



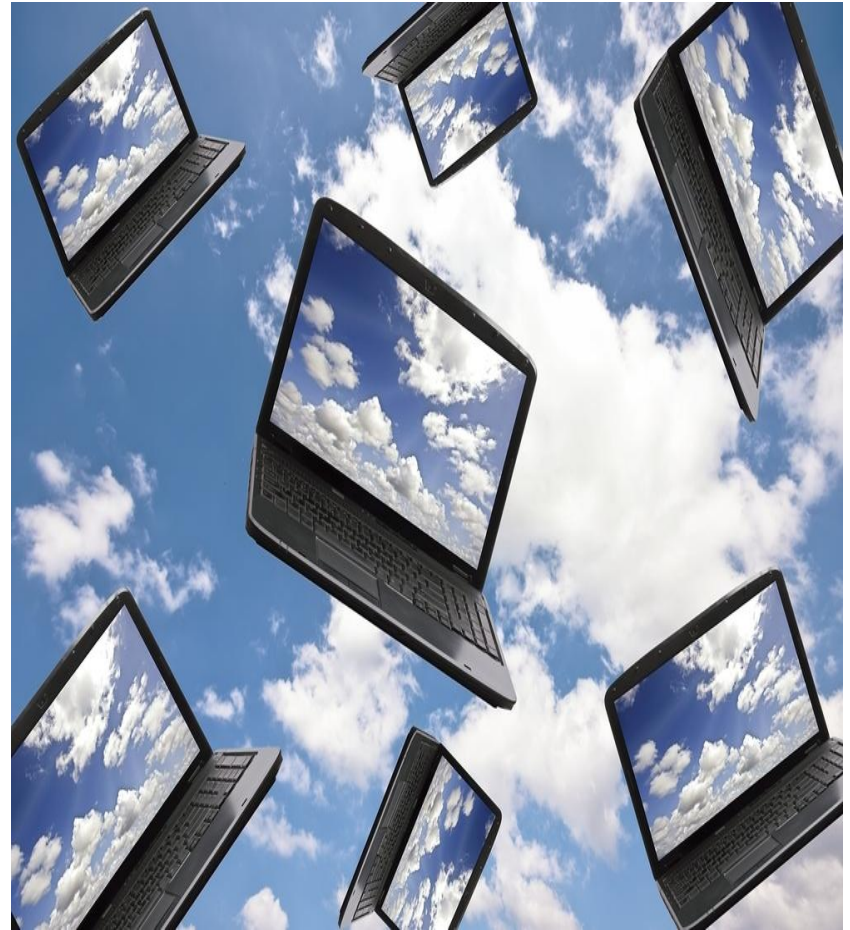
# The 2010 Symantec Break in the Clouds Report

# Introduction

The White House is urging Federal agencies to adopt cloud computing, with a clear focus on streamlining infrastructure management, improving service, and saving money.

Security concerns, however, continue to hold agencies back.

**The 2010 Symantec Break in the Clouds Report** examines current government cloud adoption, uncovers government IT professionals' top security concerns, and, importantly, captures recommendations to address the issues and move forward.



# Contents

• Key Findings	4
• Cloud Goals	5
• Adoption Status	6
• Security Concerns	7
• FedRAMP	12
• Recommendations	16
• Methodology and Demographics	18

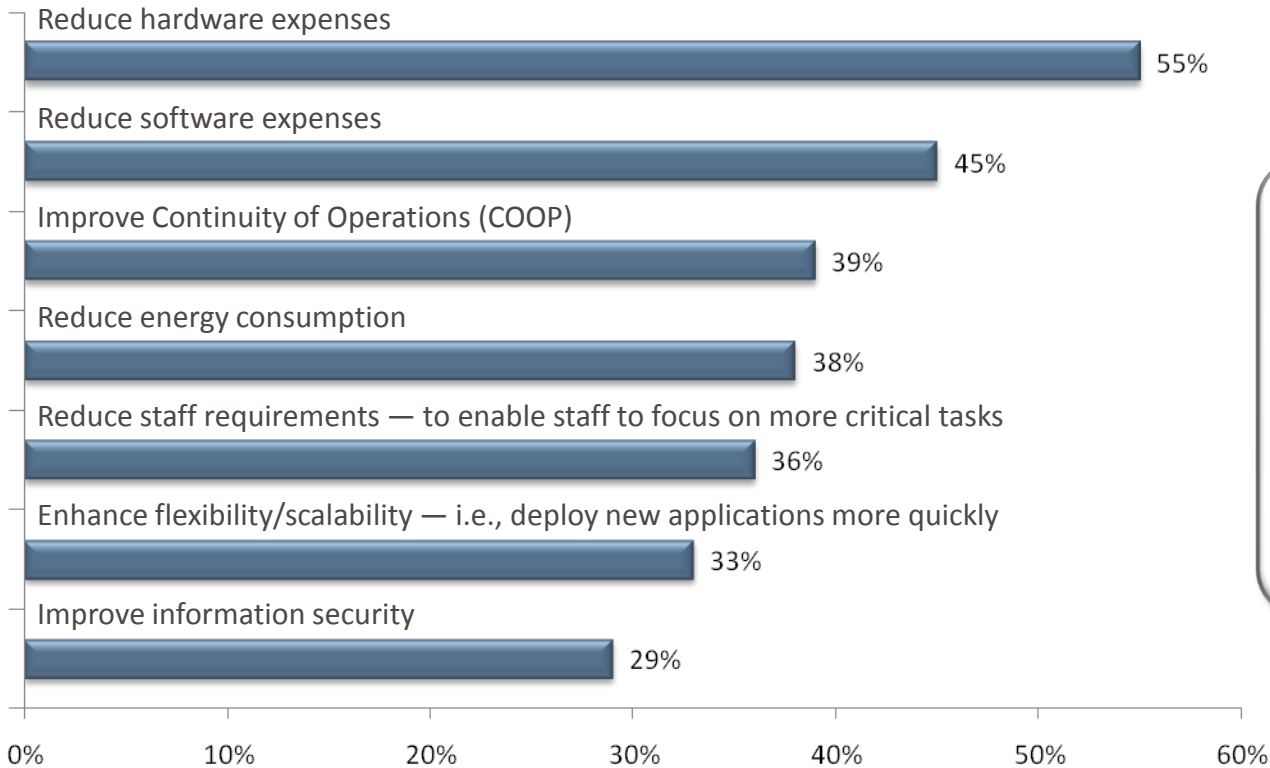
# Key Findings

- It's getting cloudy:
  - 23% of agencies have implemented cloud applications, platforms, and/or infrastructure; 35% are planning to implement
- To minimize risk, agencies moving to the cloud are favoring private clouds over public clouds:
  - 58% of agencies already in the cloud are using private, in-house clouds; 64% of those planning to implement cloud expect to use private, in-house clouds
- But, many still have concerns; 89% say data protection/privacy is their top issue. To improve security:
  - 80% say government should require encryption for data in the cloud
  - 70% say government should require data segmentation for data in the cloud
- Clear guidance on government cloud security standards will also help:
  - While government organizations expect management and oversight challenges, the majority believe a cloud security Certification and Accreditation (C&A) process will accelerate cloud adoption
  - Of those aware of Federal programs developing standards for secure government cloud computing, 46% specifically identify NIST or FedRAMP

# High Hopes

Agencies are looking to the cloud to save money, improve COOP, reduce energy consumption, and more

## Cloud Computing Goals:\*



Those who have implemented are **less likely** to cite improved Continuity of Operations as a goal than those who are planning – 44% vs. 54%

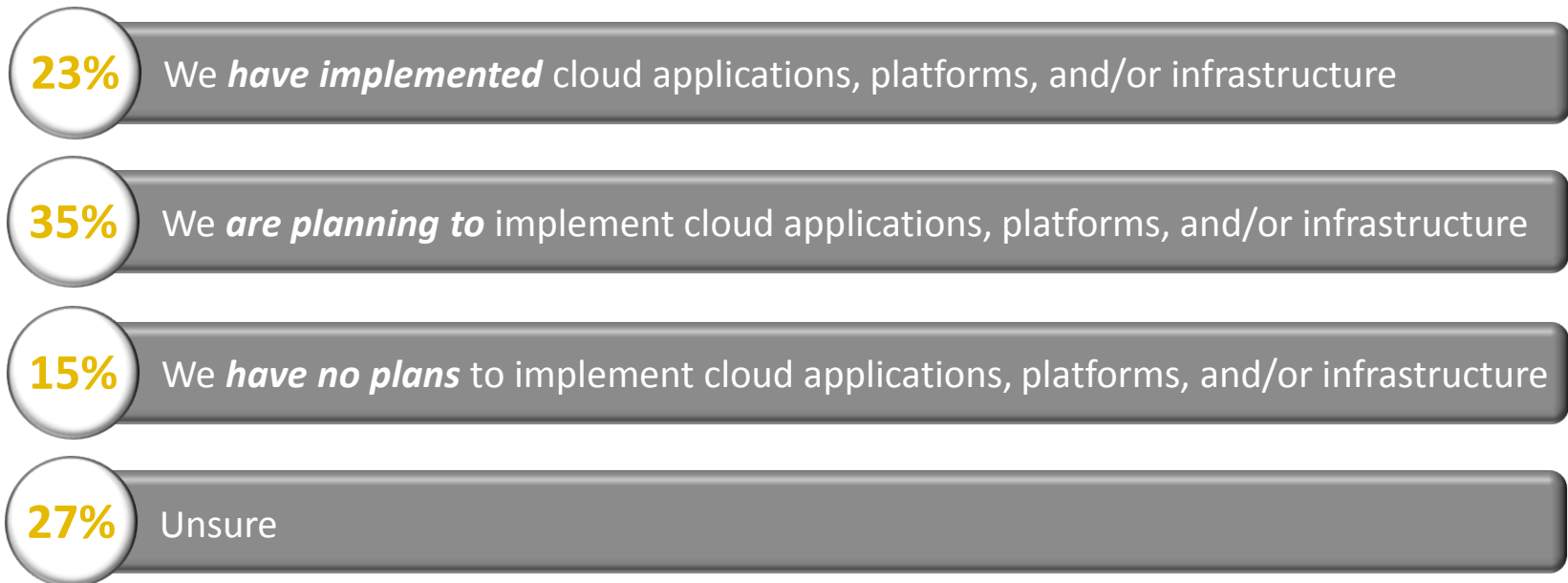
But, they are **more likely** to cite enhanced flexibility/ scalability as a goal – 44% vs. 35%

\*Respondents asked to check all that apply

# Proceeding With Caution

Nearly one quarter of agencies have implemented cloud applications, and 35% are in the planning stages

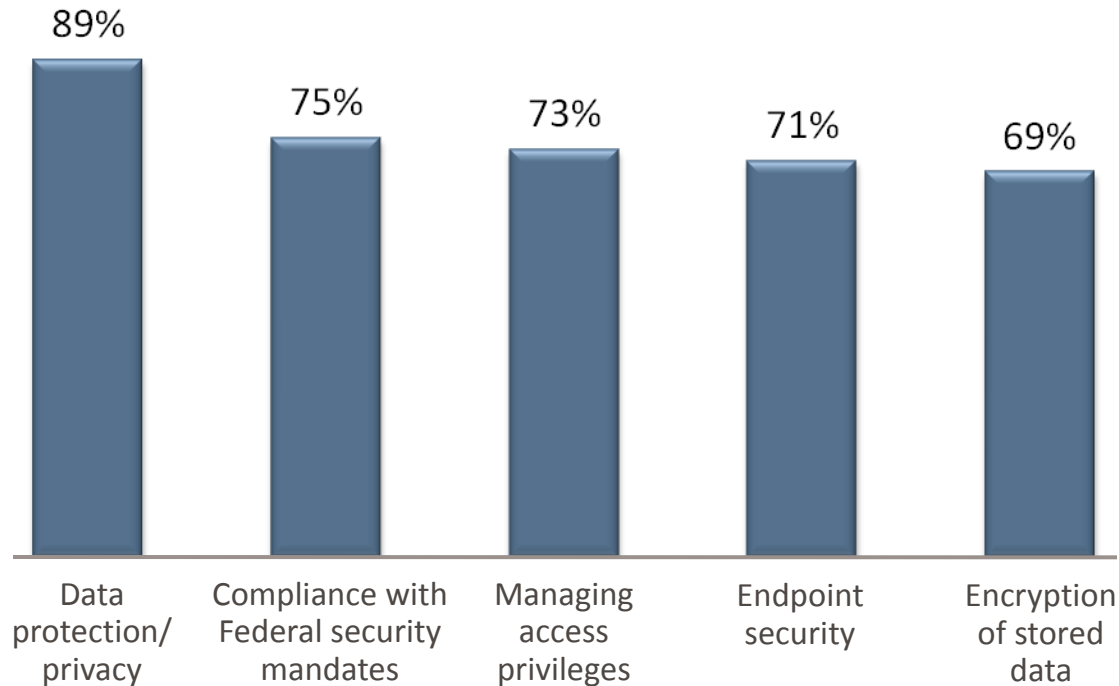
What is your organization's cloud computing status?



# Drilling Down: Cloud Security Concerns

Agencies cite data protection/privacy as their top cloud security concern

What are your top security concerns about cloud computing?\*

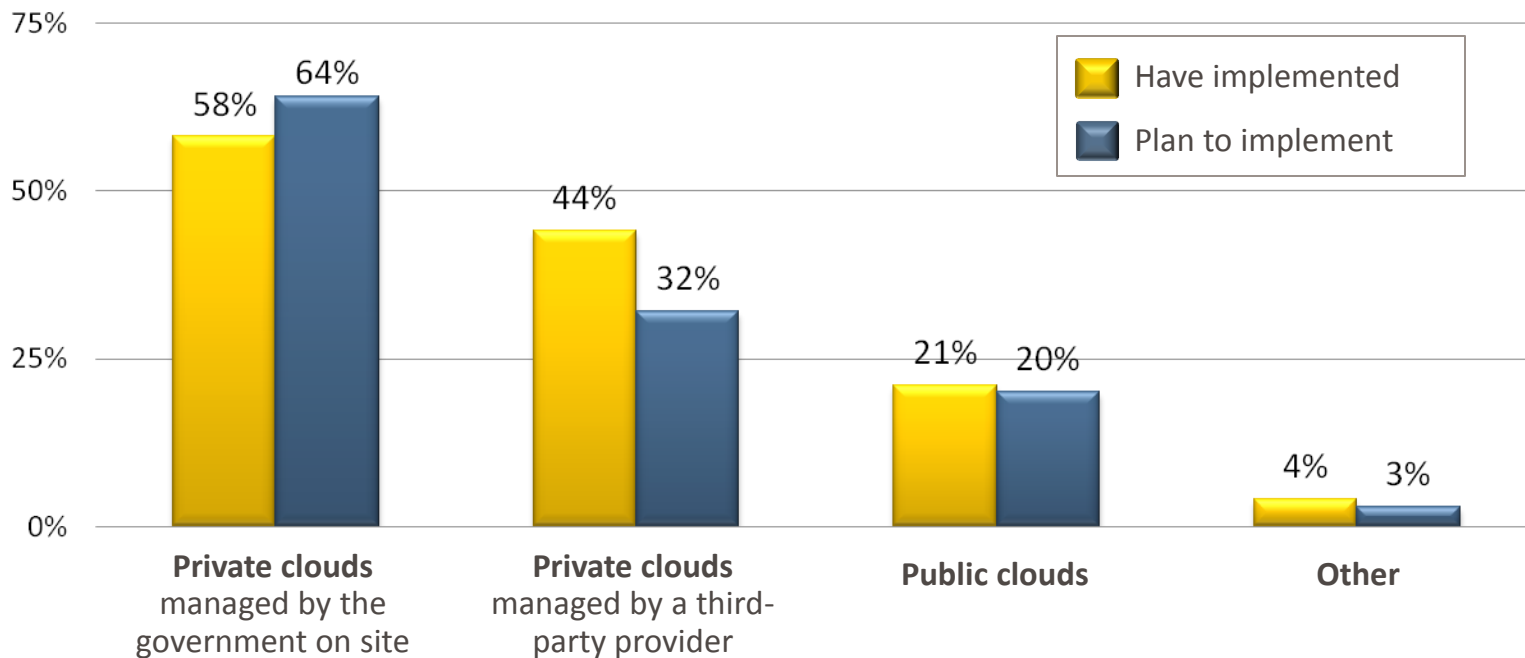


\*Percent who selected 8-10 on a scale of 1-10 with 1=not at all concerned, and 10=very concerned

# Gov IT Professionals Feel Safer in Private Clouds

Agencies implementing cloud computing favor private clouds – limiting security concerns by keeping data in house

What type of cloud have you implemented or do you plan to implement?\*

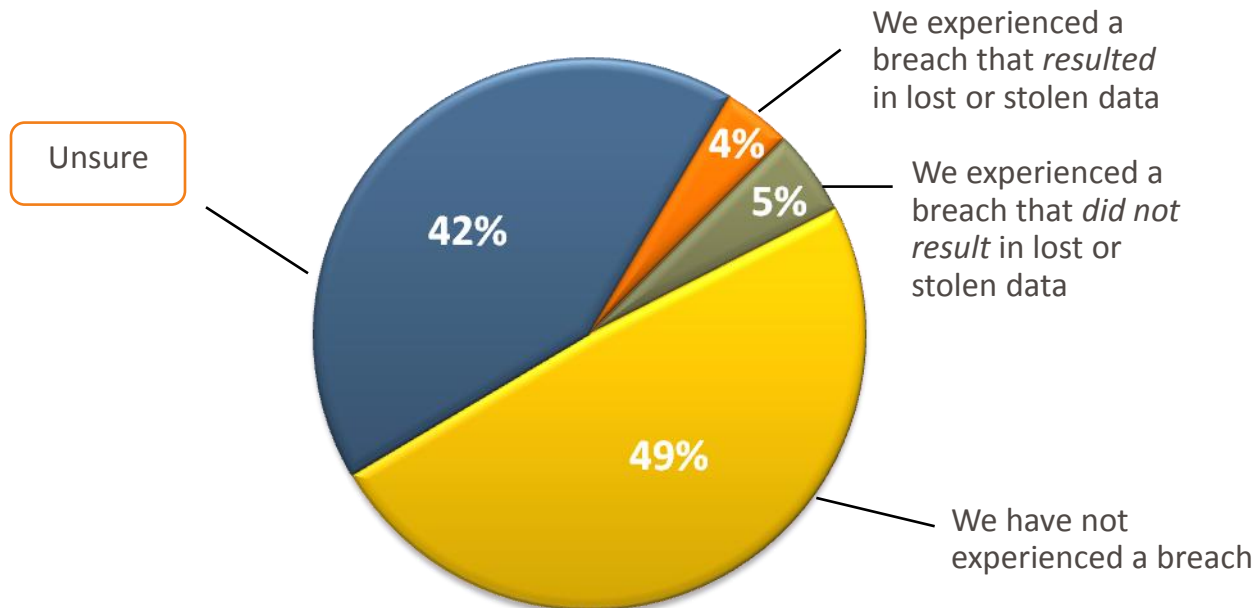


\*Respondents asked to select all that apply

# Taking the Leap Without a Safety Net

Almost half of those who have implemented cloud applications *do not know* if they have experienced a breach or attempted breach

Those who have implemented cloud applications: Have you experienced a data security breach or attempted breach?



# Call for Help

Nearly all agencies agree – government needs cloud security standards

91%

---

say they need clear guidance for government cloud information security standards



# Action Items

In addition to security guidance, agencies call for encryption and data segmentation requirements

## Most Important\* actions for government to secure the cloud:

<b>91%</b>	Issuing clear guidance for government cloud information security standards
<b>85%</b>	Establishing minimum security standards/criteria for industry partners with public cloud offerings
<b>80%</b>	Requiring data encryption
<b>74%</b>	Developing a Certification and Accreditation (C&A) process for cloud security
<b>70%</b>	Requiring data segmentation for cloud solutions (public or private)

\*selected 8, 9, or 10 on scale of 1-10

# Enter FedRAMP

## New program will deliver Federal cloud security standards

- Unified government-wide risk management program focused on large outsourced and multi-agency systems
- Provides security authorizations and continuous monitoring of shared systems
- Currently under development and deployment
- Aims to reduce duplicate efforts and security compliance expenditures, as well as encourage rapid acquisition timeframes, strong security oversight, and consistent integration with Federal government-wide security efforts\*

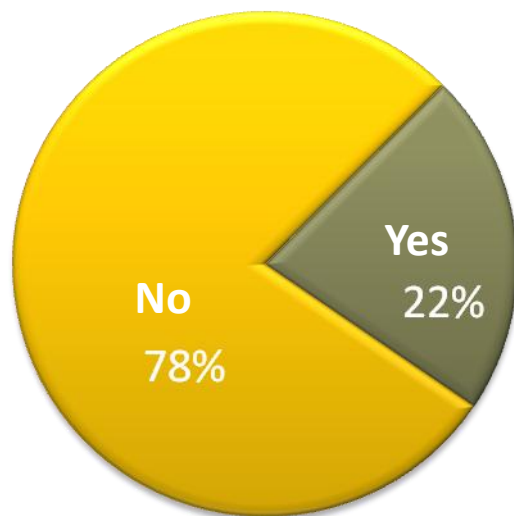


\*<http://www.cio.gov/pages.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP>

# FedWhat?

91% of agencies want guidance for government cloud information security standards; 22% say they are tracking government efforts to develop these standards

Are you tracking any Federal program(s) that are developing standards for secure government cloud computing?



Of those who say yes,

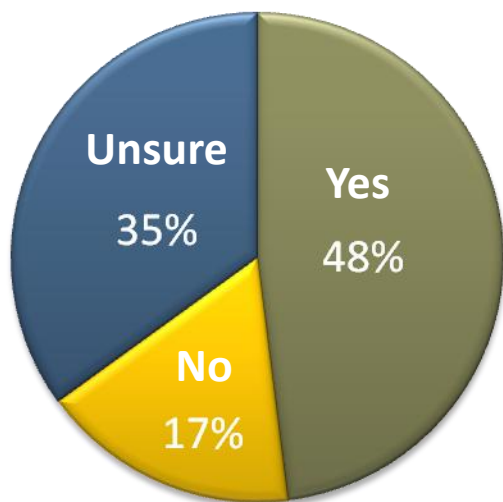
**46%**

specifically identify either NIST or FedRAMP

# Will FedRAMP Succeed?

Close to half of agencies believe a government-wide C&A process for cloud security is possible, but anticipate management and oversight as top barriers

Would agencies be able to successfully implement and manage a government-wide Certification and Accreditation (C&A) process for cloud security?



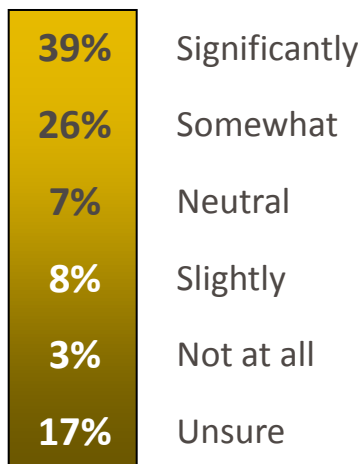
Certification and Accreditation (C&A) process for cloud security: Barriers*	
41%	<b>Management:</b> Identifying resources who can focus on the effort
40%	<b>Oversight:</b> Managing compliance
33%	<b>Technology:</b> Establishing the standards
23%	<b>Budget:</b> The cost to implement
15%	<b>Unsure</b>

\*Respondents asked to check all that apply

# The Road Ahead

If agencies can overcome the barriers, a majority believe a cloud security C&A process *would* accelerate cloud adoption

If implemented, will a clear Certification and Accreditation (C&A) process for cloud security accelerate cloud adoption in Federal agencies?




83%

believe it will take **three or more years** for the Federal government to implement a government-wide Certification and Accreditation (C&A) process for cloud security\*

\*Excluding those who are unsure and those who say it is not possible

# What Can We Do Today?

Those successfully implementing cloud computing offer advice on where to start:



“Understand information and its uses – focus on information security, not device security, as the priority.”

“Work as a whole within your agency and not individually.”

“Ensure all requirements for security are in procurement.”

“Ask questions of the vendor, make sure you have protection.”

“Protect the data first. Control the SLA.”

# Our Take...

## ✓ Cloud is Real

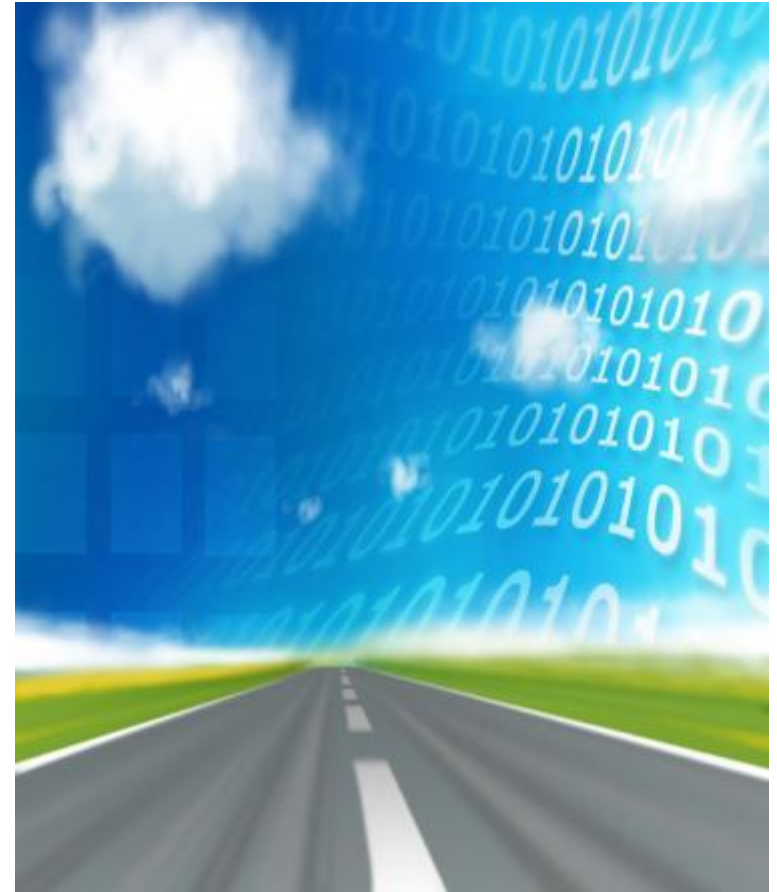
- Almost one quarter of respondents have already made the leap, and another 35% plan to – it's not coming; it's already here

## ✓ Security Double Trouble

- Security/privacy concerns still a major barrier to entry
- Lack of understanding/awareness of breaches and vulnerabilities

## ✓ FedRAMP Roadblock

- Vast majority looking for guidance on standards, but many are unaware of work in progress – major education opportunity for OMB



# Methodology and Demographics

**Symantec** commissioned a survey of **202 Federal government IT decision makers** at the 2010 Symantec Government Symposium in June 2010 (conducted by O’Keeffe & Company). The total sample size equates to a margin of error of +/- 6.87% at 95% confidence for the group.

## Organization Type

82%	Federal Government
18%	Systems Integrator

## Cloud Status

**23%** have implemented cloud computing solutions



# Thank you!

**GiGi Schumm**

[gigi\\_schumm@symantec.com](mailto:gigi_schumm@symantec.com)

(703) 668-8769

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.