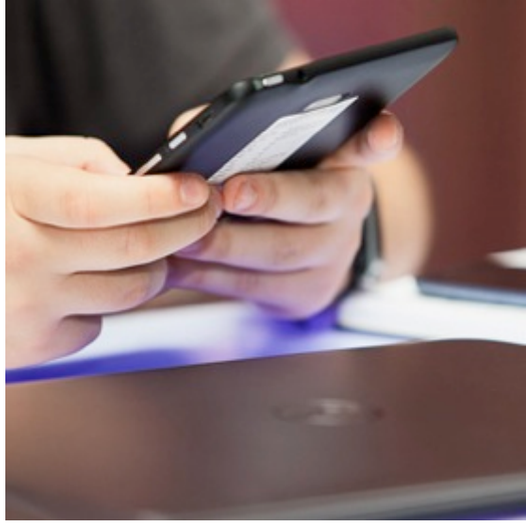
govDELIVERY



Cloud Security 101:
Why FedRAMP Matters To You

TODAY'S AGENDA

A

CLOUD SECURITY

BOB AINSBURY, GOVDELIVERY

B

FEDRAMP & WHAT IT MEANS

MATT GOODRICH, GSA

C

GOVDELIVERY & FEDRAMP: STATUS & SECURITY PRACTICES

GERRY HANSEN, GOVDELIVERY

D

Q & A

YOUR SPEAKERS TODAY

Bob Ainsbury

Chief Operating Officer
GovDelivery

Matt Goodrich

Director, Federal Risk and Authorization Management Program (FedRAMP)

GSA's Office of Citizen Services and Innovative Technologies

Gerry Hansen

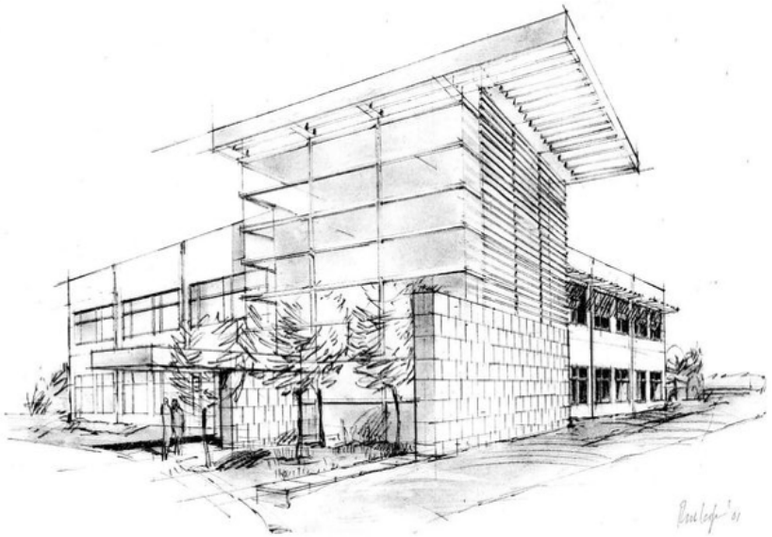
Vice President of Cloud Operations
GovDelivery

Security @ GovDelivery

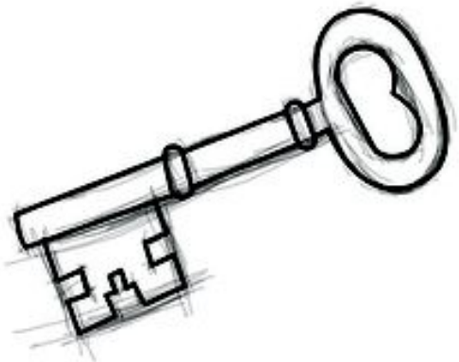
Bob Ainsbury, COO

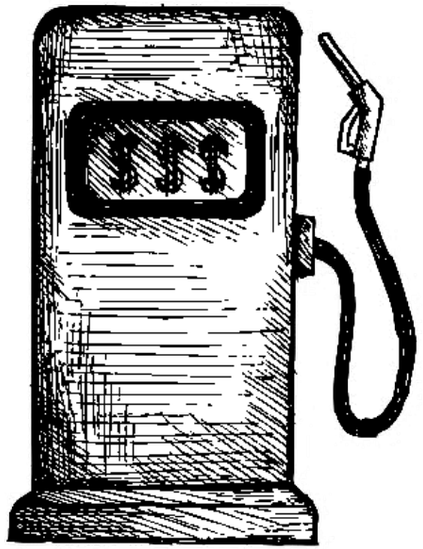
govDELIVERY

Agenda



govdelivery





govdelivery

Heartland PAYMENT SYSTEMS™

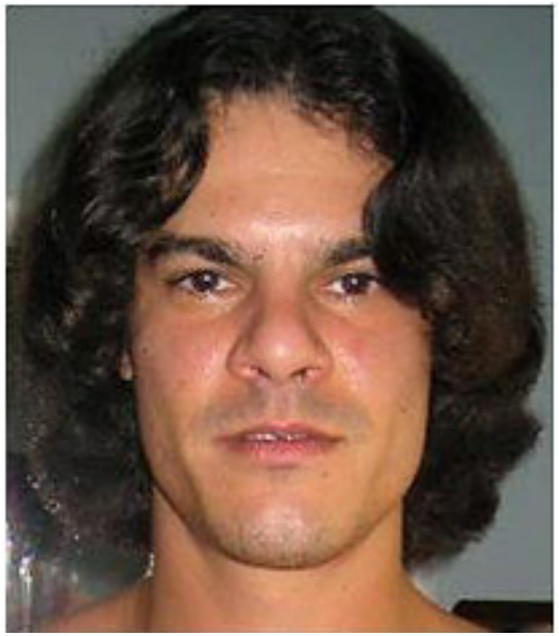
The Highest Standards | The Most Trusted Transactions

March 2008

SQL Injection

Data from 134 million credit cards

govdelivery



Albert Gonzalez

2006 2016

GOVDELIVERY

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Heartland

So, in January 2015 Heartland made a **breach warranty** promise:

Heartland Payment Systems is so confident in the security of its payment processing technology that, on Jan. 12, it announced a new breach warranty for its users. The warranty program will reimburse merchants for costs incurred from a data breach that involves the Heartland Secure credit card payment processing system.

Forbes

Heartland Payment Systems suffered a major data breach that affected their payroll customers.

May 8th2015

GOVDELIVERY

SECURITY MATTERS MORE THAN EVER

The Bottom line :)

- There were 50,315 reported public sector security incidents in 2015 alone.
- The average total cost of a data breach is $6,500,000.
- There was a 1,121% increase in federal agency security incidents from 2006 to 2014.

The Bottom line :)

govdelivery

Bring agencies closer to their communities

Public sector agencies across the globe use our end-to-end solutions to connect with more of their citizens. Our customers use GovDelivery to increase digital engagement, grow their digital audience by cross-promoting content, build communities around data, and create modern training experiences.

……digital technologies that dramatically increase **public participation in government initiatives**.

GOVDELIVERY

GovDelivery Communications

GovDelivery Learning

GovDelivery Data

govdelivery

GovDelivery
Communications

GovDelivery
NETWORK

GovDelivery
Learning

GovDelivery
Data

govdelivery

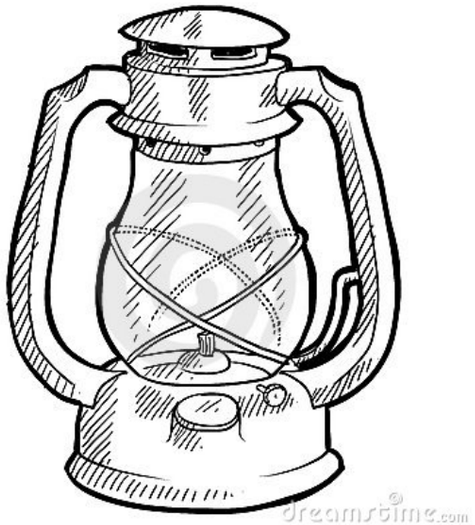
Admins 36,000+

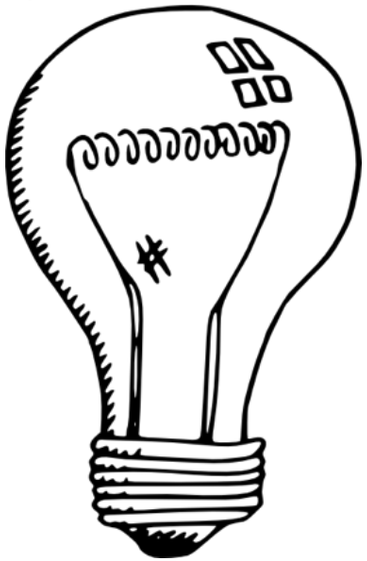
New Subscribers Each Day 40,000+

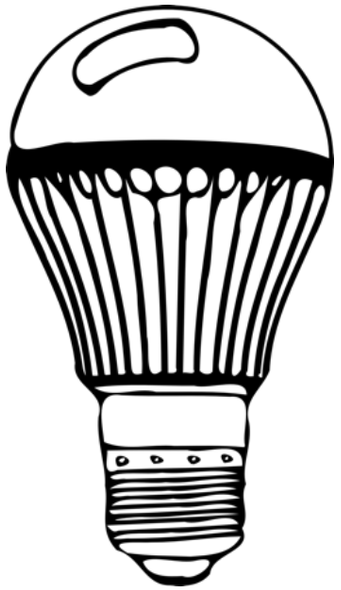
Ten times the employees of

United States Department of Education

Eyeballs on content in ’15: 2 Billion







govDELIVERY

Q4, 2009 — National Institute of Standards and Technology ATO (FISMA LOW)

Q4, 2009 — U.S. Census Bureau ATO (LOW)

Q1, 2013 — ISO 27001

Q2, 2014 — Centers for Medicare and Medicaid Services (CMS) ATO (MODERATE)

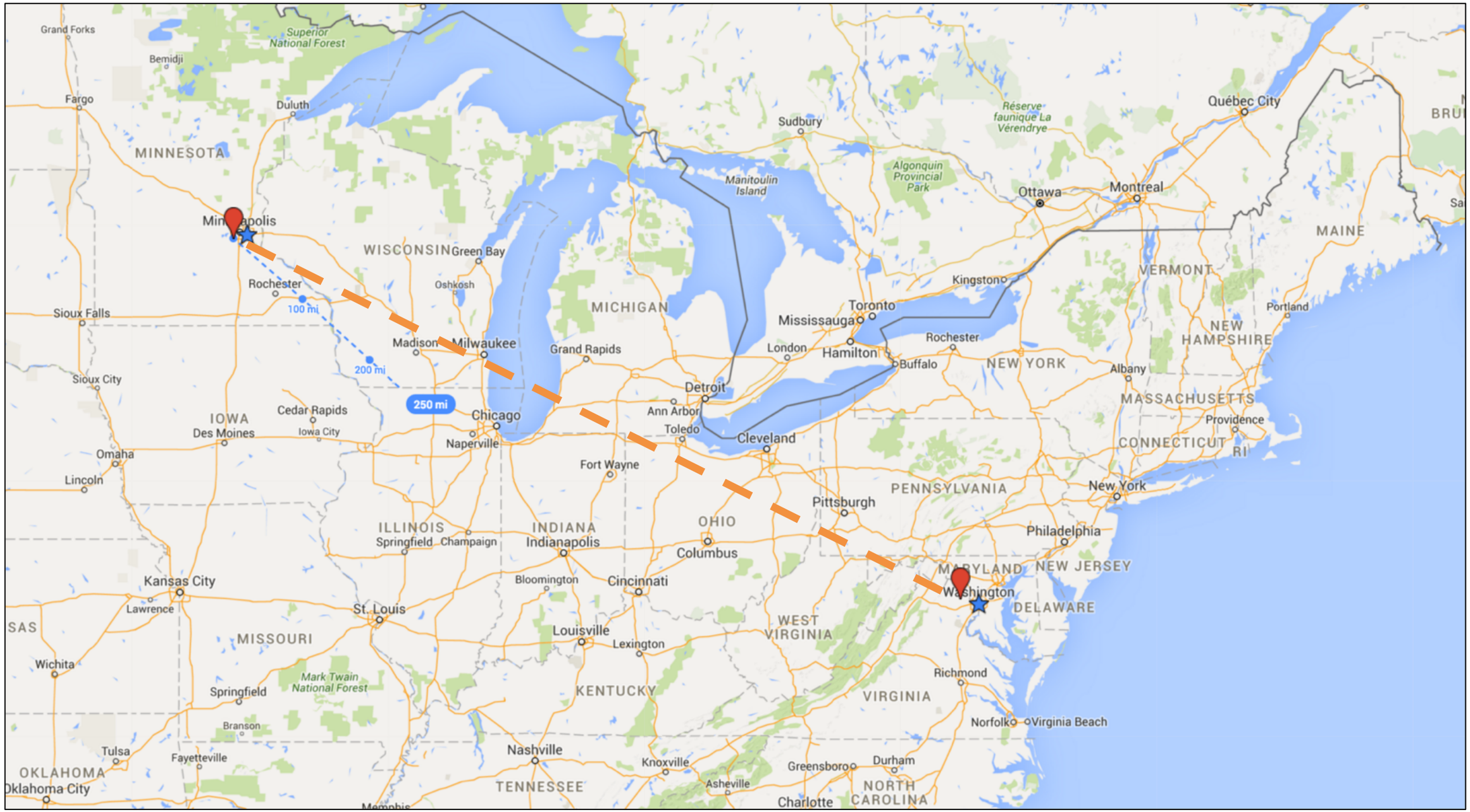
Q1, 2015 — U.S. Census Bureau ATO (MODERATE)

Q1, 2016 — FedRAMP (MODERATE)

govDELIVERY

govdelivery

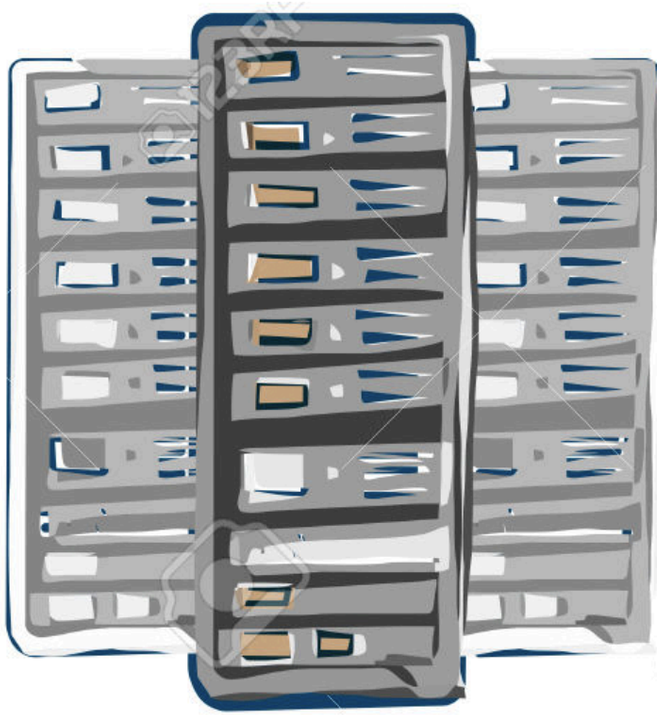
Two Data Centers



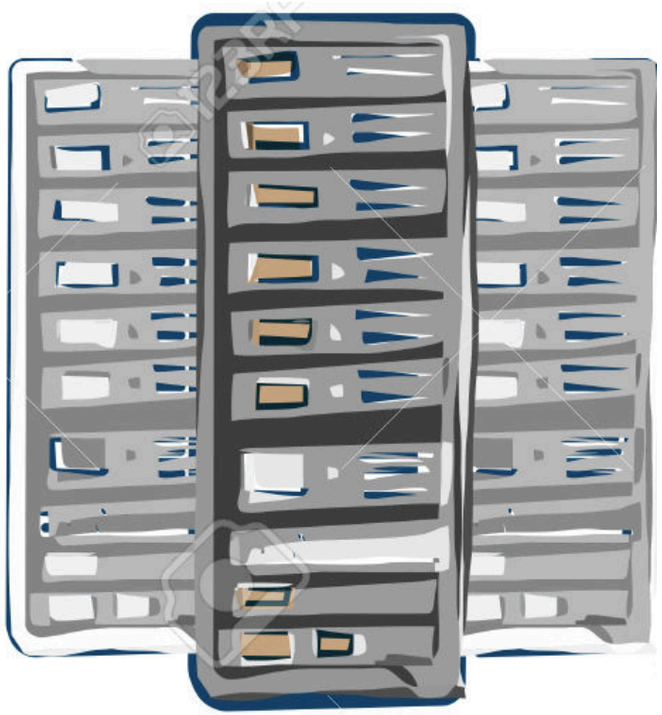
9 TERABYTES of ?????

1100+ virtual machines
2,500 DNS entries

10,000+ emails per second
Billions and billions per year



GOVDELIVERY



- Advanced firewalls
- Sophisticated DDoS Defenses
- Two factor sign in
- Intrusion detection
- Package signing
- Data encrypted in transit & at rest
- 20,000+ different monitoring nodes
- Monthly+ scanning of all hosts, networks, applications and data bases
- .....

Every employee is trained in security
The security team conducts phishing test and random audits

GOVDELIVERY

Scan information	
Start time	3/5/2016 4:14:21 PM
Finish time	3/5/2016 5:13:16 PM
Scan time	58 minutes, 55 seconds
Profile	Default
Server information	
Responsive	True
Server banner	nginx
Server OS	Unknown

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	21
High	0
Medium	1
Low	17
Informational	3

GOVDELIVERY

govloop

GOVDELIVERY

FedRAMP

Federal Risk and Authorization Management Program

FedRAMP and Why It Matters

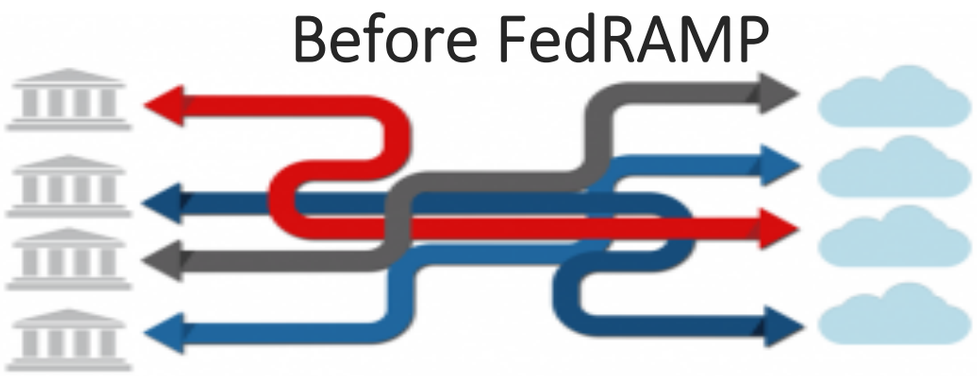
March 28, 2016

Presented by: Matthew Goodrich

www.fedramp.gov

FedRAMP: Overview

- FedRAMP was established via OMB Memo in December 2012.
- FedRAMP is the first government-wide security authorization program for FISMA – mandatory for all agencies and all cloud services
- FedRAMP's framework is being modeled in other government security programs (mobile, data) and by other countries (UK, EU, China)
- FedRAMP's focus is to ensure the rigorous security standards of FISMA are applied while introducing efficiencies to the process for cloud systems, key of which is re-use
- Conservative cost estimates for FedRAMP is $40M for the government alone



How FedRAMP Is Enforced in the USG

- December 8, 2011 Policy Memo from OMB
- Requires agencies to implement FedRAMP

- Established roles and responsibilities within FedRAMP
  - GSA, DOD, DHS CIOs are the governing body called the Joint Authorization Board (JAB)
  - GSA would host FedRAMP Program Management Office
  - DHS would coordinate the continuous monitoring and other activities
  - Agencies must implement FedRAMP and require with vendors contractually

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

December 8, 2011

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Steven VanRoekel
Federal Chief Information Officer

SUBJECT: Security Authorization of Information Systems in Cloud Computing Environments

1. Introduction

Cloud computing offers a unique opportunity for the Federal Government to take advantage of cutting edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens. Consistent with the President's International Strategy for Cyberspace and Cloud First policy, the adoption and use of information systems operated by cloud service providers (cloud services) by the Federal Government depends on security, interoperability, portability, reliability, and resiliency.

Over the past 24 months, the Administration has worked in close collaboration with the National Institute of Standards and Technology (NIST), the General Services Administration (GSA), the Department of Defense (DOD), the Department of Homeland Security (DHS), the United States Chief Information Officers Council (CIO Council) and working bodies such as the Information Security and Identity Management Committee (ISIMC), state and local governments, the private sector, non-governmental organizations (NGOs), and academia to develop the Federal Risk and Authorization Management Program (FedRAMP). This program introduces an innovative policy approach to developing trusted relationships between Executive departments and agencies[1] and cloud service providers (CSPs).

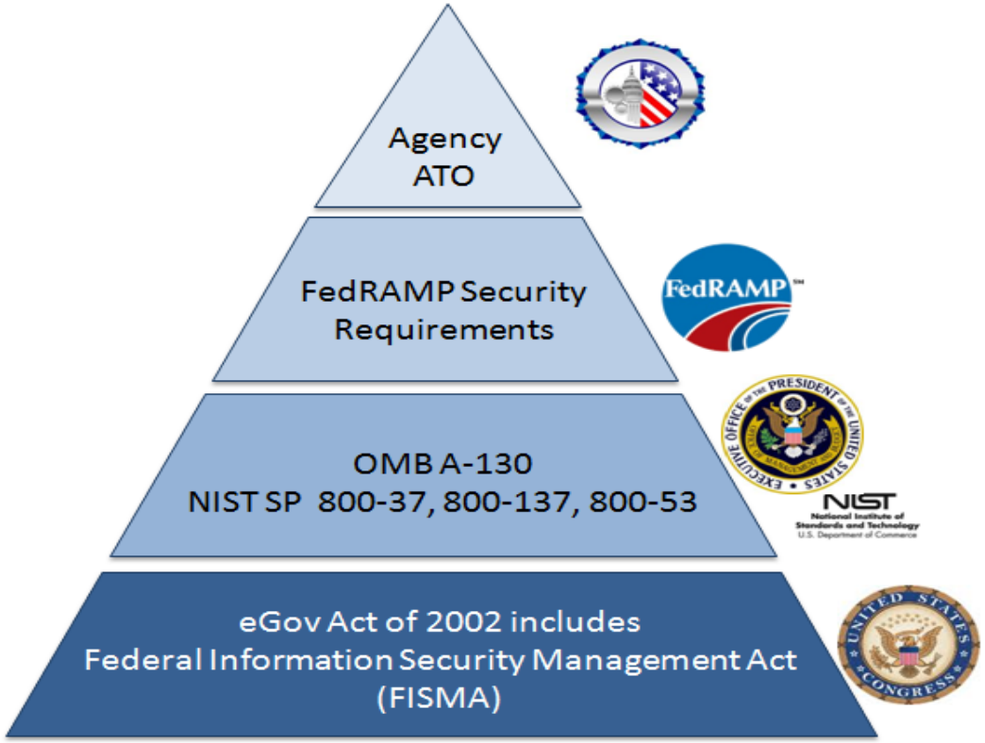
FedRAMP will provide a cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels;
- A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs;
- Authorization packages[2] of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the DHS, DOD, and GSA;

[1] References to Executive departments and agencies include all subordinate organizations within those departments and agencies.
[2] Authorization packages contain the body of evidence needed by authorizing officials to make risk-based decisions regarding the information systems providing cloud services. This includes, as a minimum, the Security Plan, Security Assessment Report, Plan of Action and Milestones and a Continuous Monitoring Plan.

FedRAMP fits within the same framework agencies are using currently to provide security authorizations of IT services

- FedRAMP is how agencies implement FISMA for use of cloud based IT products and services
- Essentially, FedRAMP is a supplemental policy to OMB A-130 for security authorizations.
- Agencies are still required to grant individual authorizations



FedRAMP SAF / NIST RMF Comparison

FedRAMP SAF Process	NIST SP 800-37 Step	FedRAMP Standard
Document	1. Categorize System	Low and Moderate Impact Levels
	2. Select Controls	Use FedRAMP Control Baselines for Low and Moderate Impact Levels
	3. Implement Security Controls	Use FedRAMP templates Implementation Guidance in "Guide to Understanding FedRAMP"
Assess	4. Assess the Security Controls	FedRAMP accredits 3PAOs 3PAOs use standard process and templates
Authorize	5. Authorize the System	ATOs with JAB P-ATO or Agency ATO CSP Supplied packages
Monitor	6. Continuous Monitoring	Use Continuous Monitoring Strategy and Guide

Effort and Resources Required by Vendors

- **Preparedness**
  - Documentation effort requires 1000+ pages
  - Over 15 documents necessary to complete the authorization
  - Documentation covers not only implementations, but internal policies and procedures – many times needing to be updated to address unique requirements of FedRAMP
  - Sometimes technical or architectural considerations

- **Time Commitment for Authorization**
  - Authorizations typically take minimum of 6 months to complete, average is 12
  - Completing a redesign of this to bring down to less than 6, but still a large commitment

- **Assessment Cost**
  - Assessments by 3PAOs typically covered by CSPs
  - Costs range from 80k to 6+ figures depending on size, scope, complexity

- **Continuous Monitoring Commitment**
  - FedRAMP is not a project – it's a program and requires resources to not only get an authorization, but to maintain an authorization

Why It Works

- **Federal Mandate**
  - Required by White House policy
  - Agencies have to do it – and if they don't they have to answer to the White House as to why

- **Uses Existing Processes**
  - Agencies and industry are familiar with FISMA – its been the law since 2002
  - Use the same framework as other types of IT
  - "Normalization" to increase reuse and trustworthiness of security packages

- **Transparency**
  - FedRAMP makes all requirements publicly available on FedRAMP.gov

- **Consensus and Stakeholder Buy in Approach**
  - Every standard FedRAMP creates – goes through some type of public comment allowing everyone to have input and ownership of the program

- **FedRAMP Branding: Service Mark**
  - "FedRAMP" is service marked
  - Gives the name meaning and power – not anyone can use it

Security @ GovDelivery

Gerry Hansen, VP Cloud Operations

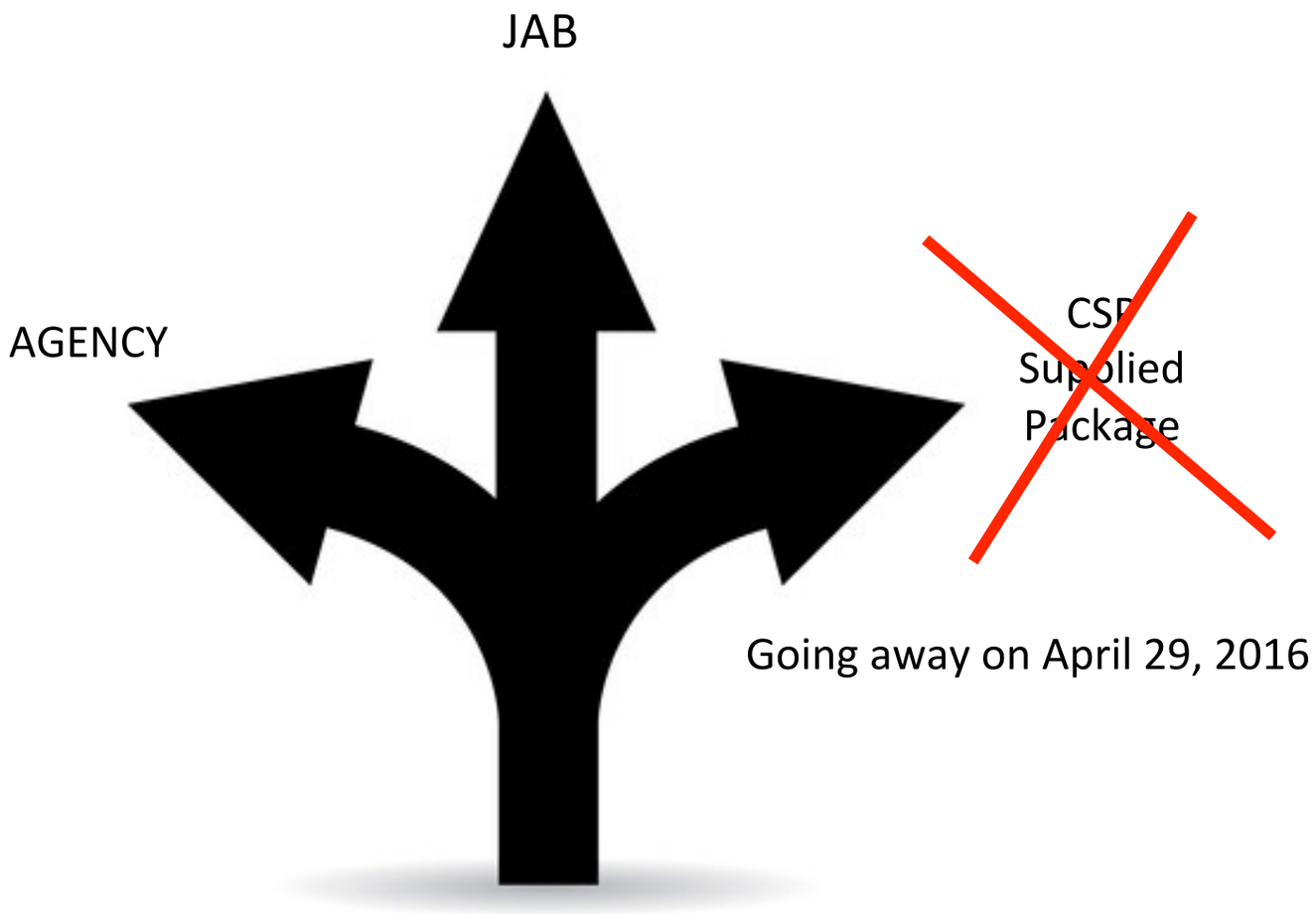
govDELIVERY

What FedRAMP means to you?

FedRAMP

govdelivery

~~Three~~ Two Paths to FedRAMP Authorization



A JAB Provisional Authorization is the <u>most rigorous technical review</u> of the three options. A JAB Provisional ATO (P-ATO) indicates that the cloud platform has undergone a technical review by the FedRAMP Project Management Office (PMO) and has been assessed by a FedRAMP accredited third-party assessor (3PAO), **representatives from the <u>Department of Homeland Security (DHS), Department of Defense (DoD), and the General Services Administration (GSA).</u>**

GOVDELIVERY

Agency Responsibility Matrix

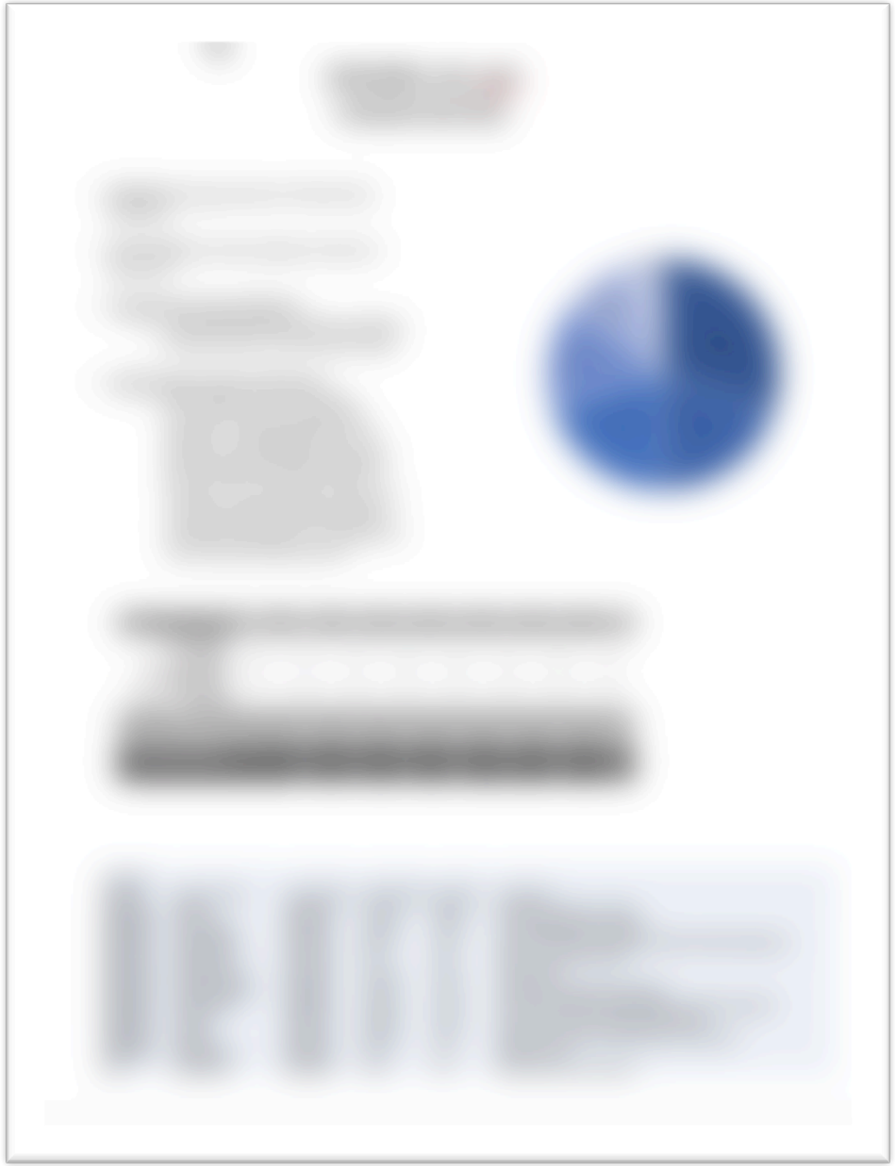
govDELIVERY

govdelivery

- Ensure password updates every 60 days
- Client administrators are responsible to authorize and review their accounts, privileges
- Agency computer screen locking
- Agencies should provide security awareness training and annual refresher training to their employees
- Administrator screening

- Review your account
- Explain your responsibilities
- Work with you to develop a compliance path

govdelivery



Quarterly Updates

- List of Admins
- Info on restricted topics: adds, changes, activity
- Failed login attempts
- Browser admin timeouts
- Admins with changed email: email other than agency
- Incident summary for the prior quarter
- Your admin activity stats
- Access exceptions: weekend, off hours, holidays, etc.
- IP Analysis: which countries, atypical IP addresses

govdelivery

FedRAMP

govdelivery

QUESTIONS?

Bob Ainsbury

Chief Operating Officer
GovDelivery

Matt Goodrich

Director, Federal Risk and Authorization Management Program (FedRAMP)

GSA's Office of Citizen Services and Innovative Technologies

Gerry Hansen

Vice President of Cloud Operations
GovDelivery

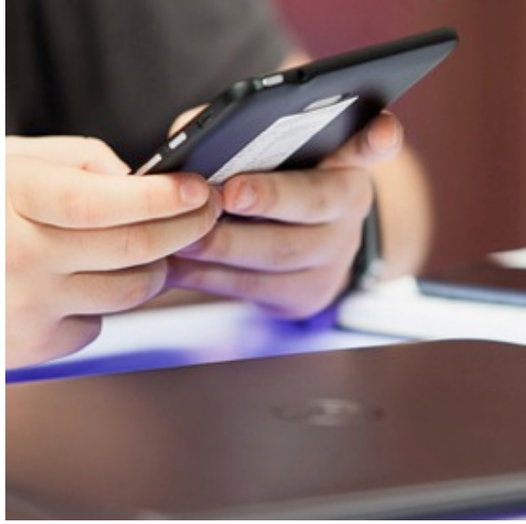
GRAB YOUR CELL PHONE - TEXT TO FILL OUT A QUICK SURVEY!

HOW WAS TODAY'S EVENT?

(A = GREAT; B=GOOD; C=OKAY; D=BAD)

571-620-6522

govDELIVERY



THANK YOU FOR YOUR TIME