Cloud Computing Security for

DoD / Governments (U.S.)

7th Annual IT Security Automation Conference

October 31 – November 2, 2011 • Crystal City, Virginia
Hyatt Regency

Dr. Antonio Mauro, PhD
info@antoniomauro.it

November 2011

- **NIST Cloud Computing Standards Roadmap**
  - Document: NIST CCSRWG – 092 - First Edition - July 5, 2011
  - Special Publication 500-291

- **NIST Cloud Computing Reference Architecture**
  - Special Publication 500-292 – September 2011

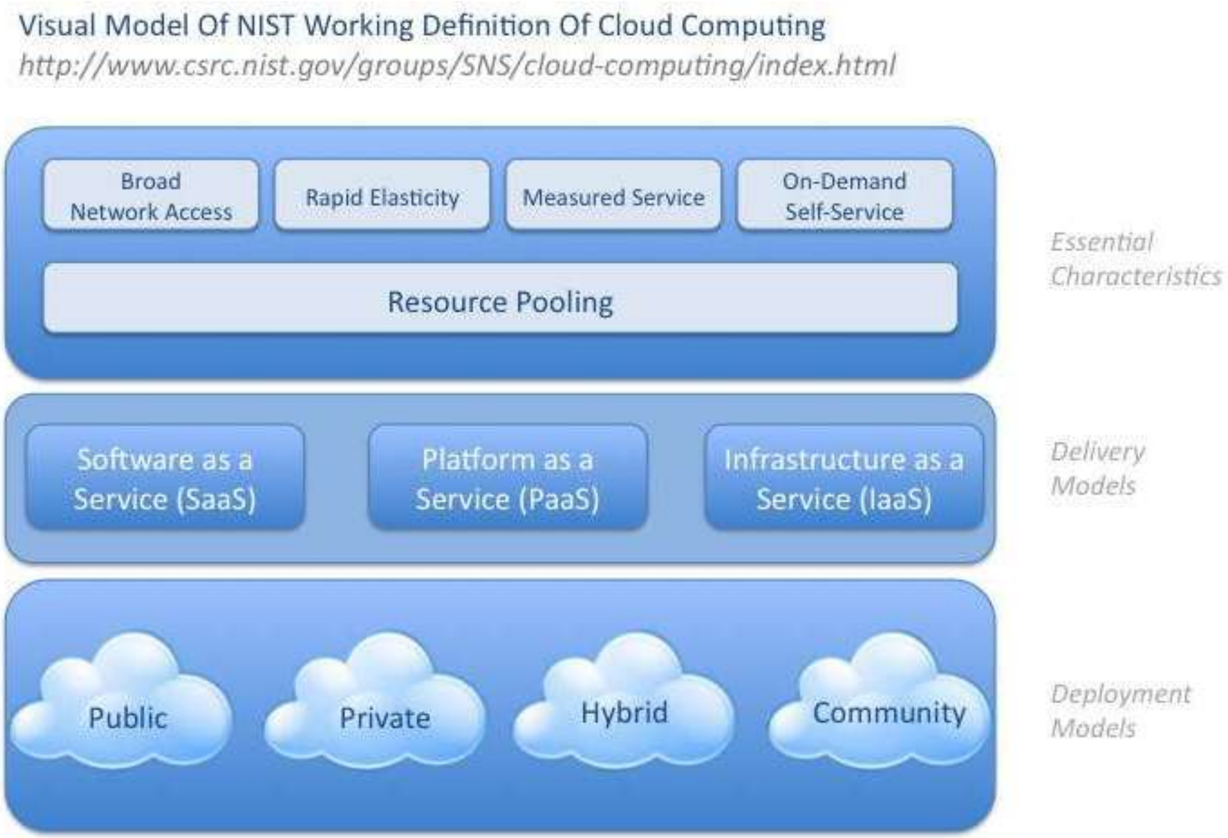
- **NIST US Government Cloud Computing Technology Roadmap - Volume I – Release 1.0 (Draft)**
  - Special Publication 500-293 - (Draft) - November 2011
  - High-Priority Requirements to Further USG Agency Cloud Computing Adoption

- **NIST US Government Cloud Computing Technology Roadmap - Volume II – Release 1.0 (Draft)**
  - Special Publication 500-293 - (Draft) - November 2011
  - Useful Information for Cloud Adopters

- **NIST US Government Cloud Computing Technology Roadmap - Volume III – Release 1.0 (Draft)**
  - Special Publication 500-293 - (Draft) - November 2011
  - Technical Considerations for USG Cloud Computing Deployment Decisions

Cloud Computing?

- **Essential Characteristics**
  - Resource Pooling
  - Broad Network Access
  - Rapid Elesticity
  - Measured Service
  - On-demand Self-Service
- **3 delivery Models**
- **4 deployment models**



Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

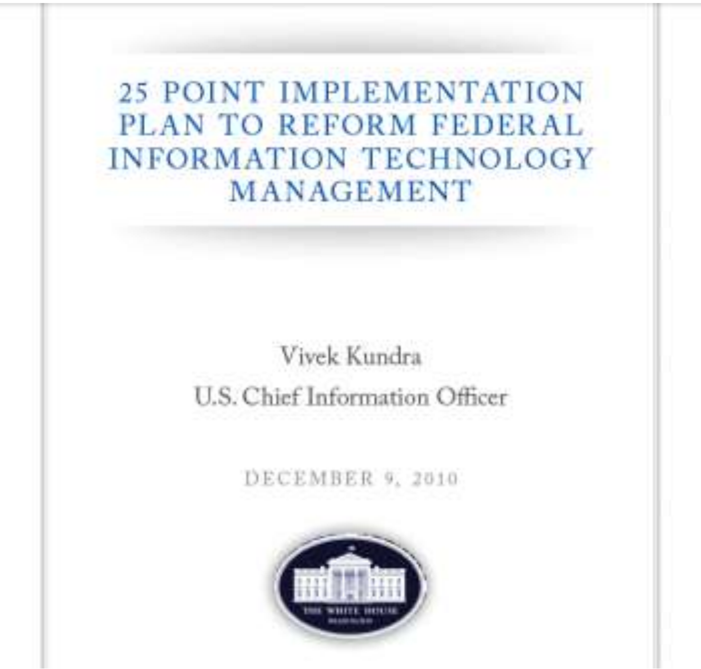
Why Cloud Computing?

- **ICD 501**
  - President Obama: “Reduce Cost, Increase efficiency and Lower IT operation costs”
  - SOLUTION: **CLOUD COMPUTING**
  - Office of Management and Budget (OMB): “cloud first”

Trasparency – Partecipation – Collaboration

25 Point Implementation

25 POINT IMPLEMENTATION PLAN TO REFORM FEDERAL INFORMATION TECHNOLOGY MANAGEMENT



25 POINT IMPLEMENTATION PLAN TO REFORM FEDERAL INFORMATION TECHNOLOGY MANAGEMENT

Vivek Kundra

U.S. Chief Information Officer

DECEMBER 9, 2010

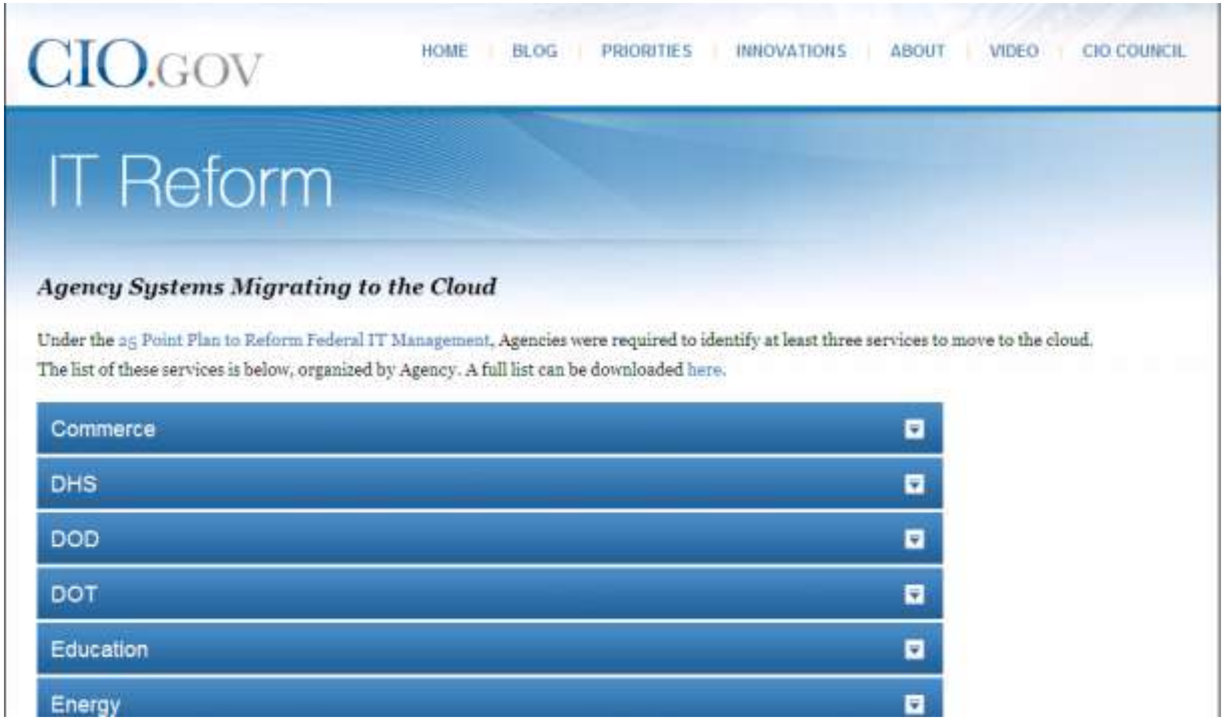
http://www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf

Cloud Computing Deadlines

- **Febrary 2011**: cloud first Strategy Published
- **May 2011**: Three “must move” services identified for migration to the Cloud
- **May 2012**: First “must move” service migrated to the Cloud
- **November 2012**: “must move” services 2&3 migrated
- **FY2015:** 800 data centers

Agency Systems Migrating to the Cloud

http://www.cio.gov/itreform/cloud_migrations.cfm



Agency Systems Migrating to the Cloud

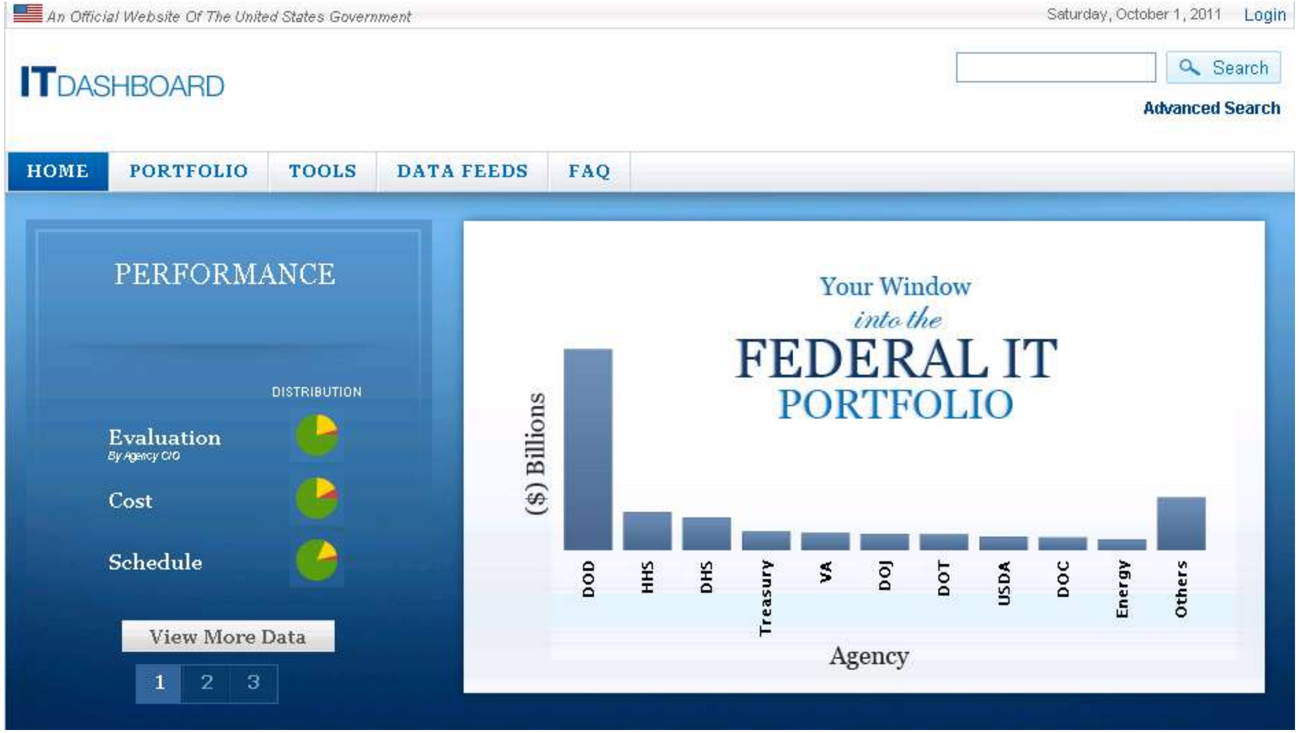
Under the 25 Point Plan to Reform Federal IT Management, Agencies were required to identify at least three services to move to the cloud. The list of these services is below, organized by Agency. A full list can be downloaded here.

- Commerce
- DHS
- DOD
- DOT
- Education
- Energy

IT Dashboard

IT Dashboard for Federal IT

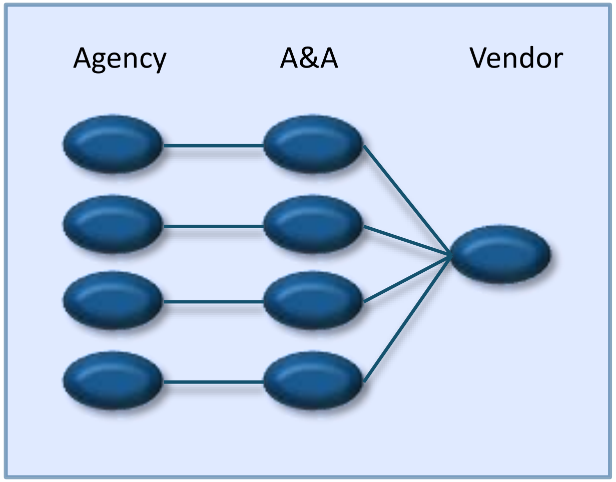
http://www.itdashboard.gov/

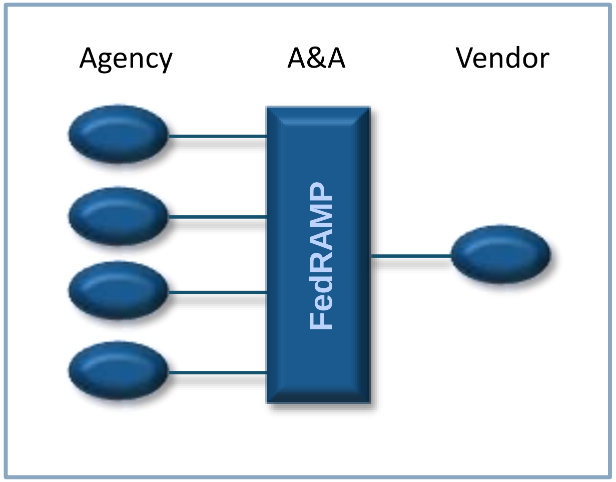


Federal Risk and Authorization Management Program (FedRAMP)

- **Reduce redundant processes** across government by providing security **authorizations and continuous monitoring of cloud systems**
- Established to provide a **standard approach** to assessing and authorizing cloud computing services and products

Details of Federal Risk and Authorization Management Program (FedRAMP)





BEFORE

- Duplicative risk management effort
- Incompatible requirements
- Potential for inconsistent application & interpretation of Federal security requirements
- Redundant agency security certification costs

AFTER

- Unified Risk management & associated cost savings
- Inter-Agency vetted & compatible requirements using a shared cloud service
- Effective & consistent assessment of cloud services

FedRAMP Authorizing Officials (AO)

The FedRAMP Authorizing Officials (AO) **must authorize**, in writing, all **cloud computing systems before they go into operational** service for government interest.

A **Service Provider's cloud computing** systems **must be authorized/reauthorized** at least every **three (3) years** or whenever there is a significant change to the system's security posture in accordance with NIST SP 800-37 R1

FedRAMP Guidance

1. **Categorize Cloud System:** (FIPS 199 / NIST Special Publications 800-30, 800-39, 800-59, 800-60)
2. **Select Security Controls:** (FIPS Publications 199, 200; NIST Special Publications 800-30, 800-53 R3, FedRAMP security control baseline)
3. **Authorization Request:** (FedRAMP primary Authorization Request letter, FedRAMP secondary authorization request letter
4. **Implement Controls:** (FedRAMP control tailoring workbook; Center for Internet Security (CIS); United States Government Configuration Baseline (USGCB); FIPS Publication 200; NIST Special Publications 800-30, 800-53 R3, 800-53A R1)

FedRAMP Guidance

5. **Access Controls:** (FedRAMP Test Procedures: Center for Internet Security (CIS); United States Government Configuration Baseline (USGCB); NIST Special Publications 800-53A R1)
6. **Authorize Cloud System:** OMB Memorandum 02-01; NIST Special Publications 800-30, 800-53A R1)
7. **Continuous Monitoring:** FedRAMP Test Procedures; NIST Special Publications 800-30, 800-53A R1, 800-37 R1)

FISMA - FCCI - GSA

Federal Information Security Management Act (FISMA)

- ***Protecting the Nation's Critical Information Infrastructure;***
- *To produce several **key security standards and guidelines** required by Congressional legislation*
- *Promote the development of key security standards and guidelines to support the implementation of and compliance*

Federal Cloud Computing Initiative (FCCI)

- *Implementing cloud computing solution for Federal Government to **increase the operational efficiencies**, **optimize common services and solutions** across organizational boundaries, and enable transparent, collaborative, and participatory government*

General Services Administration (GSA)

- *For economics aspect*

Standard Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)

- *Goal is to facilitate the development of cloud computing standards.*
- ***Increase the confidence in cloud computing adoption during the interim period before cloud computing standards are formalized.***

ISIMC

Information Security and Identity Management Committee (ISIMC)

Provides a consensus based forum to support the Federal CIO Council (FCIOC) that enables Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) to collaborate on:

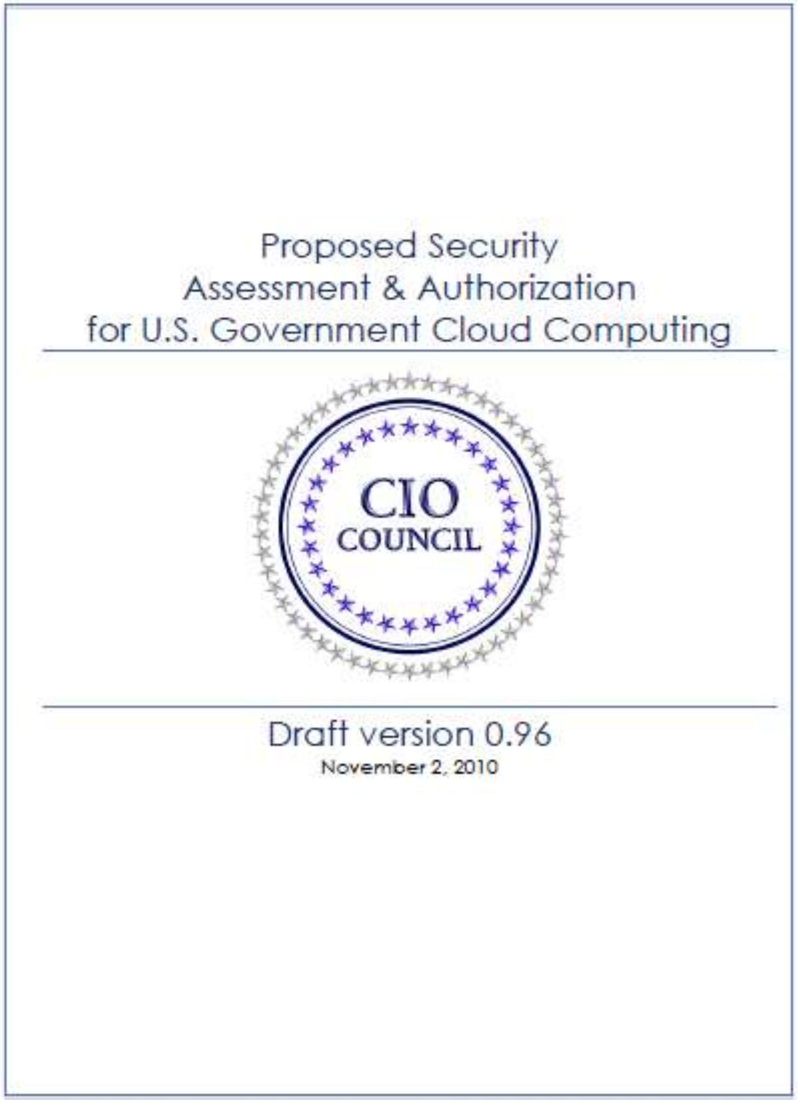
identifying high priority security and identity management initiatives;

developing recommendations for policies, procedures, and standards to address those initiatives that enhance the security posture and protection afforded to Federal Government networks, information, and information systems.

Indipendent Verification and Validation (IV&V)

- Indipendent Verification and Validation is going to be an integral component to a **successful implementation of FedRAMP**
- Include:
  - Scheduled annual assessments of the system security documentations;
  - Verification of testing procedures;
  - Validation of testing tools and assessments;
  - Validation of assessments methodologies employed by the CSP and independent assessors;
  - Verification of CSP continuous monitoring program and validation of CSP risk level determination criteria
- **FISMA, FedRAMP and IV&V performing penetration testing**

CIO Council



Proposed Security
Assessment & Authorization
for U.S. Government Cloud Computing

CIO COUNCIL

Draft version 0.96
November 2, 2010

- **Chapter 1:** Cloud Computing Security Requirement Baseline
- **Chapter 2:** Continuous Monitoring
- **Chapter 3:** Potential Assessment & Authorization Approach

U.S. Department of Homeland Security

Department of Homeland Security

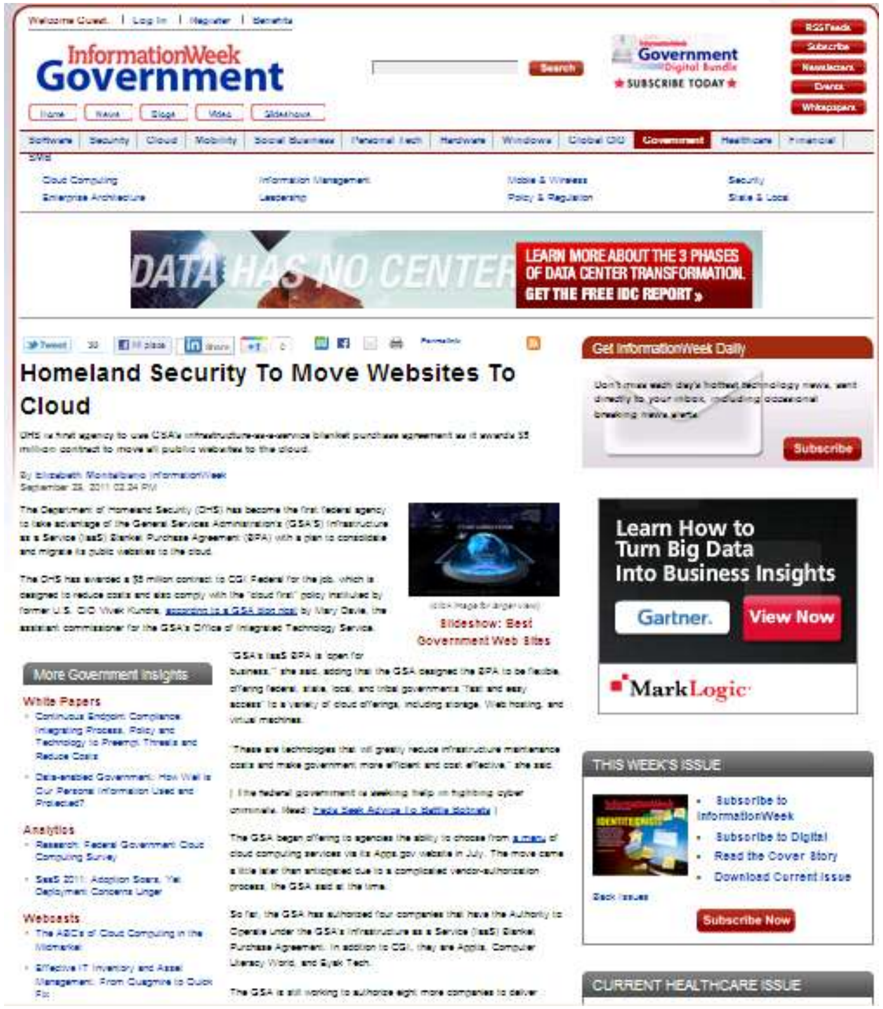
National Cyber Security Division

Cloud Computing from the Security Perspective:
A Primer for Federal IT Managers

DHS FIRST AGENCY

Homeland Security To Move Websites To Cloud

DHS is first agency to use GSA's infrastructure-as-a-service blanket purchase agreement as it awards $5 million contract to move all public websites to the cloud



Homeland Security To Move Websites To Cloud

DHS is first agency to use GSA's infrastructure-as-a-service blanket purchase agreement as it awards $5 million contract to move all public websites to the cloud.

By Elizabeth Montalbano InformationWeek
September 28, 2011 02:24 PM

The Department of Homeland Security (DHS) has become the first federal agency to take advantage of the General Services Administration's (GSA'S) Infrastructure as a Service (IaaS) Blanket Purchase Agreement (BPA) with a plan to consolidate and migrate its public websites to the cloud.

The DHS has awarded a $5 million contract to CGI Federal for the job, which is designed to reduce costs and also comply with the "cloud first" policy instituted by former U.S. CIO Vivek Kundra, according to a GSA blog post by Mary Davie, the assistant commissioner for the GSA's Office of Integrated Technology Service.

(click image for larger view)

Slideshow: Best Government Web Sites

"GSA's IaaS BPA is 'open for business,'" she said, adding that the GSA designed the BPA to be flexible, offering federal, state, local, and tribal governments "fast and easy access" to a variety of cloud offerings, including storage, Web hosting, and virtual machines.

"These are technologies that will greatly reduce infrastructure maintenance costs and make government more efficient and cost effective," she said.

| The federal government is seeking help in fighting cyber criminals. Read: Feds Seek Advice To Battle Botnets |

The GSA began offering to agencies the ability to choose from a menu of cloud computing services via its Apps.gov website in July. The move came a little later than anticipated due to a complicated vendor-authorization process, the GSA said at the time.

So far, the GSA has authorized four companies that have the Authority to Operate under the GSA's Infrastructure as a Service (IaaS) Blanket Purchase Agreement. In addition to CGI, they are Apptis, Computer Literacy World, and Eyak Tech.

The GSA is still working to authorize eight more companies to deliver

More Government Insights

White Papers
- Continuous Endpoint Compliance: Integrating Process, Policy and Technology to Preempt Threats and Reduce Costs
- Data-enabled Government: How Well is Our Personal Information Used and Protected?

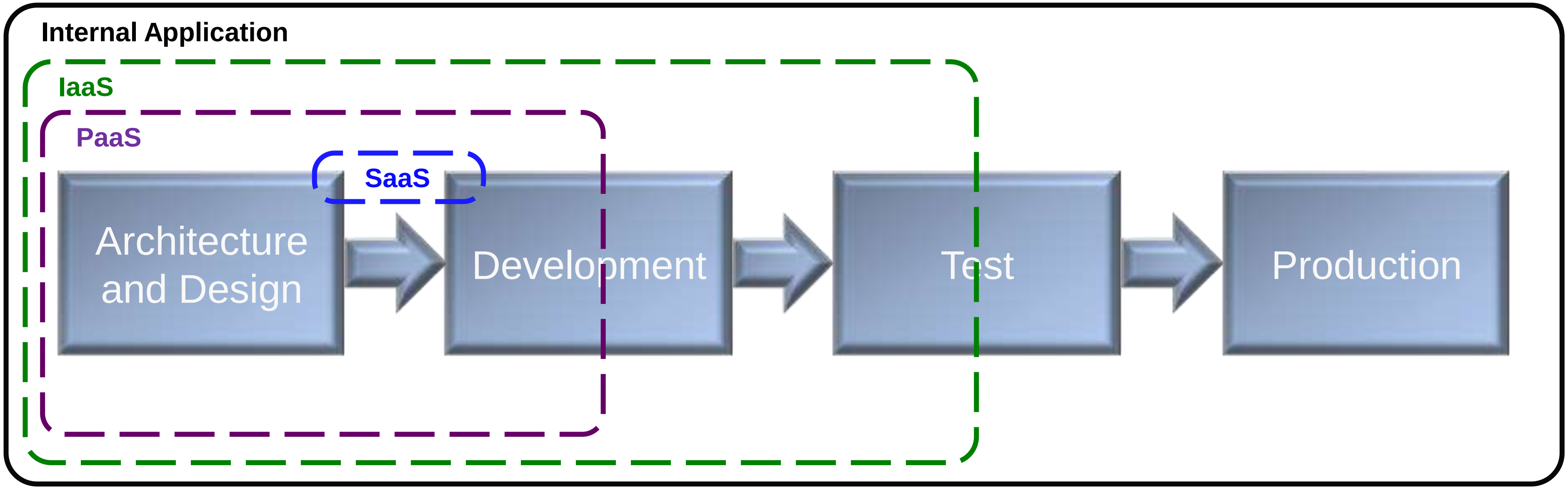
Analytics
- Research: Federal Government Cloud Computing Survey
- SaaS 2011: Adoption Soars, Yet Deployment Concerns Linger

Webcasts
- The ABCs of Cloud Computing in the Midmarket
- Effective IT Inventory and Asset Management: From Quagmire to Quick Fix

Don't miss each day's hottest technology news, sent directly to your inbox, including occasional breaking news alerts.

Cloud Computing

view of Information Assurance Concerns and Opportunities



NSA move Cloud Computing

US Intelligence Community Is Moving To The Cloud!

James R. Clapper Jr. - Director of National Intelligence

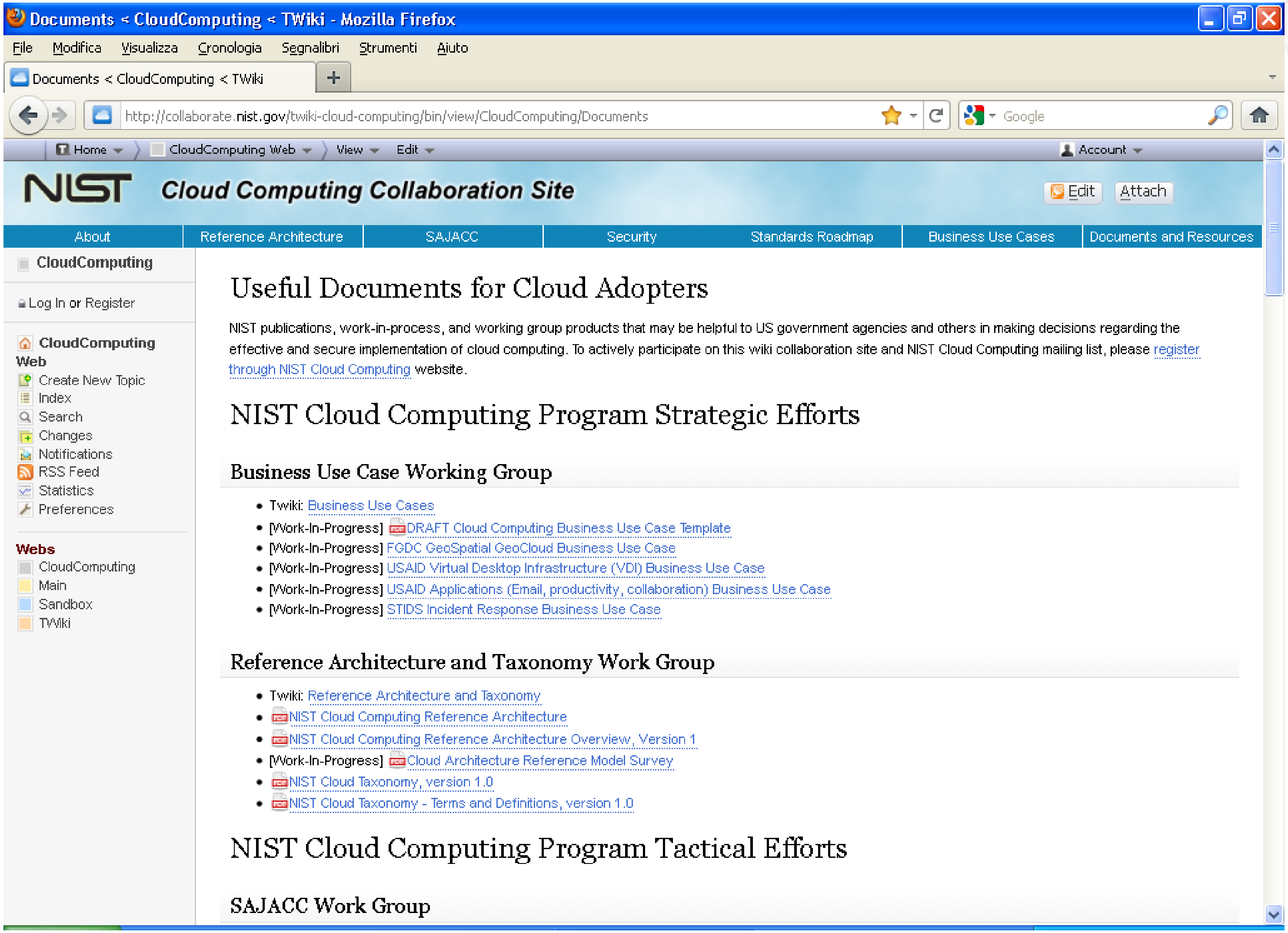
The biggest portion of those cuts, spread across 10 years, will come from anything labeled information technology….**Cloud computing — while not a panacea — makes possible much of those savings**.”

Director National Security Agency and head of Cyber Command General Keith Alexander echoed the DNI’s comment stating that NSA operations will move to the cloud by the end of this year.

“**Moving to the cloud, will provide huge savings of 30 percent to 40 percent savings in the NSA’s IT budget…. Moving to the cloud enables better security in some respects, for example, because all systems receive all security patches at the same time. It also removes updating systems from the hands of a large number of humans, making it more certain they will happen.”**

NIST Cloud Computing Collaboration Site

http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/Documents



Useful Documents for Cloud Adopters

NIST publications, work-in-process, and working group products that may be helpful to US government agencies and others in making decisions regarding the effective and secure implementation of cloud computing. To actively participate on this wiki collaboration site and NIST Cloud Computing mailing list, please register through NIST Cloud Computing website.

NIST Cloud Computing Program Strategic Efforts

Business Use Case Working Group

- Twiki: Business Use Cases
- [Work-In-Progress] DRAFT Cloud Computing Business Use Case Template
- [Work-In-Progress] FGDC GeoSpatial GeoCloud Business Use Case
- [Work-In-Progress] USAID Virtual Desktop Infrastructure (VDI) Business Use Case
- [Work-In-Progress] USAID Applications (Email, productivity, collaboration) Business Use Case
- [Work-In-Progress] STIDS Incident Response Business Use Case

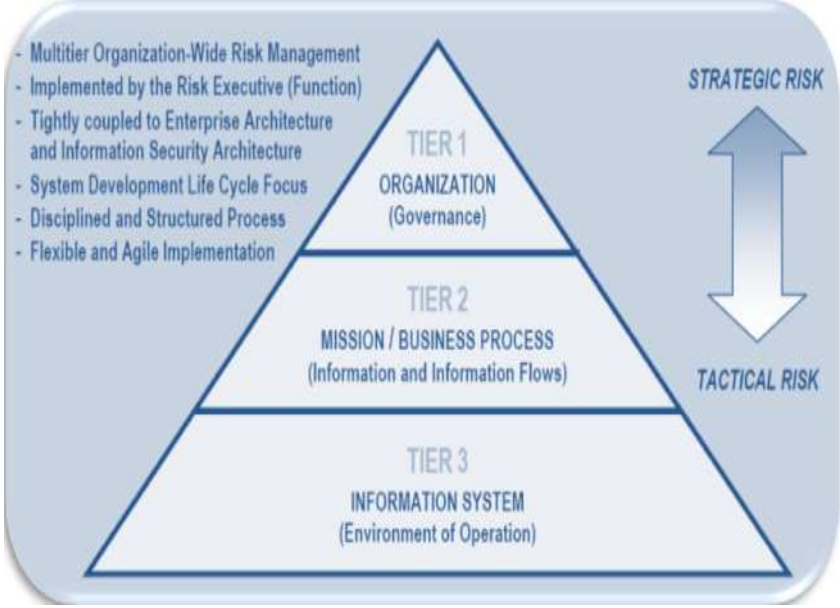
Reference Architecture and Taxonomy Work Group

- Twiki: Reference Architecture and Taxonomy
- NIST Cloud Computing Reference Architecture
- NIST Cloud Computing Reference Architecture Overview, Version 1
- [Work-In-Progress] Cloud Architecture Reference Model Survey
- NIST Cloud Taxonomy, version 1.0
- NIST Cloud Taxonomy - Terms and Definitions, version 1.0

NIST Cloud Computing Program Tactical Efforts

SAJACC Work Group

RISKS by NIST



- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation

TIER 1
ORGANIZATION
(Governance)

TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)

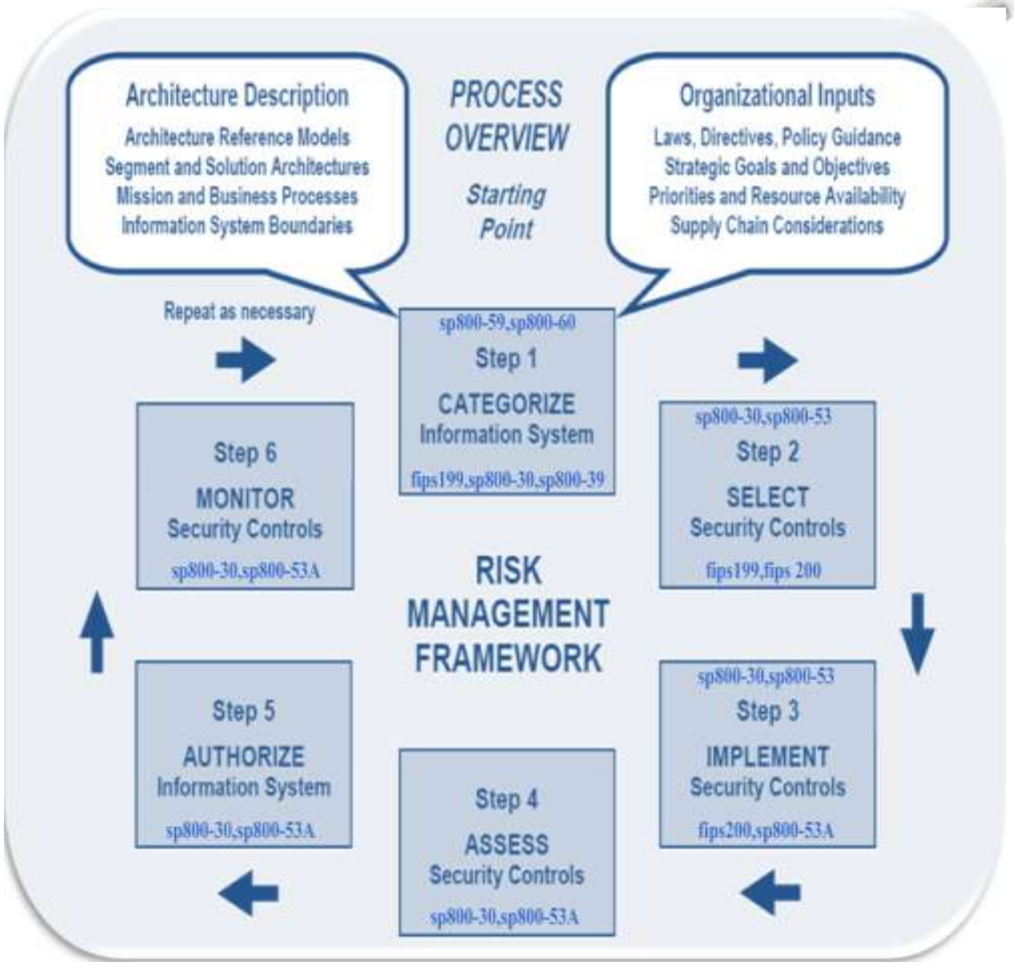
TIER 3
INFORMATION SYSTEM
(Environment of Operation)

STRATEGIC RISK

TACTICAL RISK

NIST

Tiered Risk Management Approach



Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

PROCESS OVERVIEW

Starting Point

Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Repeat as necessary

sp800-59,sp800-60
Step 1
CATEGORIZE
Information System
fips199,sp800-30,sp800-39

sp800-30,sp800-53
Step 2
SELECT
Security Controls
fips199,fips 200

sp800-30,sp800-53
Step 3
IMPLEMENT
Security Controls
fips200,sp800-53A

Step 4
ASSESS
Security Controls
sp800-30,sp800-53A

Step 5
AUTHORIZE
Information System
sp800-30,sp800-53A

Step 6
MONITOR
Security Controls
sp800-30,sp800-53A

RISK MANAGEMENT FRAMEWORK

NIST

Risk Management Framework

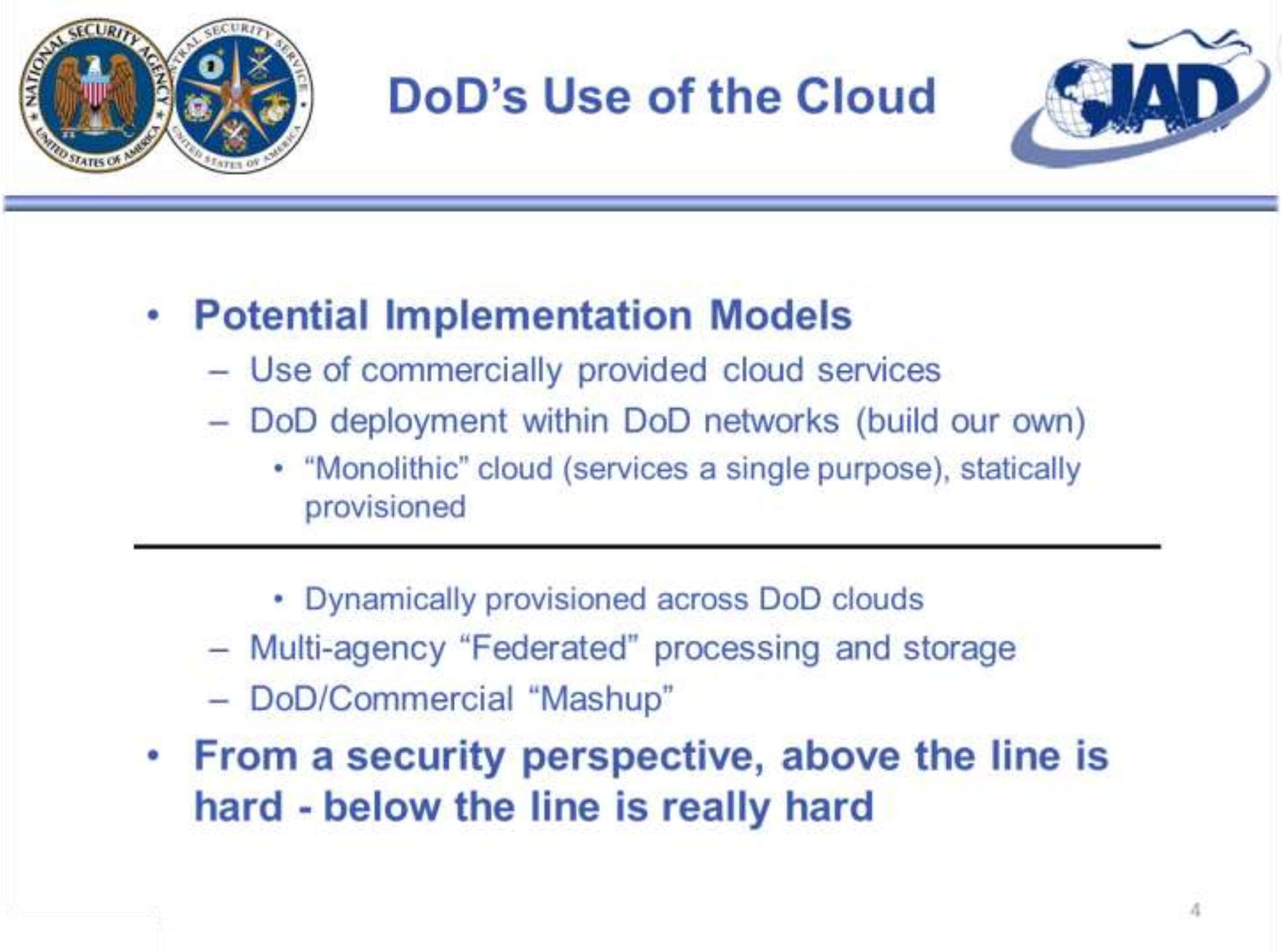
U.S. Use Cases

Federal, Defense, State and Other Cloud Initiatives

Apps.gov

Apps.gov, which went live, Sept. 15, 2009, is an online storefront for federal agencies to quickly browse and **purchase cloud-based IT services for productivity**, **collaboration, and efficiency.** By consolidating available services, Apps.gov is intended to be a one-stop source for cloud services. GSA conducted the competitive bidding process to commercially obtain **IaaS services for cloud storage services, virtual machines, and cloud web hosting**. In a reflection of the commoditized nature of cloud computing, government agencies will be able to procure IaaS units of service on a fixed-price basis.

DoD’s Use of the Cloud



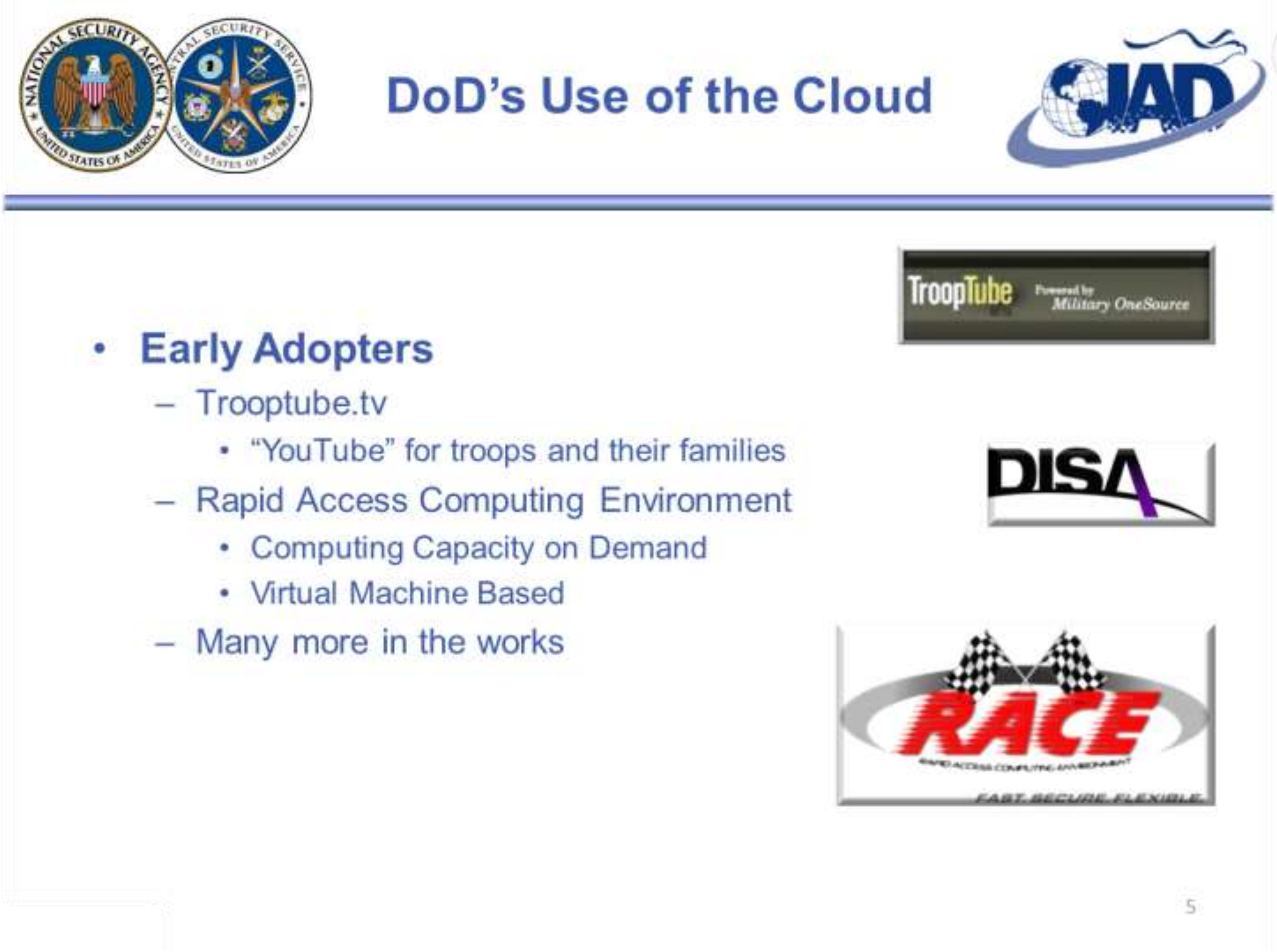
DoD’s Use of the Cloud

- **Potential Implementation Models**
  - Use of commercially provided cloud services
  - DoD deployment within DoD networks (build our own)
    - “Monolithic” cloud (services a single purpose), statically provisioned

---

    - Dynamically provisioned across DoD clouds
  - Multi-agency “Federated” processing and storage
  - DoD/Commercial “Mashup”
- **From a security perspective, above the line is hard - below the line is really hard**

DoD’s Use of the Cloud



NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
CENTRAL SECURITY SERVICE
UNITED STATES OF AMERICA
IAD
TroopTube Powered by Military OneSource
DISA
RACE
RAPID ACCESS COMPUTING ENVIRONMENT
FAST. SECURE. FLEXIBLE.

DoD’s Use of the Cloud

- **Early Adopters**
  - Trooptube.tv
    - “YouTube” for troops and their families
  - Rapid Access Computing Environment
    - Computing Capacity on Demand
    - Virtual Machine Based
  - Many more in the works

NASA

National Aeronautics and Space Administration

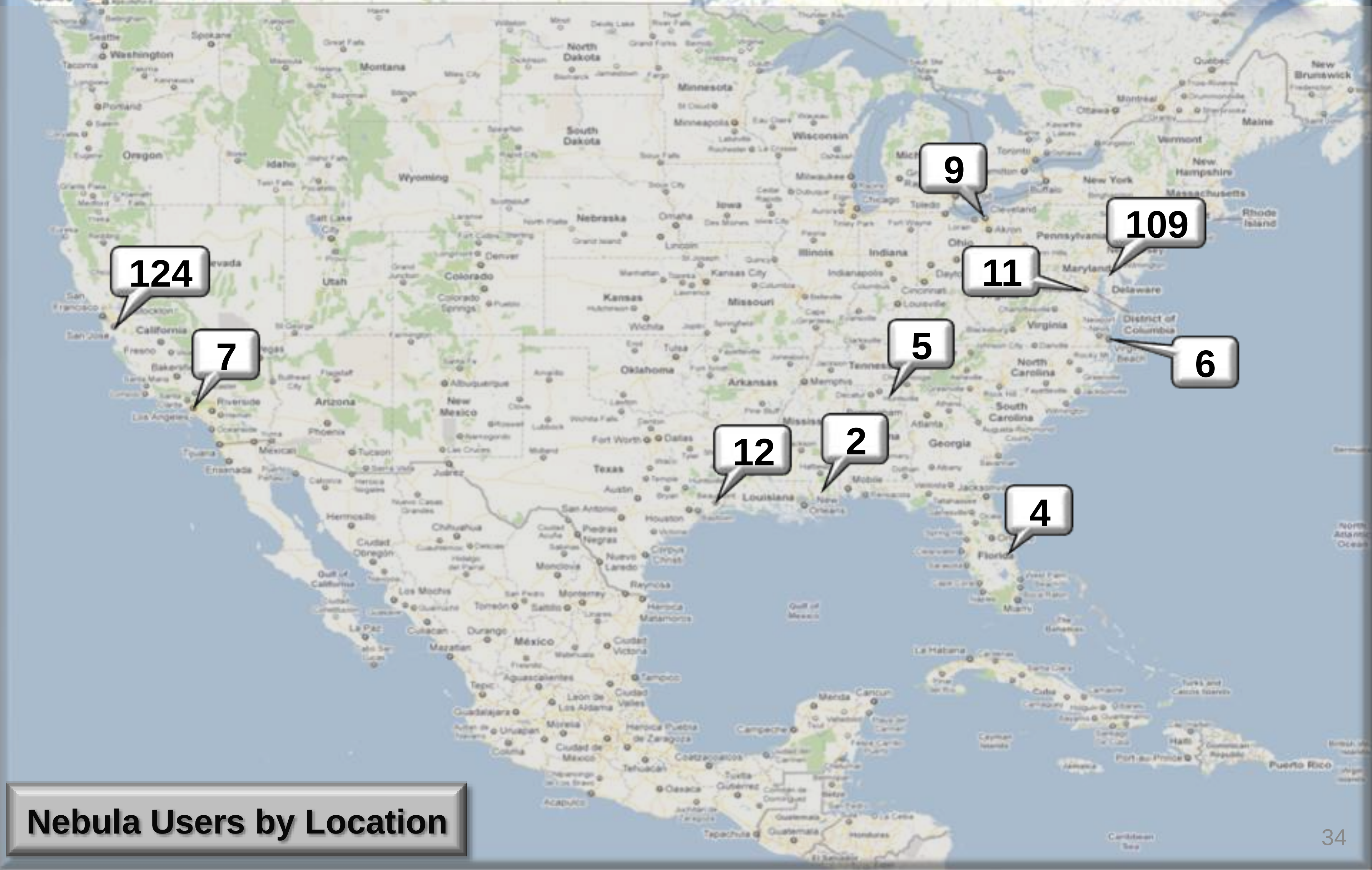
One of NASA's first cloud computing initiatives, called **Nebula, is up and running and could be used in support of the agency's space missions and to give Earth-based observers greater participation in the space program**. Chris Kemp, CIO of NASA's Ames Research Center, mentioned Nebula for the first time recently at the Federal Information Technology on a Budget Forum in Washington, DC. NASA describes Nebula as a cloud computing environment that integrates open source components into a seamless, self-service platform. **Nebula can be used for the rapid development of policy-compliant, secure Web apps, NASA says, adding that it will be used to support education, public outreach, collaboration, and mission support.**

NASA - NEBULA

NEBULA Cloud Computing Platform 2010

NEBULA Cloud Computing Platform 2010

NASA - NEBULA



Nebula Users by Location

Example

Defense Information Systems Agency

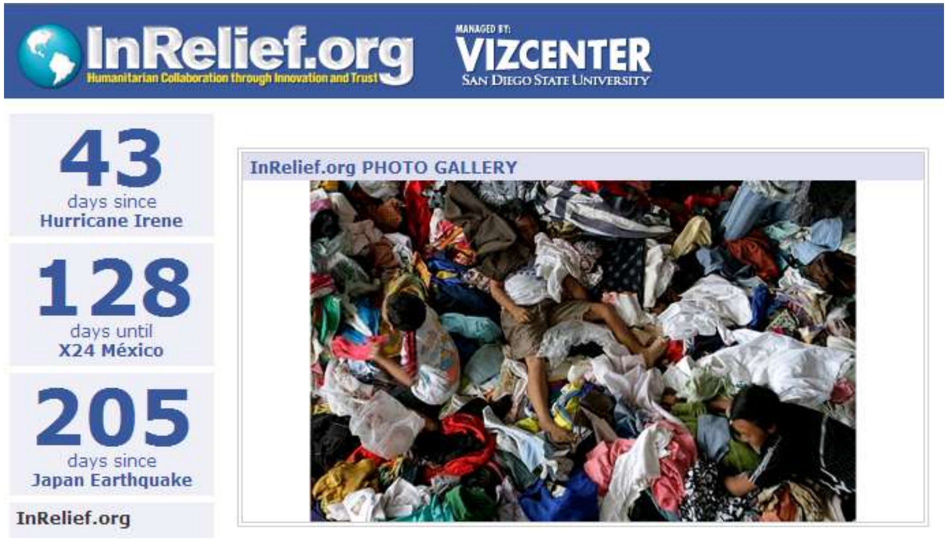
The Defense Information Systems Agency (DISA) is involved in one of few examples of cloud computing in government. In October, the agency launched the **Rapid Access Computing Environment (RACE),** which allows Defense IT developers to test applications before they go live. **RACE allows users to provision a server within 24 hours inside one of DISA's data centers, using a charge card**. The agency plans to offer RACE on its **classified network by the end of the year**. The applications are stored at a DISA data center, and customers pay the agency only for the computing resources they need when they need them. Among the benefits it hopes to achieve are lower IT costs, pay-per-use accounting, accelerated deployment of mainframe -class systems, data center standardization, and flexibility in scaling up and down

Example – US NAVY

InRelief.org’s mission is to **increase the velocity of the response during Humanitarian Assistance and Disaster Relief** (HADR) events by connecting military/civilian organizations, disseminating data freely over the internet, and providing the collaborative tools to expedite the sharing of **critical information**.

https://sites.google.com/a/inrelief.org/about/Home

http://www.inrelief.org/



InRelief.org
Humanitarian Collaboration through Innovation and Trust

MANAGED BY:
VIZCENTER
San Diego State University

43
days since
Hurricane Irene

128
days until
X24 México

205
days since
Japan Earthquake

InRelief.org

InRelief.org PHOTO GALLERY

Example

Army Deploys First DoD Tactical Cloud Computing Node

Col. Charles Wells, project manager of the Distributed Common Ground System-Army (DCGS-A), told Defense Systems magazine today that **DCGS-A Version 3 represents the Defense Department’s first tactical cloud computing node**. **Called the Griffin software build**, this capability is in response to a joint urgent operational need from Army Maj. Gen. Michael Flynn.

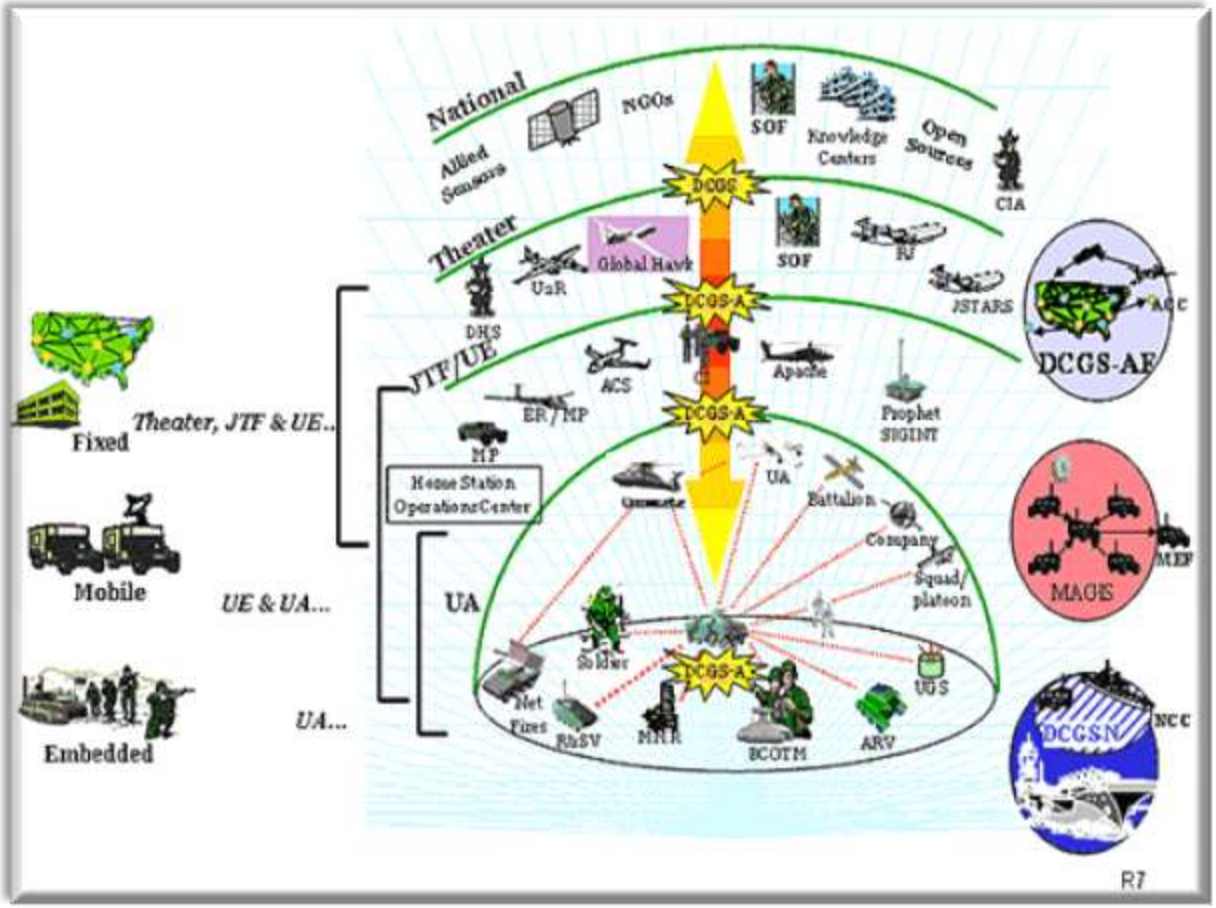
Griffin provides multidiscipline intelligence to **Afghanistan forces** in order to provide:

- A capability to use historical data to predict logistics routes that are most likely to experience an IED attack;
- UAV **full-motion video exploitation** tool
- **A direct tie into a cloud-computing node**.

The DCGS program establishes the **core framework for a worldwide distributed**, network centric, system-of-systems architecture that conducts **collaborative intelligence operations and production**. **The DCGS Integration Backbone provides a distribution of Intelligence Surveillance and Reconnaissance (ISR) data, processes, and systems**.

Example

DCGS-A Operational Concepts



[Army set to deploy tactical intelligence cloud to Afghanistan - Defense Systems]().

Thank You!!!

7th Annual IT Security Automation Conference

October 31 – November 2, 2011 • Crystal City, Virginia
Hyatt Regency

Dr. Antonio Mauro, PhD
info@antoniomauro.it

November 2011