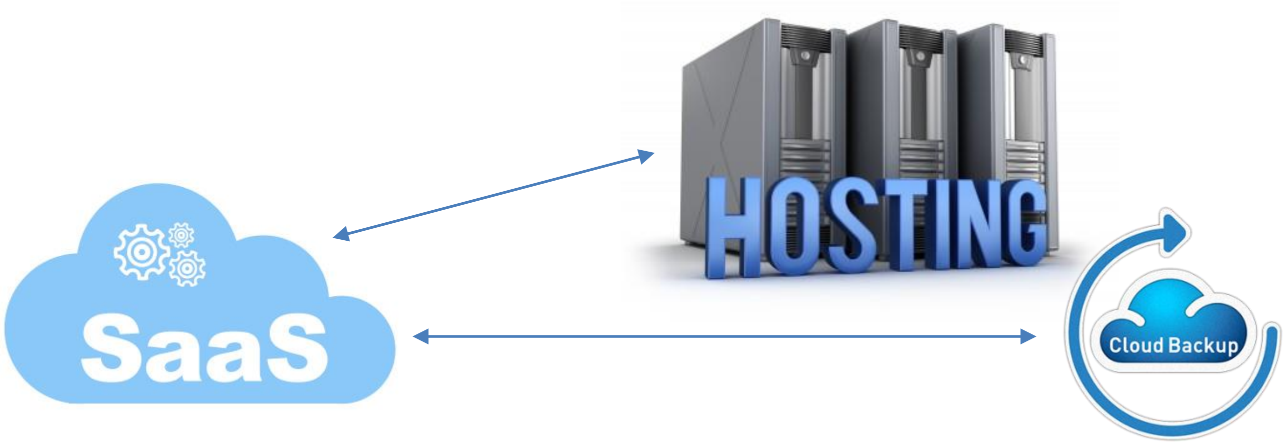
8.2.3 Passwords/phrases must meet the following:
Require a minimum length of at least seven characters.
Contain both numeric and alphabetic characters.
Payment Card Industry (PCI) Data Security Standard
Requirements and Security Assessment Procedures
Version 3.0 November 2013

Software as a Service (SaaS)

Often the SaaS vendor will use a separate vendor for hosting services
Could use additional vendors such as backup

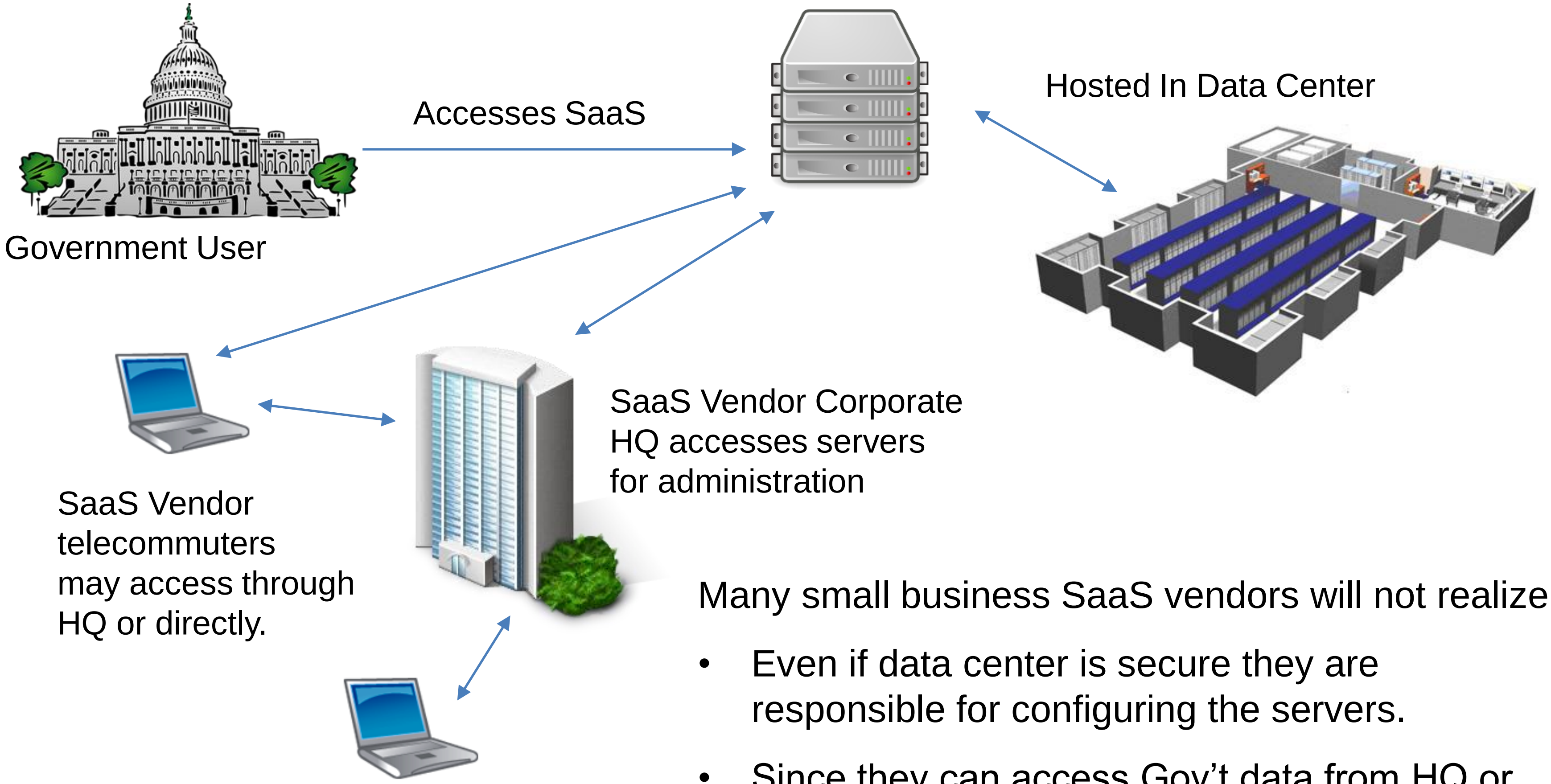
All vendors must be assessed if they can access the data in any way

SaaS vendor may not understand that they need to be assessed too!



Software as a Service (SaaS)

Typical Small Business
Cloud Vendor layout



Government User

Accesses SaaS

Hosted In Data Center

SaaS Vendor Corporate
HQ accesses servers
for administration

SaaS Vendor
telecommuters
may access through
HQ or directly.

Many small business SaaS vendors will not realize:

- Even if data center is secure they are responsible for configuring the servers.
- Since they can access Gov't data from HQ or admin telecommuters, all controls are in play for them.

Cloud Service Providers (CSP)

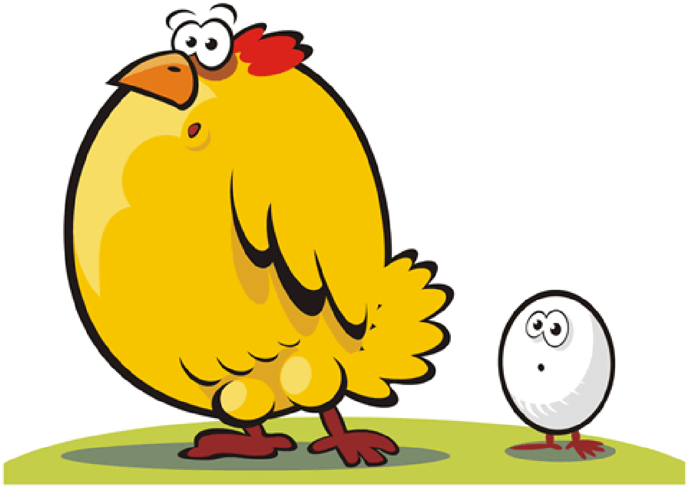
Providers seem to fall into two groups:

- Those who understand FISMA and federal government cyber security requirements
- Those that do not

Chicken and the egg problem for the vendors

Resources necessary for compliance

Fairness to small businesses



Some other Challenges

Common controls do not apply

In house don't assess control common to your agency for every system. With cloud vendor need to look at all controls.

Procurement language for security

Challenges in working with procurement to ensure that requisitions and contracts are drafted to include proper security requirements.

Incident response

How will the vendor notify you if a possible breach or incident has occurred? How with they interface with your incident response team? Will they share logs (could be difficult if a shred tenant)?

OPM requirements (IPv6, PIV, TIC, 508)

OPM Cloud First mandate vs. other OPM mandates. Many cloud vendors may not be able to currently meet all Federal Government technical requirements.

Continuous Monitoring

Most likely do not have 'feeds' from vendor. Validate continuous monitoring via artifacts.

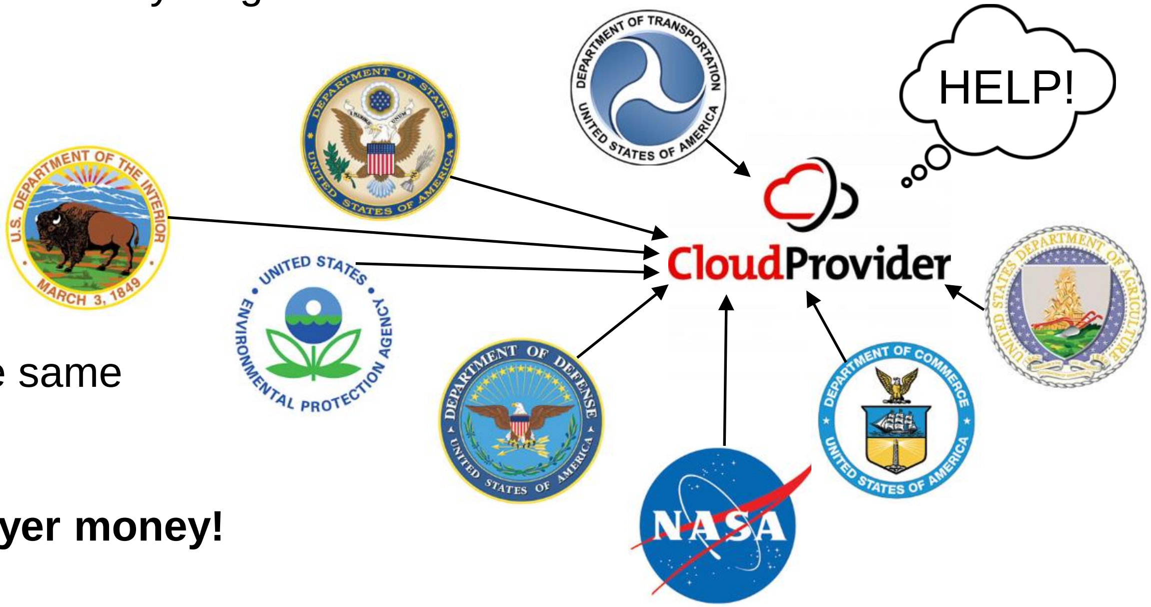
Loss of control

No matter how you slice it, you will have to accept some risk in loss of control.

Leveraging Assessments

Old way:

- Each agency (or agencies within agencies) authorized their own systems
  - Generally worked fine when everything was in house



But with cloud:

- Each agency assesses the same CSP over and over?
  - Does not make sense
  - **Inefficient use of taxpayer money!**

Led to an ad hoc sharing and leveraging of assessments

Sometimes worked, but needed to be scalable and centralized… Led to →

One assessment

FedRAMP

Leveraged by
multiple agencies

Ensuring secure cloud computing for the Federal Government

http://www.fedramp.gov

OMB Authorizing Memo December 8, 2011: https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf

Contact: info@fedramp.gov

FedRAMP does not issue ATO

ONLY your agency can issue an ATO

JAB board provides ‘provisional’ authorization only

All cloud projects must meet FedRAMP (not just FISMA) requirements
(as of June 6, 2014, which has passed)

FedRAMP is an extension of FISMA.

- Additional SP 800-53 controls
  - 1 additional low control (independence)
  - 46 additional moderate controls
  - High baseline available
- Specific FedRAMP templates

Uses validated Third Party Assessor (3PAO) for assessment.

It is your agencies responsibility to review the FedRAMP package for applicability to your agencies security requirements

  - Your agency may have additional requirements – perform gap analysis

Challenge with FedRAMP will be Continuous Monitoring

Ultimately up to your agency to ensure proper continuous monitoring

Conclusions

Government data is Government data. If a provider has access to that data in any way that that provider must be fully assessed.

- Everything must be assessed; use scoping – commensurate with the risk…

The point of this is to keep our Country's data safe. Make sure the authorizing officials understand the system and risks so they can make informed decisions.

All assessments of "cloud" vendors must follow the FedRAMP process.

Bring security in at the beginning!

- Put language in contracts.

Contact:
John Connor
john.connor@nist.gov
(301) 975-3409

Background Image: Deer at the NIST campus in Gaithersburg, MD