

Google Groups

Assessment and Authorization – Lessons Learned

John Connor, Rathini Vijayaverl
IT Security Specialists, OISM, NIST

February 13, 2018



NIST

**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.

IN THE NEWS

Equifax - 143 million consumers PII exposed

PII of 57 million Uber users exposed, Uber pays hackers bounty

LastPass saw potentially millions of passwords accessed

CVS, Walgreens, others hit by credit card breach

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

UCLA Health hacked - 4.5 million records, including PII

IRS data breach led to hackers taking tax returns

Hacked toymaker leaked gigabytes' worth of kids' headshots and chat logs

Major Security Breaches Found In Google And Yahoo Email Services

Hundreds of millions of usernames and passwords have been stolen.

OPM Breach

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.

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.

Hacking Team

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:

UserName : Neo
Password : Passw0rd

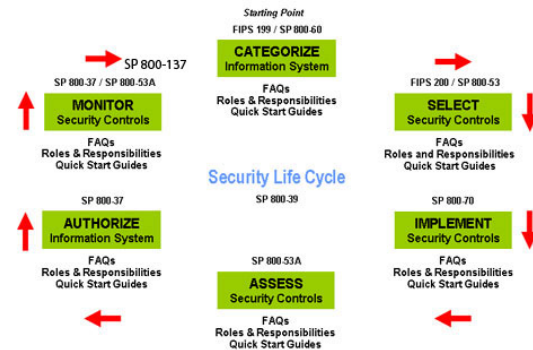
UserName : c.pozzi
Password : P4ssword



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.



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

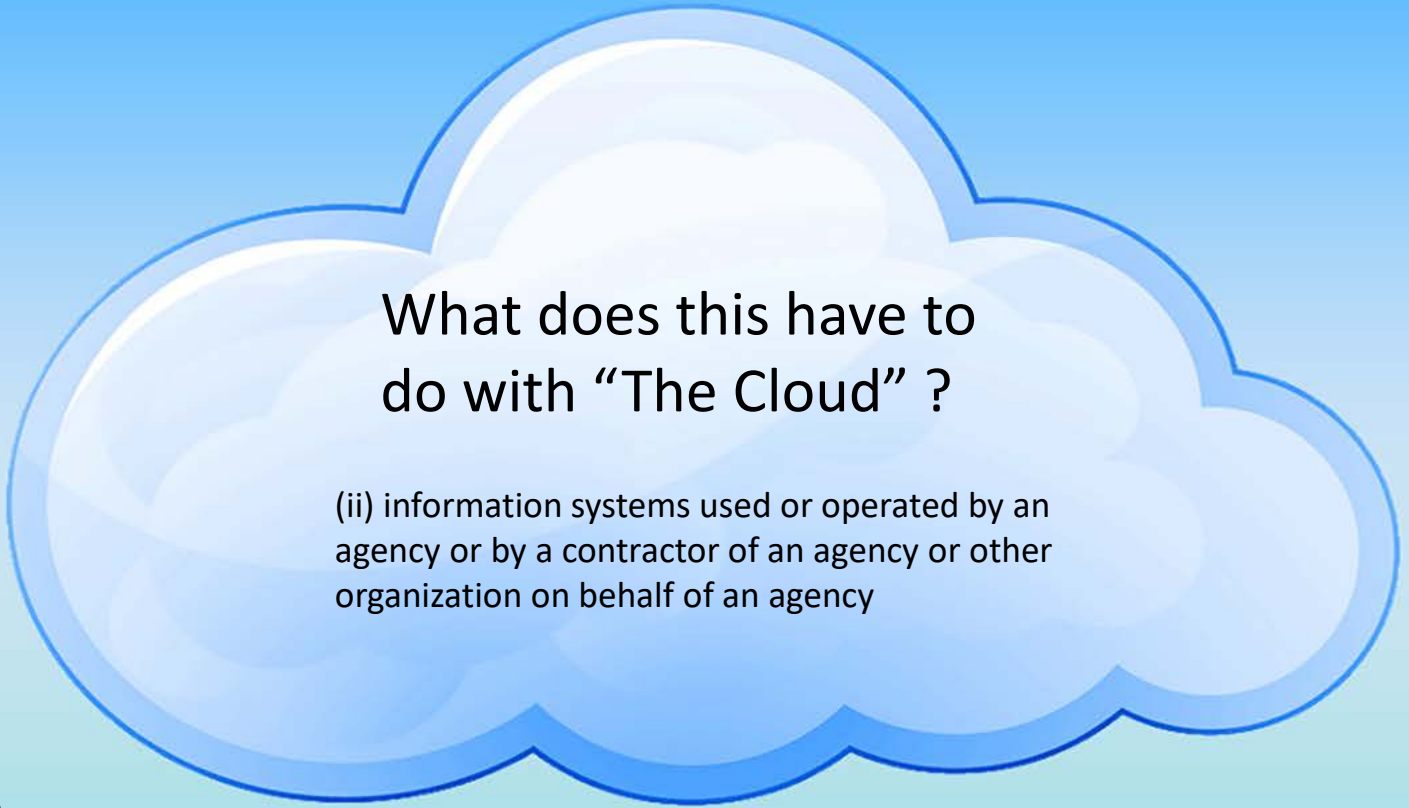
“(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

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

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.

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-145 for definition of “cloud”



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

FISMA is Risk Based – Authorizing Officials weigh residual risks vs the risk to the Agency of exposure. Not pass/fail

Risk Based Decisions:

Security plans, security assessment reports, and plans of action and milestones for common controls are used by authorizing officials within the organization to make risk-based decisions in the security authorization process for their information systems.

When security controls are provided to an organization by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization ensures that the information needed for authorizing officials to make risk-based decisions, is made available by the provider.

NIST Special Publication 800-37

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

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...

Platform/Infrastructure as a Service (P/IaaS)

Could still use other vendors...

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

Tend to have independent assessments (though not always)

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!

Leveraging other assessments

SSAE 16 (SOC 1,2,3) (Statement on Standards for Attestation Engagements)

PCI (Payment Card Industry)

HIPPA (Health Insurance Portability and Accountability Act)

Sarbanes–Oxley – ISO 27001

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

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’



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.

Created scoping guidance for Social Media sites:

(excerpts only)

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.

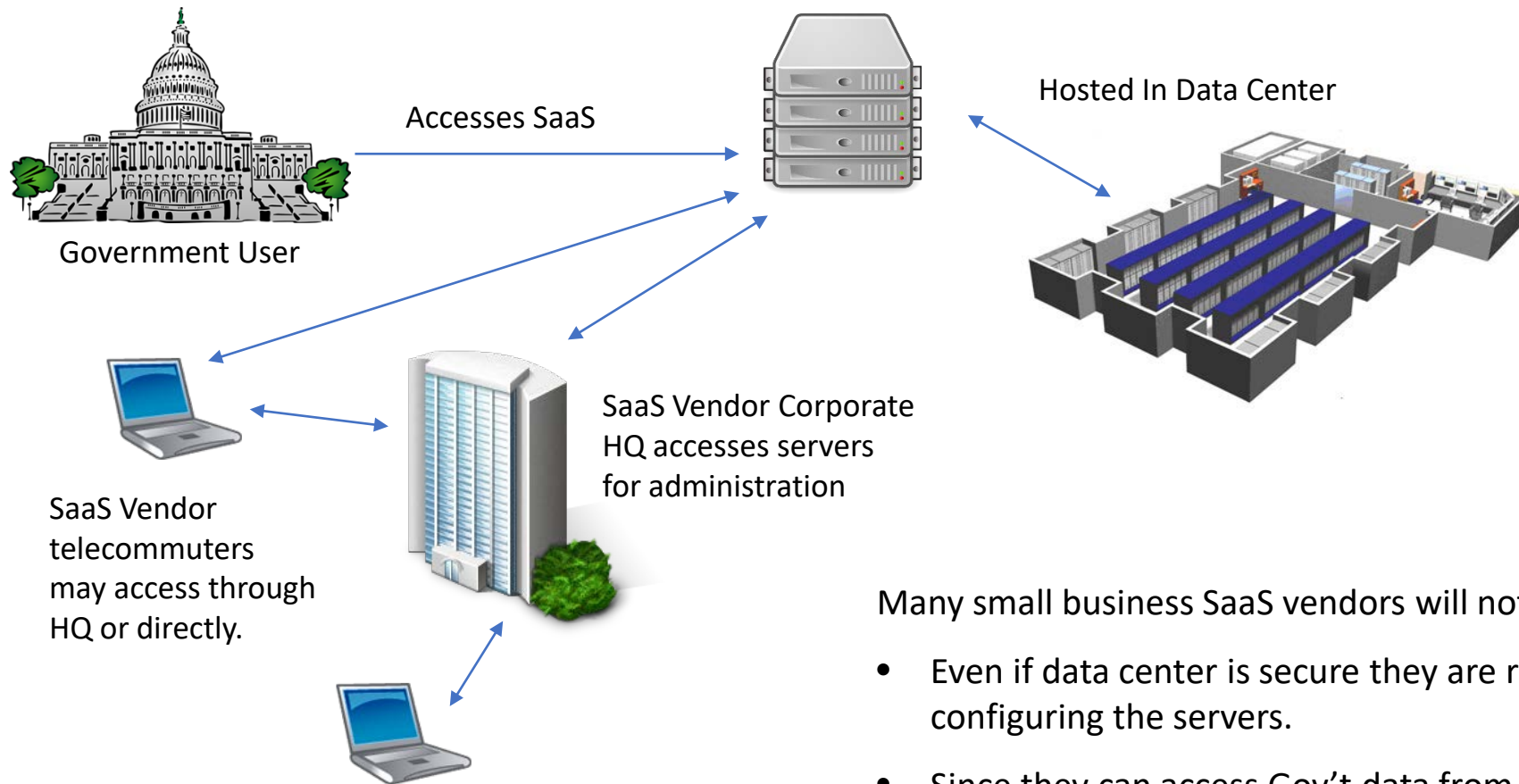
AC-3 - Access Enforcement:
Answer how access is enforced. In most cases NIST will have no control over the enforcement on the technical side, but one can state how we enforce this for what NIST does control. State that policies are controlled based on the procedures in AC-1 if the procedures are complete.

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.

Software as a Service (SaaS)



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.

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!**



Ad hoc sharing and leveraging of assessments
Sometimes worked, but needed to be scalable and centralized...
Led to →

One assessment



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 an ATO!!!
ONLY an 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)

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

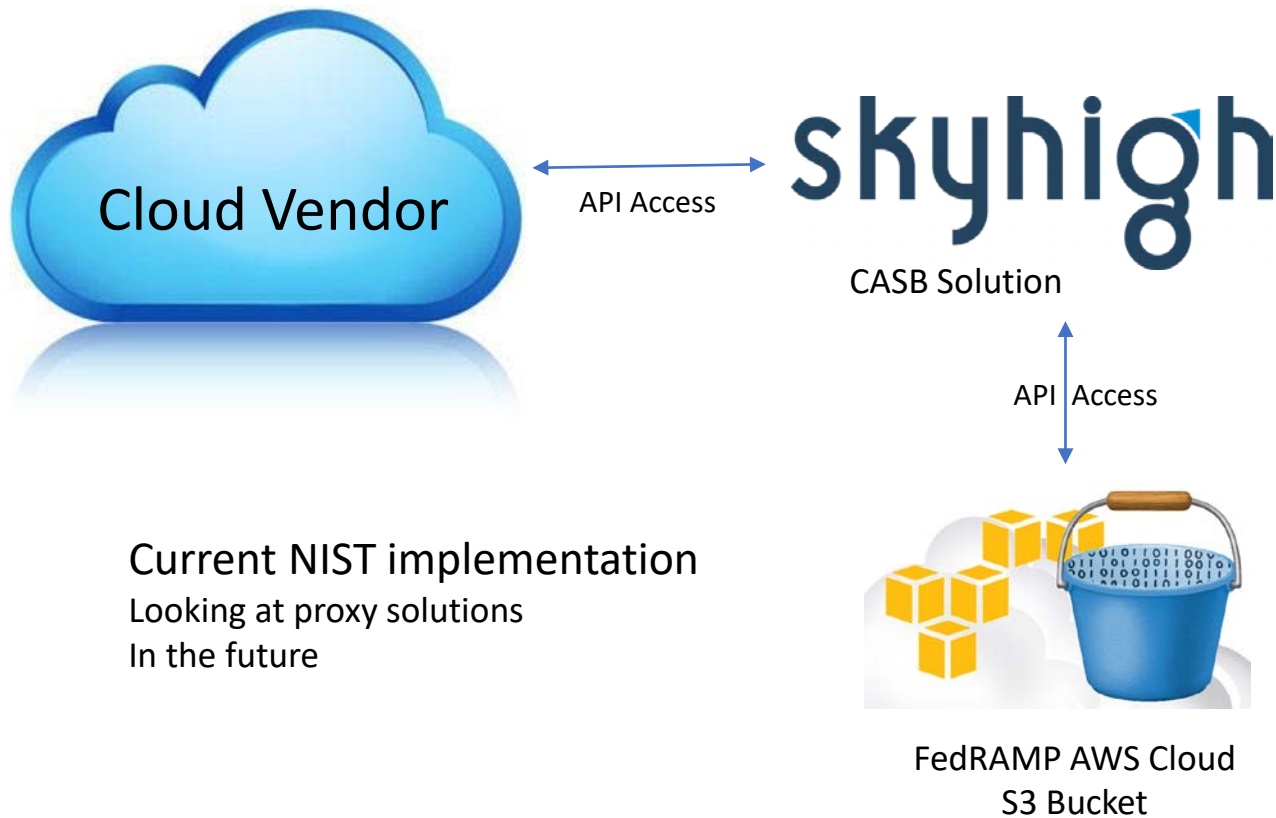
- Your agency may have additional requirements – perform gap analysis

Challenge with FedRAMP will be Continuous Monitoring

Ultimately up to your agency to ensure proper continuous monitoring



CASB Solution for DLP



Current NIST implementation
Looking at proxy solutions
In the future

Currently authorized at a low level
across the board

Moderate authorization on a case by
case basis

- DLP 'flipped' - Instead of looking for moderate data and blocking/quarantining/alerting, now must allow certain data to pass through.
- Specific NIST side controls to ensure moderate use case is properly used.

G Suite Applications



- Drive
- Docs, Sheets, Slides, & Drawings
- Hangouts
- Vault
- Groups
- Sites
- Classroom
- Gmail
- Contacts
- Calendar

**Applications
Authorized for use
at NIST**

FedRAMP.gov → Marketplace



10
Authorizations

Google - Google G Suite



System Profile

Service Models

PaaS, SaaS

Deployment Model

Hybrid Cloud

Impact Level

Moderate

Package ID

F1206081364

[Package Access Request Form](#)

FedRAMP Authorization Details

Authorization Type: Agency

Independent Assessor: Coalfire Systems, Inc.

Agency Authorization Date: 10/26/2016

Request FedRAMP Package Access

- Completed by assessor and approved by CISO or DAA
- Details on package requested
- Reason for request
- Accept terms of access for assessor and CISO
- Access provided for 30 days for evaluation
- Perpetual access after issuance of Agency ATO

Terms of Agreement

I will not disclose information in FedRAMP Security Packages to any third-parties, i.e., any parties not expressly authorized to have access to the information by the FedRAMP Program Management Office or the company that submitted the Security Package.

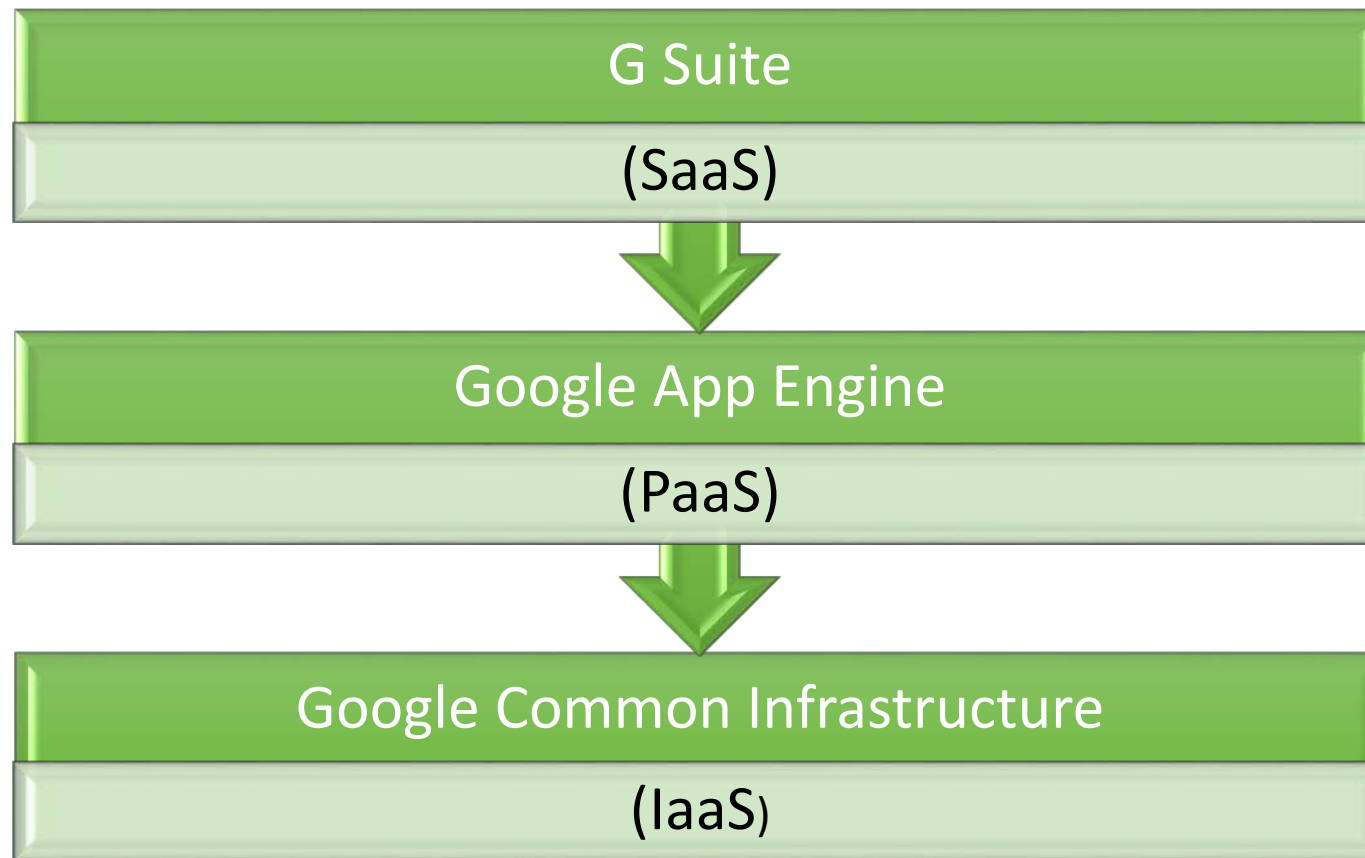
I will not save, print, email, post, publish, or reproduce any FedRAMP Security Package documents in any form including all electronic methods.

To the extent I must download FedRAMP Security Package documents in order to view them, once my review is complete for a given session, I agree to destroy and delete all copies of FedRAMP Security Package documents.

To the extent I must download FedRAMP Security Package documents in order to view them, I agree to do so only on government furnished equipment and devices. I will not download FedRAMP Security Package documents on non-government equipment and devices.

The undersigned prospective package reviewer certifies that the information listed above is current and accurate.

Google FedRAMP Package Components



G Suite FedRAMP Documents

- FIPS 199 Worksheet
- Electronic authentication
- System Security Plan
- Privacy Impact Analysis
- Contingency Plan
- Configuration management Plan
- Continuous Monitoring Plan
- Incident Response Plan
- Rules of Behavior
- Penetration Test Report
- Security Assessment Report (SAR)
- Security Assessment Plan (SAP)
- Policies and Procedures
- POA&M Report
- Control Implementation Summary

Policies and Procedures Provided

- Access Control
- Asset Inventory
- Backup and Disaster Recovery
- Change Management
- Configuration & Patch Management
- Risk Management
- Security Architecture Review
- Vulnerability Scans and Management
- Governance
- Roles and Responsibilities
- Monitoring and Logging
- Third party Management
- Policy Management
- Scope Overview

Google Assessment at NIST

Key NIST Assessment Areas

- Infrastructure Security
- Encryption of Customer Data
- Continuous Monitoring
- Incident Response
- Personnel Screening
- Corporate Network

Assessment Sources

- System Security Plan
- FedRAMP SAR
- POA&M Report
- Process Documents

FedRAMP SAR Tables

SAR Security Assessment Summary

- Risks Corrected During Testing
- Risks With Mitigating Factors
- Risks Remaining Due to Operational Requirements
- Risks Known for Interconnected Systems



**Include in NIST
Security Assessment
Report**

Evidence of Continuous Monitoring

- POA&M Report in FedRAMP package
- Request more recent monthly reports
- View evidence of monitoring process
- How findings are documented
- Explanation for deviations

High Level Findings in NIST Review

- Risk Accepted by Google
- G Suite POA&M Status
- Corporate office infrastructure
- Use of proprietary software
- Personnel screening

Lessons Learned

- External assessments are unique
 - Leveraged FedRAMP assessment
- Scope of the assessment
 - Included supporting infrastructure
- Helpful to have usage guidelines
 - Rules of Behavior for NIST users

Questions?

Contact:

John Connor

john.connor@nist.gov

Rathini Vijayaverl

rathini.vijayaverl@nist.gov

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