Federal GIS Conference 2014

February 10–11, 2014 | Washington DC

ArcGIS Cloud Security Roadmap and Best Practices for Federal Agencies

Michael Young

Erin Ross

Agenda

- Introduction
- ArcGIS Cloud Capabilities
- ArcGIS Online (SaaS) Security
- ArcGIS IaaS Security
- Esri Managed Services
- Summary

Introduction

- **Michael E Young**
  - Esri Principal Security Architect
  - AGOL FISMA Information System Security Officer (ISSO)
  - MBA, CISSP
- **Erin Ross**
  - Esri Managed Services Program Manager

Introduction

Cloud security affected by many moving parts

- **Cloud Security Standards Evolving**
- **Cloud First Initiative**
- **Advancing ArcGIS Security Capabilities**
- **Evolution of Cloud Provider Capabilities**
- **Mobilization of workforce**

Introduction

Choosing an appropriate cloud deployment

- Not just technical issues/concerns
- Political push/pull issues
  - Cloud first vs. “We don’t trust cloud providers, yet”
- No silver bullet for all cloud security concerns
  - This session provides a roadmap of options and best practices, not just a “Safe” button to push

Introduction

Top Cloud Threats for 2013 - CSA

1. Data Breaches – Sensitive data ends in the wrong hands
   - Hybrid model can eliminate storage of data in the cloud
2. Data Loss - Accidental or purposeful deletion
   - Measures put in place to mitigate this exacerbates above issue.
3. Account Hijacking - Frequently with stolen credentials
   - Avoid shared accounts and use 2 factor auth
4. Insecure APIs
   - Use secure coding guidelines and validate API's are scanned for vulnerabilities
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

Introduction

Cloud Security Standards Evolving

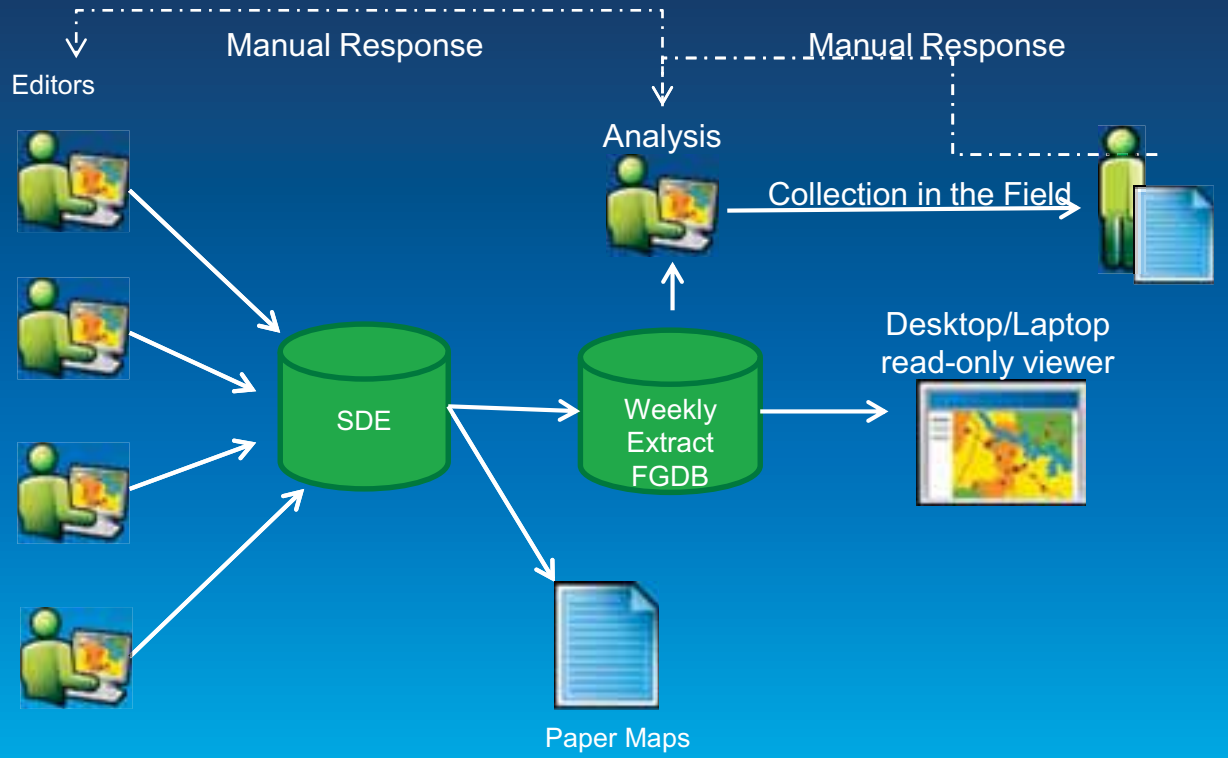
- FISMA
  - Per solution, per agency accreditation since 2002
  - Pre-cloud
- FedRAMP
  - “Do once, use many times” cloud security framework
  - First IaaS ATO December 2012
- Esri’s stance
  - Align with more extensive FedRAMP requirements to meet FISMA requirements at same time
  - Customers can pursue FISMA or FedRAMP accreditations with this approach

Introduction

Esri's Security Strategy Evolution

Introduction

Pre-Cloud Deployment



Ineffective dissemination to field workers and external groups

ArcGIS Cloud Capabilities

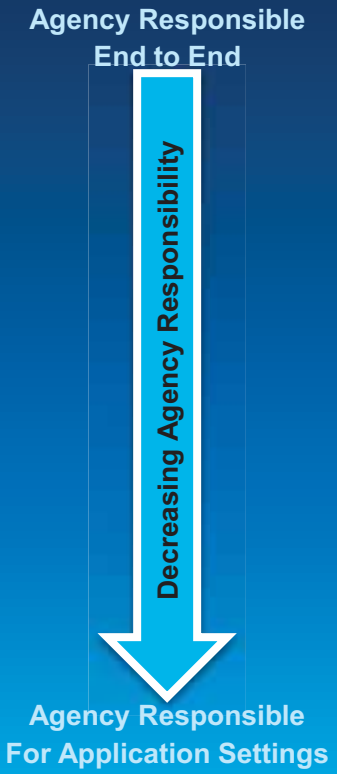
ArcGIS Cloud Capabilities

- Cloud Service Models
- Cloud Deployment Models
- Cloud Management Models

ArcGIS Cloud Capabilities

Service Models

- **Non-Cloud**
  - Traditional systems infrastructure deployment
  - Portal for ArcGIS & ArcGIS Server
- **IaaS**
  - Portal for ArcGIS & ArcGIS Server
  - Some Citrix / Desktop
- **SaaS**
  - ArcGIS Online
  - Business Analyst Online
  - Community Analyst



ArcGIS Cloud Capabilities

Deployment Models

- On-Premises
  - Information cannot go outside an organizations walls
  - Solution: Portal for ArcGIS
- Community
  - Data / Systems management constraints
  - Amazon GovCloud – ITAR / US Persons
    - Esri Managed Services Prototype in place
  - CGI Federal – ITAR / US Citizen
- Hybrid
  - Customer can manage services and data in their walls (Segmentation)
  - Common implementation
- Public
  - Accessible and cost effective
  - ArcGIS Online
  - Uses secure, public cloud infrastructure like SalesForce / Google Apps

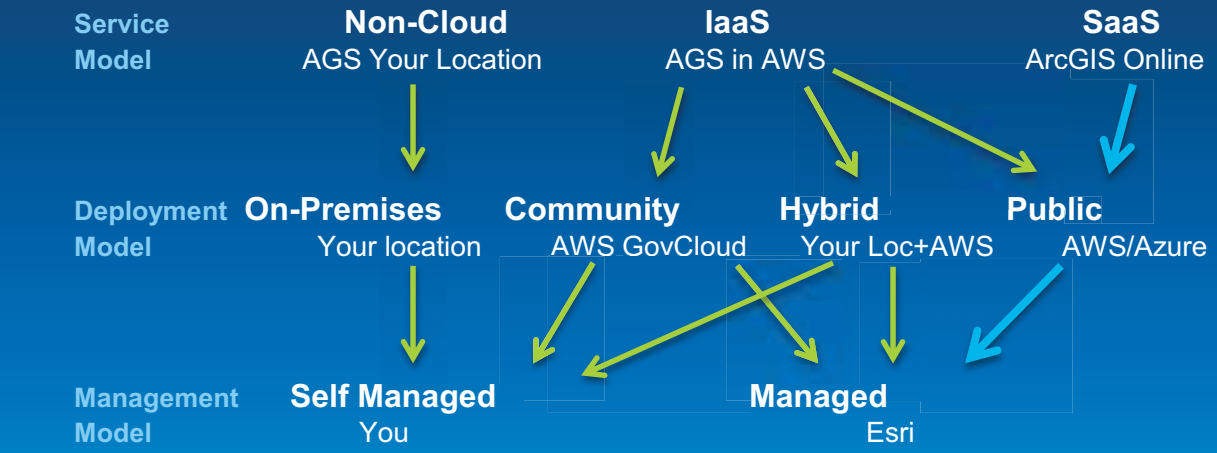
ArcGIS Cloud Capabilities

Management Model

- Self-Managed
  - Your responsibility for managing IaaS deployment security
  - Key security controls discussed later
- Esri Managed
  - Managed Services
  - FedRAMP/FISMA compliant environment capabilities in 2014
  - Government community cloud management now available

ArcGIS Cloud Capabilities

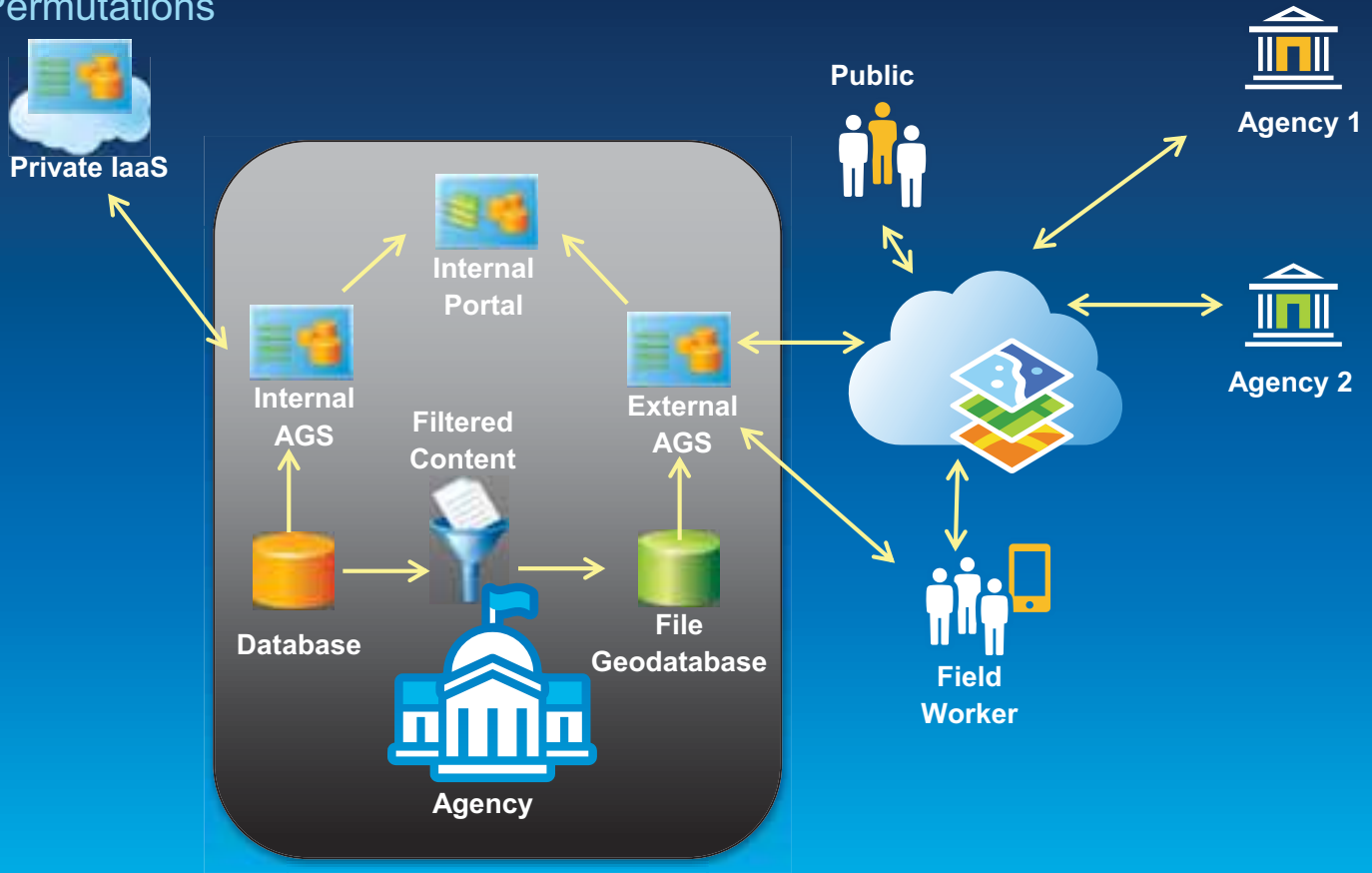
Implementation options



*AWS is a placeholder on this slide for any cloud provider such as Azure, CGI, or Terremark

ArcGIS Cloud Capabilities

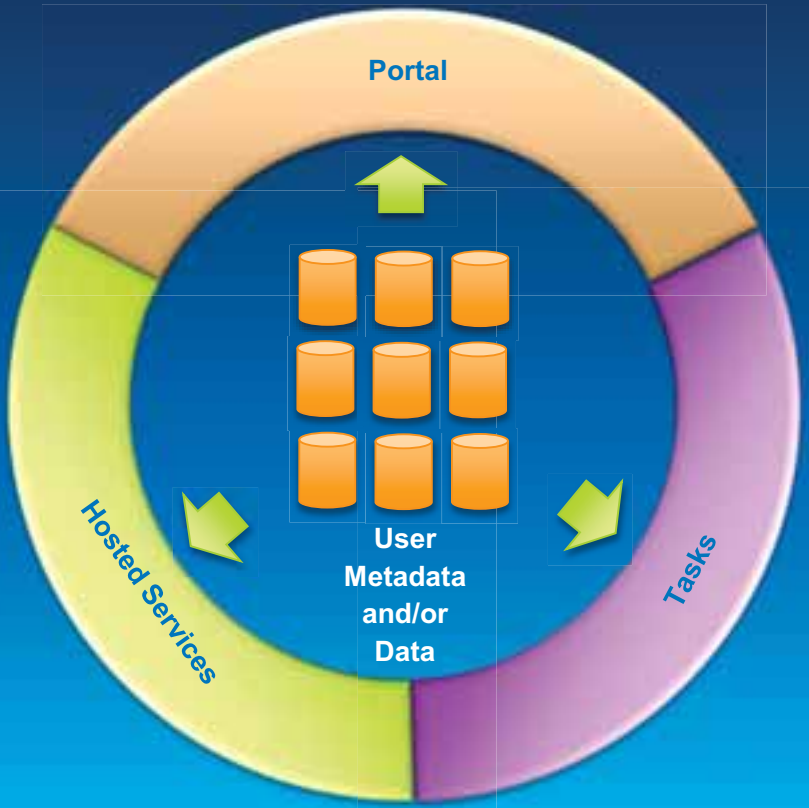
Real Permutations



ArcGIS Online Security

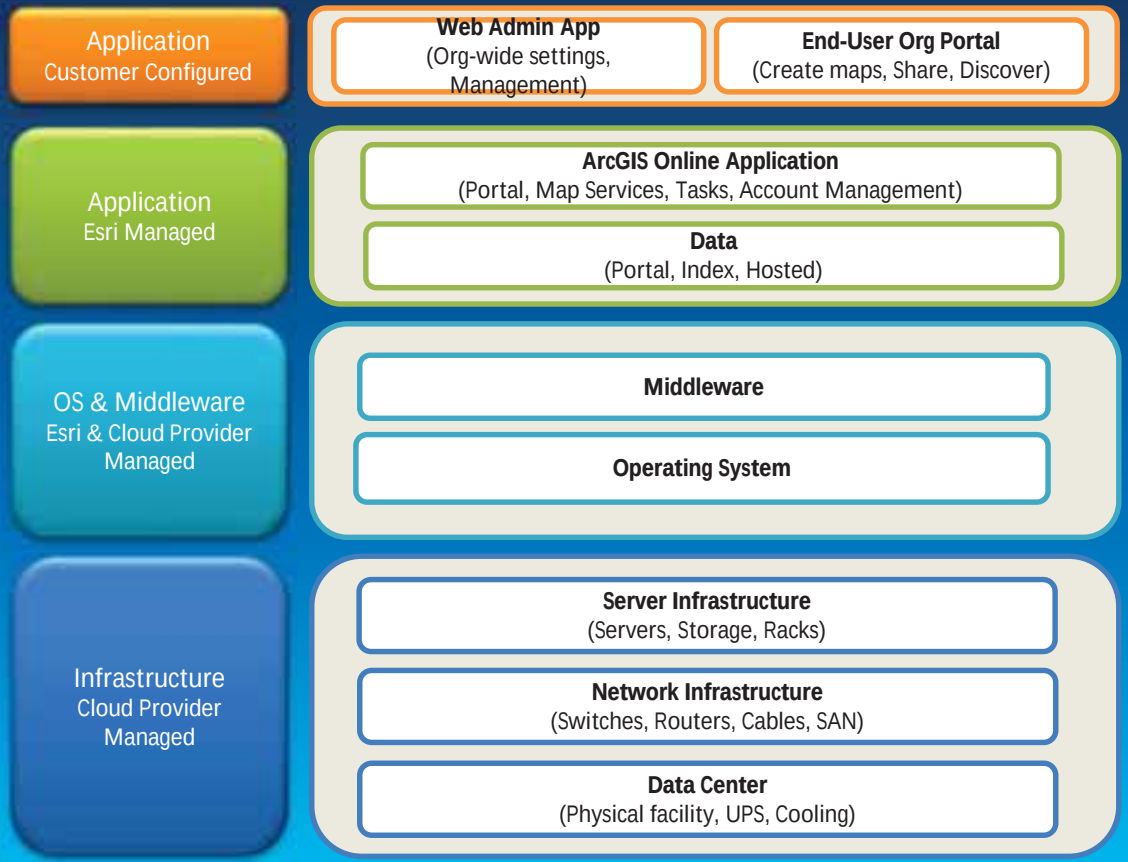
ArcGIS Online Security

A multi-tenant system



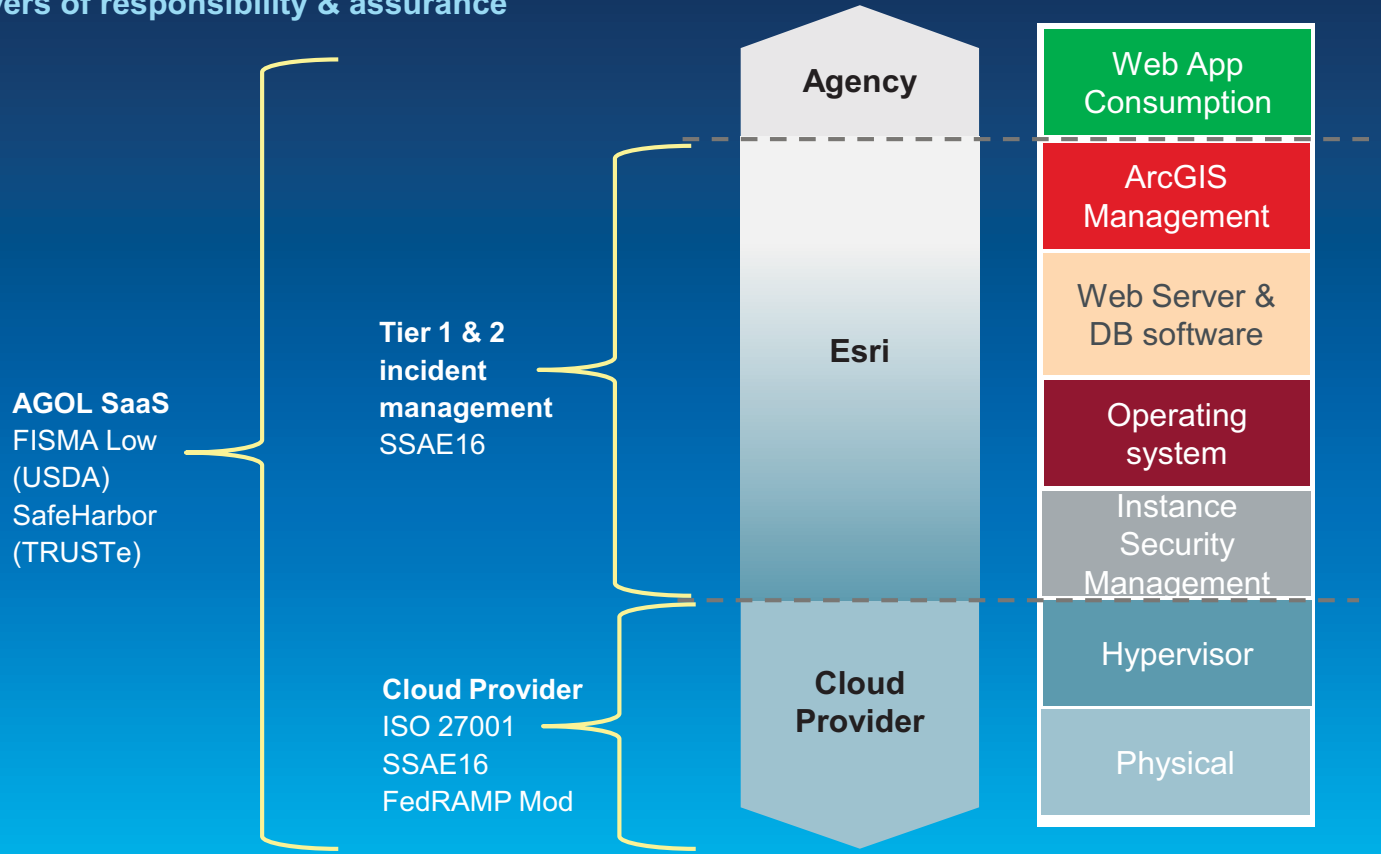
ArcGIS Online Security

Responsibility across components



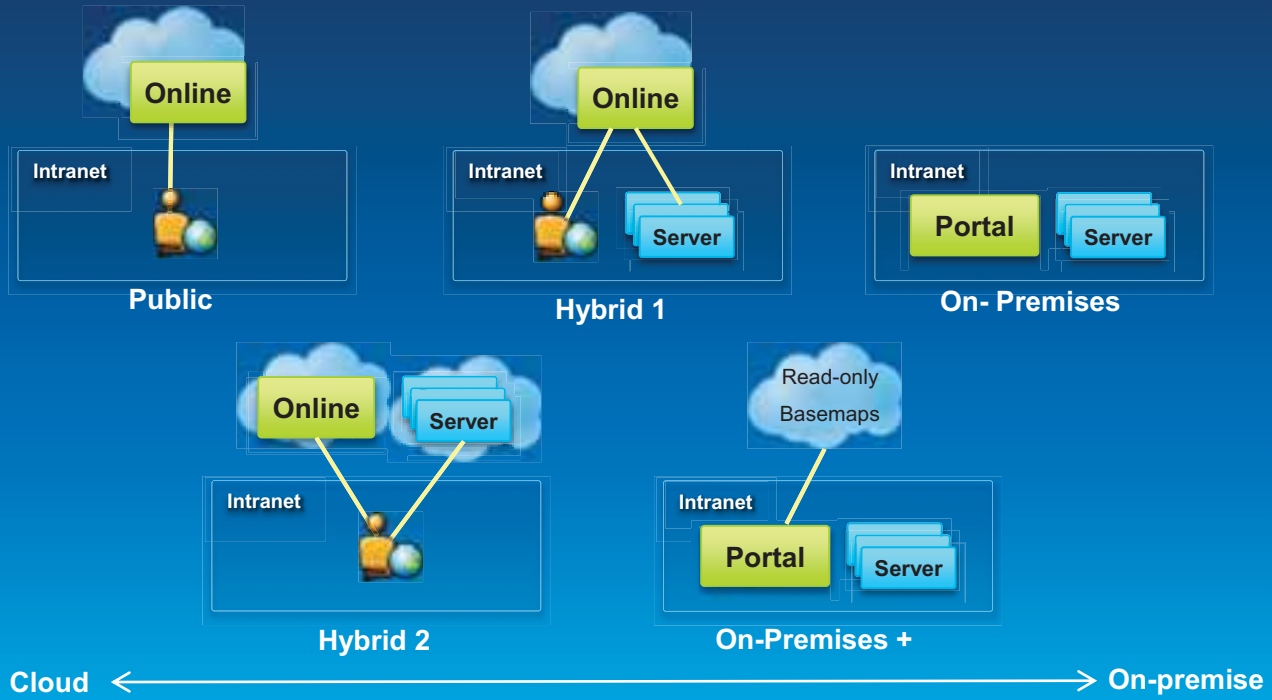
ArcGIS Online Security

Layers of responsibility & assurance



ArcGIS Online Security

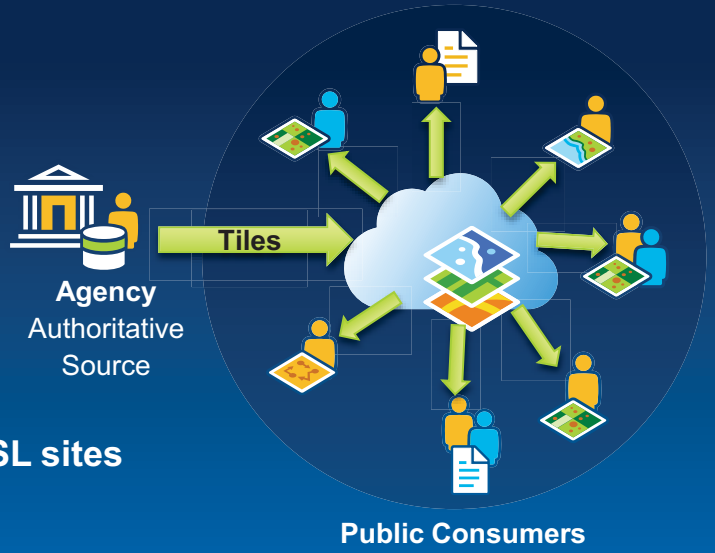
Basic Deployment Options



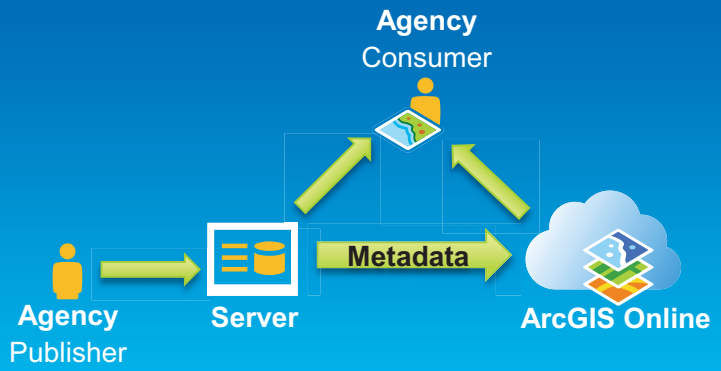
ArcGIS Online

Federal Use Cases

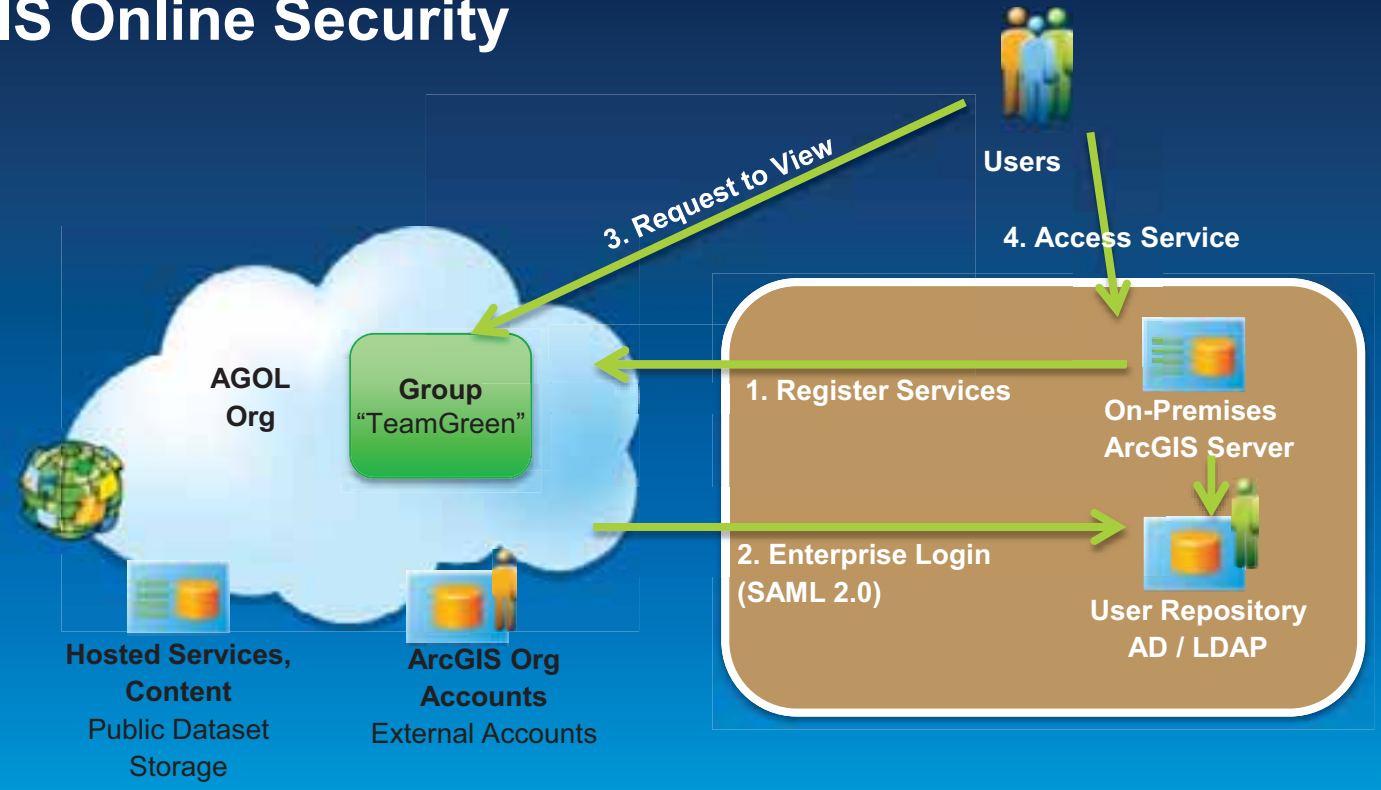
- **Use Case 1 – Public Dissemination**
  - Publish tiles for fast, scalable visualizations
  - Share information with the public
  - Can be used for mashing up services with external non-SSL sites



- **Use Case 2 – Internal Operations**
  - Hybrid deployment of ArcGIS Server and ArcGIS Online
  - Share operational data within or between agencies
  - Sensitive data maintained on Agency premises or other accredited environment
  - ArcGIS Online operates as a discovery portal



Hybrid ArcGIS Online Security



Segment sensitive data internally and public data in cloud

ArcGIS Online Security

Hybrid Cloud Deployment - Metadata

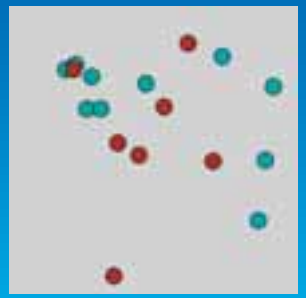
- **Common reason for hybrid cloud deployment is to prevent storing sensitive data in the cloud**
- **Initial FISMA accreditation based on this deployment**
- **What is stored in AGOL?**
  - **Metadata**
- **5 metadata items that could be deemed sensitive are:**
  1. **Service username & password –** Default, not saved
  2. **Service initial extent –** Adjust to a less specific area
  3. **Service name & tags –** Address with organization naming convention
  4. **Service IP Address –** Utilize DNS names within URL's
  5. **Service thumbnail image –** Replace with any image as appropriate

ArcGIS Online Security

Hybrid Cloud Deployment – Data sources

- **Where are internal and cloud datasets combined?**
  - **At the browser**
  - **The browser makes separate requests for information to multiple sources and does a “mash-up”**
  - **Token security with SSL or even a VPN connection could be used between the device browser and on-premises system**

On-Premises Operational Layer Service



https://YourServer.com/arcgis/rest...

Cloud Basemap Service ArcGIS Online

http://services.arcgisonline.com...

Browser Combines Layers

ArcGIS Online Security

Standard Authentication

- **New Enterprise Logins**
  - SAML 2.0
  - Provides federated identity management
  - Integrate with your enterprise LDAP / AD

- **New API's to Manage users & app logins**
  - Developers can utilize OAuth 2-based API's
  - https://developers.arcgis.com/en/authentication/

ArcGIS Online Security

Common Questions

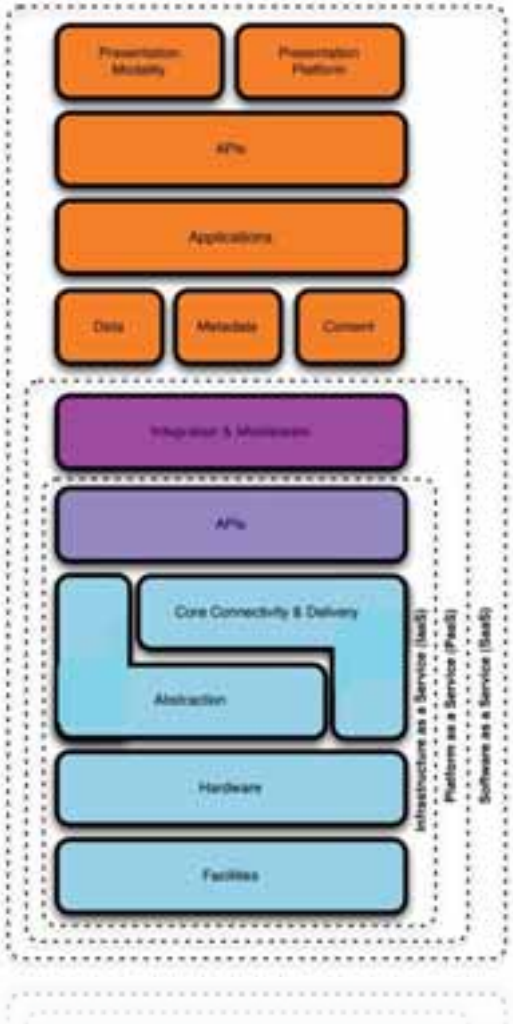
1. **Where is my data?**
   - All ArcGIS Online data and processing resides within US Data centers on US soil

2. **Is my information encrypted?**
   - Organization administrator can force SSL encryption for all communications
   - ArcGIS Online does not encrypt data at rest; however sensitive items can be encrypted by 3rd party solutions

3. **Is it security accredited?**
   - FISMA Accreditation is Imminent

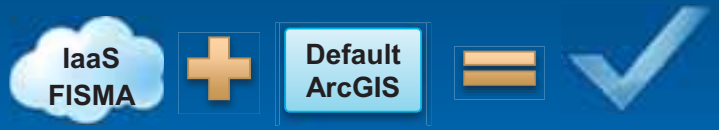
4. **Is my data locked into ArcGIS Online?**
   - Data publishers can extract and download data back to their organization via shapefiles, CSVs, or original publication package.

ArcGIS IaaS Security



ArcGIS IaaS Security

- Question
  - If my cloud IaaS is FISMA/FedRAMP accredited and I deploy my app into that cloud, is the overall implementation FISMA/FedRAMP equivalent?
- Answer
  - No



- Question – Part 2
  - Okay, so it's not FISMA/FedRAMP equivalent, but the IaaS by itself ensures the solution is "secure enough", right?
- Answer
  - No

ArcGIS IaaS Security

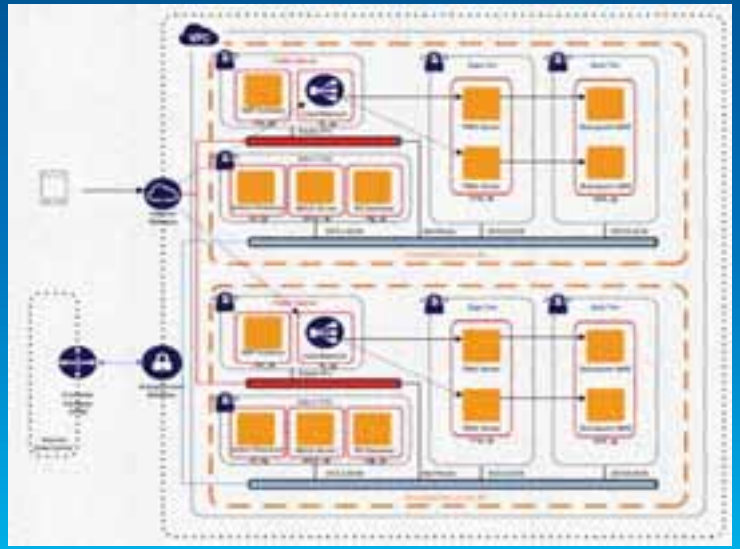
Why is IaaS accreditation by itself not enough?

- **Where are most of the vulnerabilities & who is responsible for mitigating them?**

ArcGIS IaaS Security

- Common ArcGIS IaaS Deployments
  - Deploy ArcGIS Server Windows AMI to AWS
  - Deploy ArcGIS Server via Cloud Builder to AWS

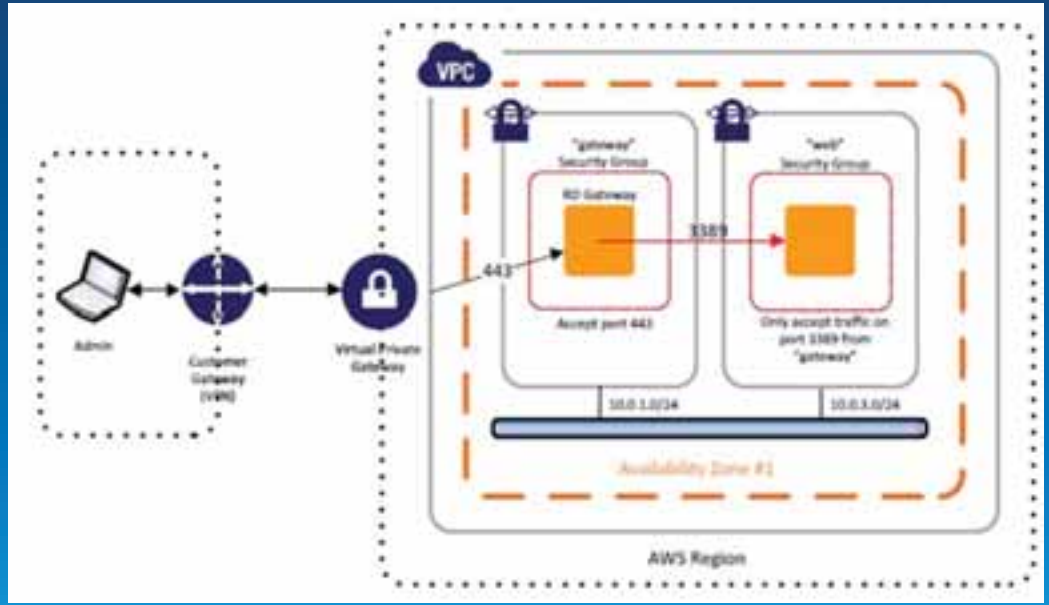
- ArcGIS AWS Security Best Practices
  - Infrastructure Controls
  - Big Data Transfer
  - Application Controls



ArcGIS IaaS Security

Best Practices in AWS

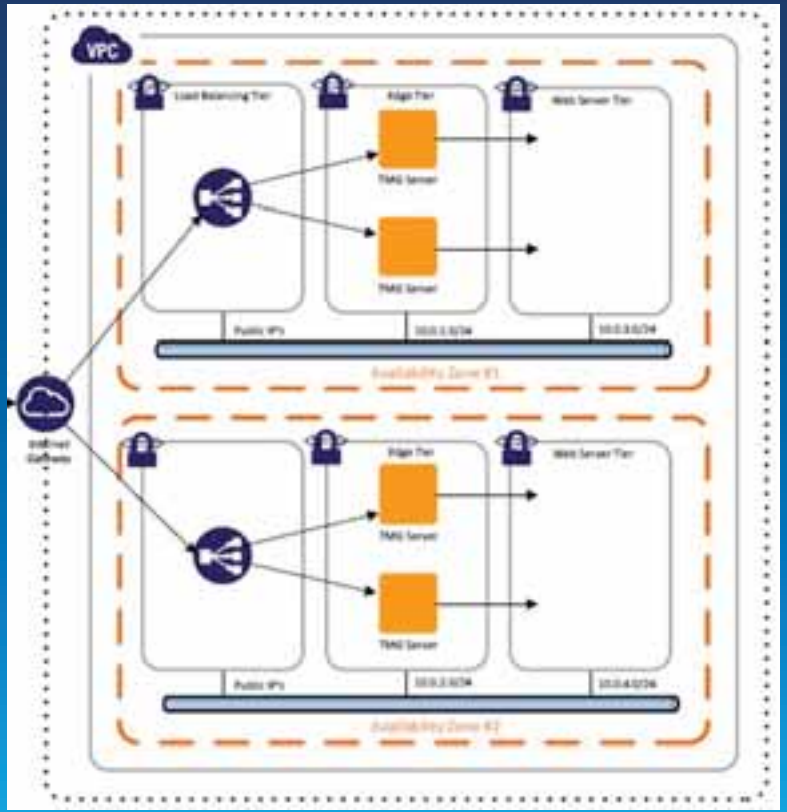
- **Segment cloud infrastructure**
  - Utilize Amazon Virtual Private Cloud (VPC)
  - Utilize separate VPC's for DMZ, Web, App, DB, and Admin systems
- **Utilize Amazon Identity & Access Management (IAM)**
  - Implement two-factor authentication
- **Establish a remote admin gateway**
  - Reduce the number of internet facing admin connections



ArcGIS IaaS Security

Best Practices in AWS

- Reduce attack surface of all interfaces
  - Security harden system & disable unused services
  - Reference GeoCloud instance for policies
  - Potential future ArcGIS Server STIG
- Establish change management & logging infrastructure
  - SIEM & HIDS integration
  - Patch management deployment (SCCM)
- Centralized systems authentication & authorization
- Establish Web Application Firewall capabilities



ArcGIS IaaS Security

Transferring “Big Data” to the cloud

- FTP? – Don’t do it!
- Compression Tools
  - RainStor – 1/40th original size
  - No time/storage consuming re-inflation
- TCP / UDP Optimization Tools
  - Aspera
  - Utilize UDP for throughput and TCP for error-free
- Multifunction Optimization Tools
  - Cloud Opt & Attunity Cloudbeam
  - Compression, protocol optimization, data de-duplication, SSL acceleration

ArcGIS IaaS Security

Minimize ArcGIS Server Attack Surface

- Don’t expose Server Manager to public
- Disable Services Directory
- Disable Service Query Operation (as feasible)
- Enable Web Service Request Filtering
  - Windows 2008 R2+ Request Filtering - Nice
  - XML Security Gateway - Better
- Limit utilization of commercial databases under website
  - File GeoDatabase can be a useful intermediary
- Require authentication to services

Esri Managed Services

Erin Ross

Esri Managed Services

Cloud based GIS infrastructure support

HIGH AVAILABILITY
INFRASTRUCTURE
MONITORING
SCALABILITY
STORAGE
ARCHIVE
REPORTING
SOFTWARE
PERFORMANCE TESTING
NETWORK
SYSTEM DESIGN
REDUNDANCY
Deployment
DISASTER RECOVERY
SECURITY
BANDWIDTH
DATA MANAGEMENT
BACKUP
AGOL INTEGRATION
HARDWARE
CACHING
CHANGE MANAGEMENT

- **Access to Enterprise GIS Expertise**
- **Scalable Resources**
- **Reduced cost of ownership**
- **Rapid Deployment**

Experienced, Secure, Reliable, Scalable

Deployment Patterns

Flexible offerings to support a variety of needs

ArcGIS Online and Managed Services

Users

- ✓ Desktop
- ✓ Web
- ✓ Mobile

ArcGIS Online

- ✓ Online Basemaps
- ✓ Geocoding, Routing
- ✓ Hosted Feature & Tile Map Services
- ✓ App Templates

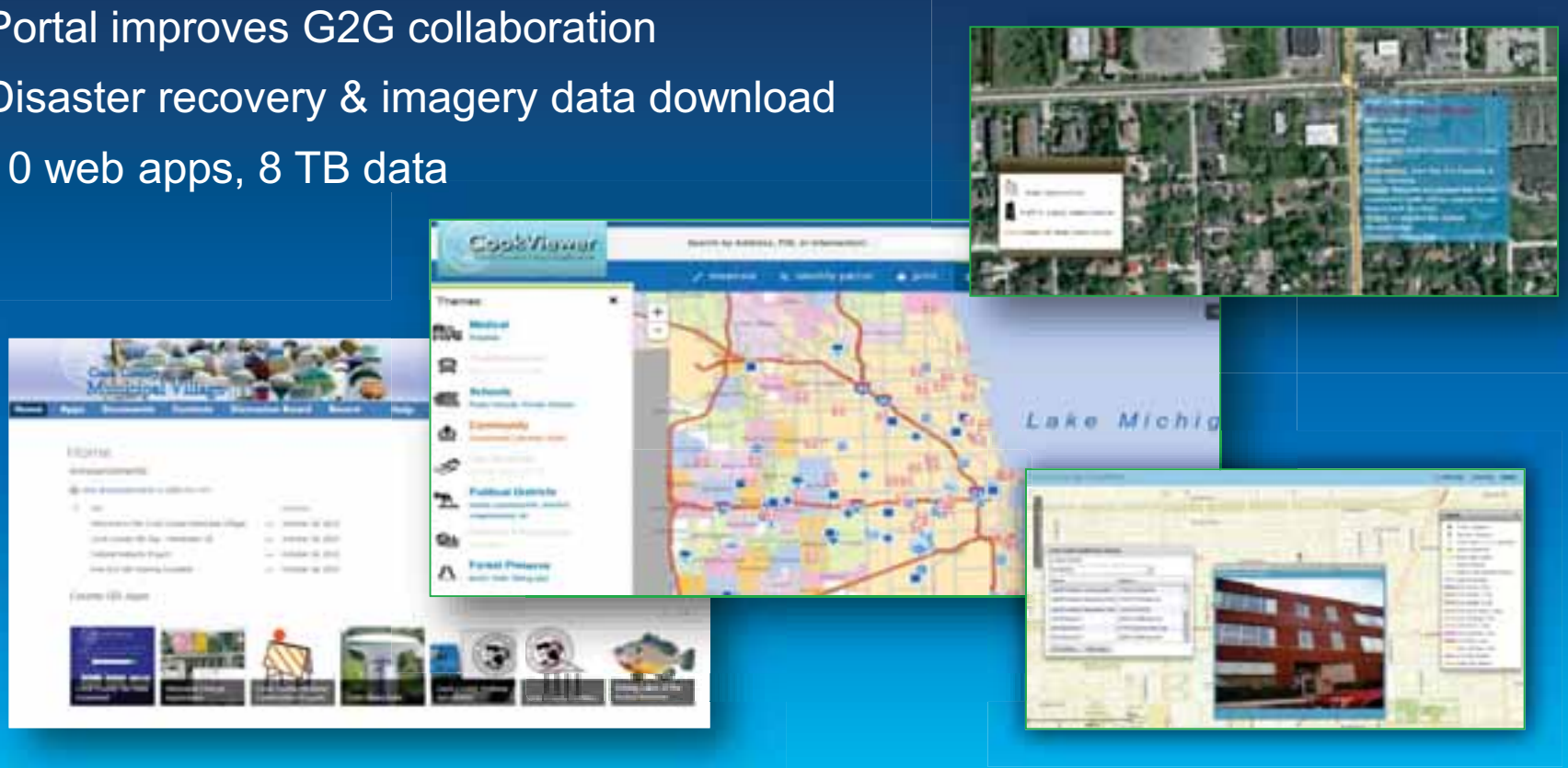
Esri Managed Services

- ✓ Custom Web Apps
- ✓ GP, Reporting Services
- ✓ Imagery, Large Datasets
- ✓ Dynamic Map Services
- ✓ RDBMS (Oracle, SQL Server)

ArcGIS Online front-end, Managed Services back-end

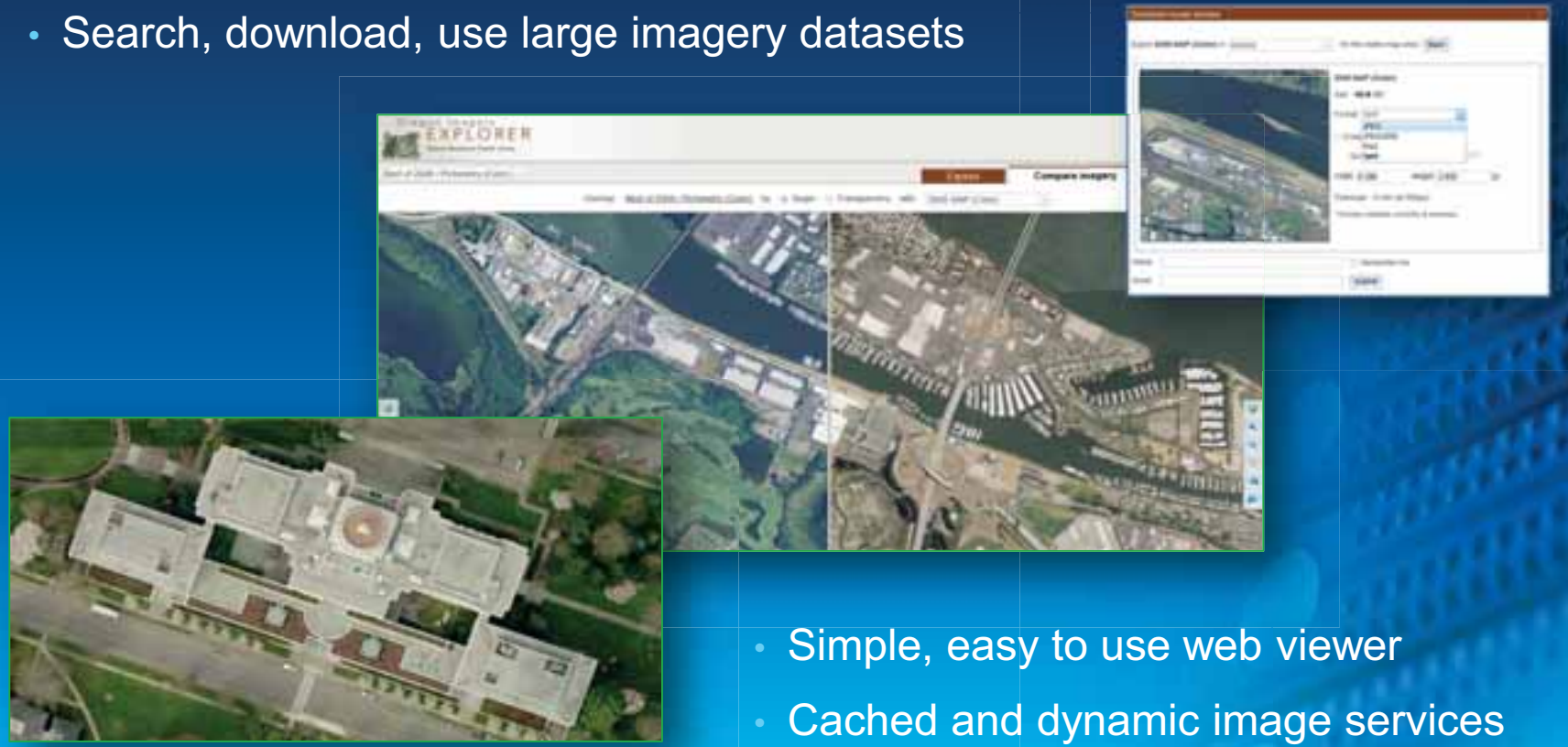
Cook County Municipal Cloud

- Portal improves G2G collaboration
- Disaster recovery & imagery data download
- 10 web apps, 8 TB data



Oregon Imagery Explorer

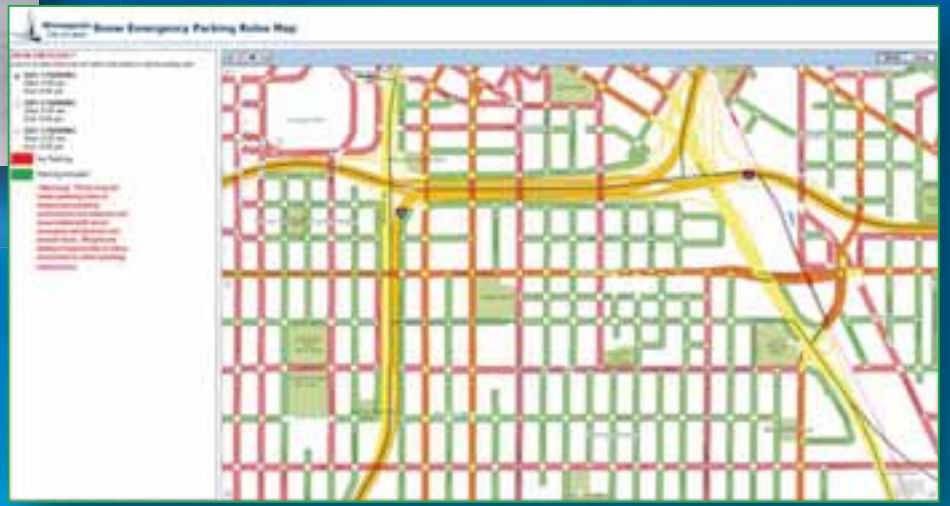
- Search, download, use large imagery datasets



- Simple, easy to use web viewer
- Cached and dynamic image services

City of Minneapolis Snow Emergency

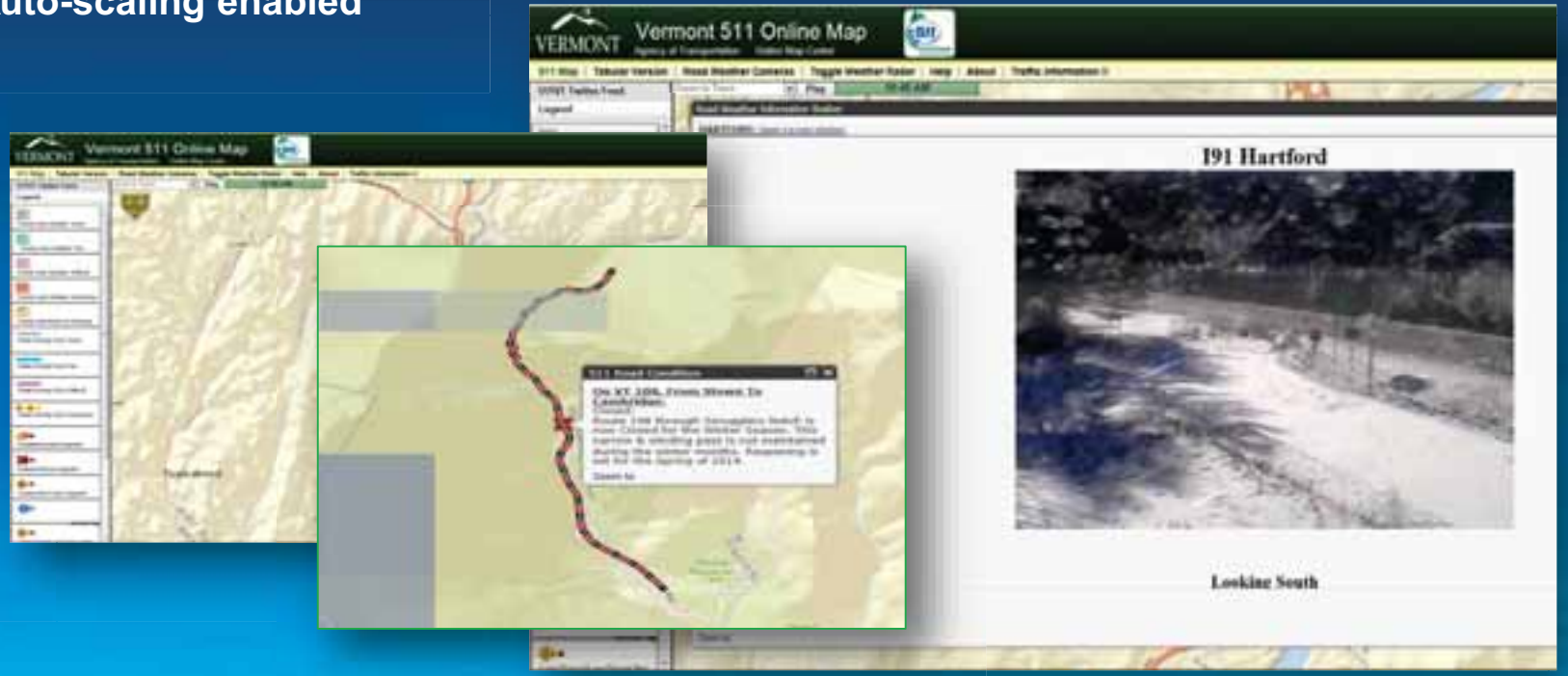
- Scalable environment available during snow emergencies
- Dev and Prod environments



- ArcGIS Online + Managed Services Hybrid

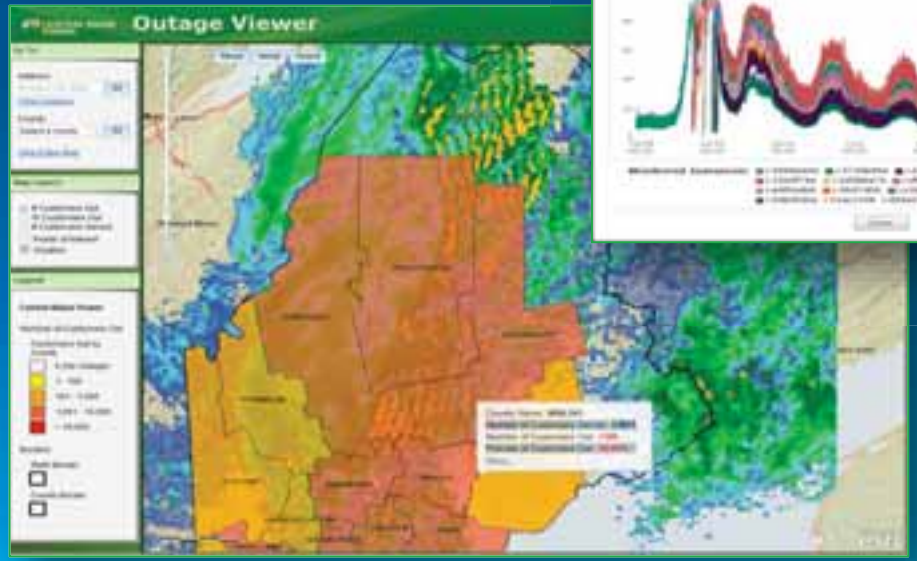
State of Vermont 511

- Road closures and traffic conditions available to the public
- Auto-scaling enabled



Iberdrola USA Outage Viewer

- Server Auto-Scaling
- Data Update Automation



- High Availability
- Geographic Redundancy

National Grid IMAP

- Sandbox used for prototyping
- Quick, easy access to GIS
- Mobile capabilities

- Hybrid ArcGIS Online + Managed Services
- Secure VPN access

What's new in 2014?

- FedRAMP/FISMA Moderate Security Offering
- ArcGIS Desktop in the cloud support
- Utilize new platforms (Azure, CGI, Verizon, IBM)

FedRAMP AGENCY

FISMA

IBM

Windows Azure

CGI

verizon terremark

Federal Cloud Accredited Solution Overview

FedRAMP and FISMA Moderate

ArcGIS Online

Customer Instances

- ✓ ArcGIS for Server
- ✓ Portal for ArcGIS

Customer Databases

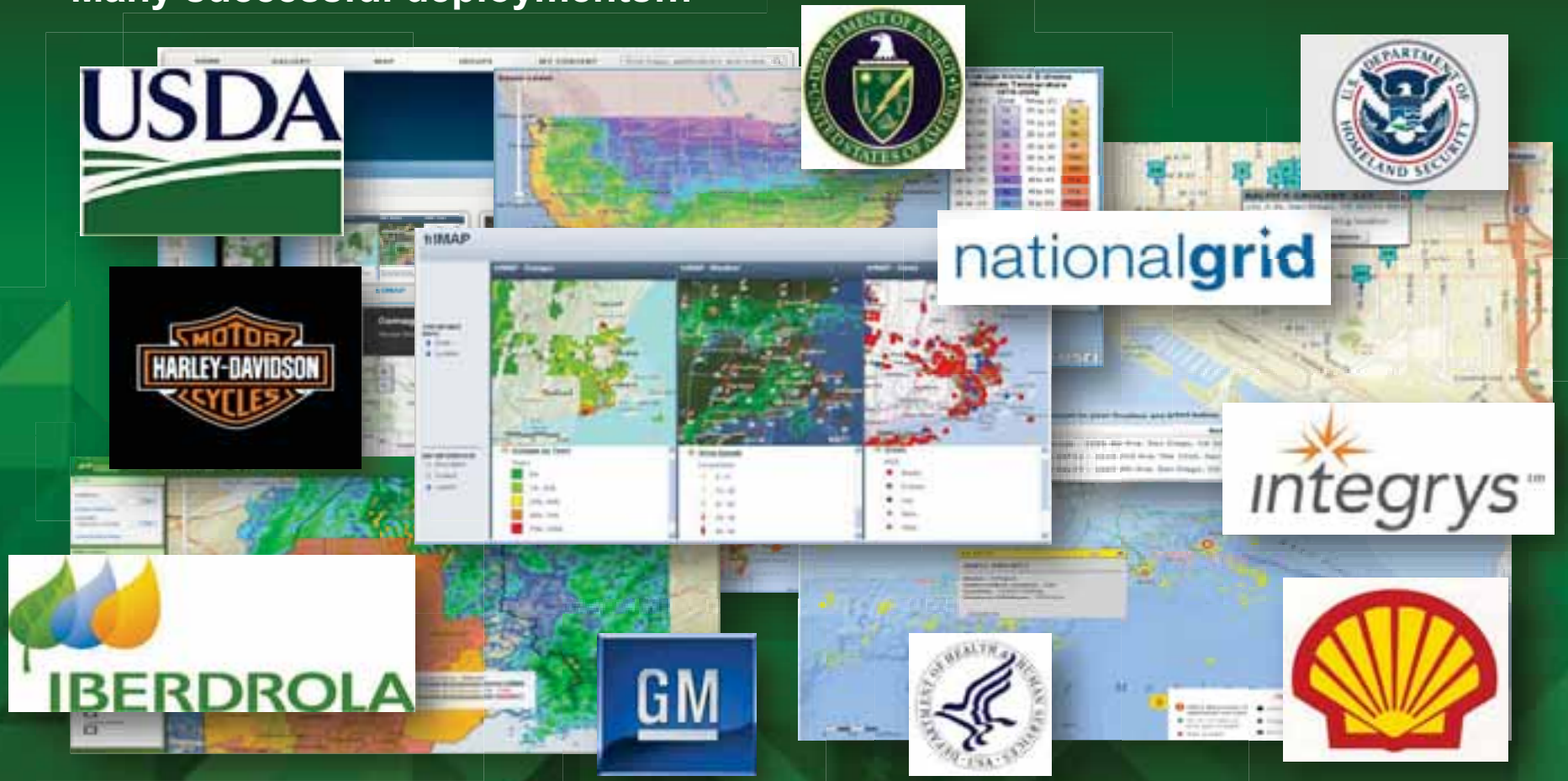
End Users

Esri Cloud GIS Administrator

Security Infrastructure

- ✓ Centralized Authentication (2-factor)
- ✓ Hardware Key Management
- ✓ Network Address Translation
- ✓ Virtual Private Cloud (Segmentation)
- ✓ Redundancy (multiple data centers)
- ✓ IDS/SIEM
- ✓ Logging

Many successful deployments…



Summary


Attack
Location
CGI
CSA
Compliance
Confidentiality
FISMA
AWS
IaaS
SaaS
VPN
SSL
Cloud
Assessments
ArcGIS
Metadata
Terremark
Encryption
Deployment
Machines
FedRAMP
ADFS
Availability
Security
Segmentation
Accreditation
Roadmap
Hybrid
Surface
Private
Integrity
Responsibility
Public
Virtual
SAML
Azure
Mobile
Online
PaaS

Summary

ArcGIS Security Resources

- **Available Now**
  - ArcGIS Online Security Flyer
    - http://www.esri.com/software/arcgis/arcgisonline/~/media/Files/Pdfs/software/arcgis/arcgis-online/agol-security-overview-flyer.pdf
  - ArcGIS For Professionals Site
    - http://pro.arcgis.com/enterprise-gis/
  - ArcGIS Online Cloud Security Alliance
    - Standardized security documentation

CSA STAR

- **Future**
  - Trust.ArcGIS.com site for Security, Privacy and Status
  - ArcGIS Server STIG
    - DISA / FISMA Alignment

Summary

- Cloud security is NOT just about technology
  - Understand your organizations Cloud GIS risk level
  - Utilize Defense-In-Depth
- ArcGIS Cloud Capabilities are expanding rapidly
  - Deployments across numerous cloud providers
  - Deployments in government community clouds
- Expect standardized cloud security from Esri
  - Product Security Capabilities – SAML Web SSO
  - Alignment with Federal Regulations – FedRAMP, FISMA
  - Security Control Documentation – CSA
  - Security Hardened Images – Checklist

What is still needed?

- **Your Input is Crucial**
  - **Your Feedback and Insight Today is Essential**
    - **Current Security Issues**
    - **Upcoming Security Requirements**
    - **Areas of concern Not addressed Today**

Contact Us At:

Enterprise Security esinfo@esri.com

Federal GIS Conference 2014

February 10–11, 2014 | Washington DC

esri

Don’t forget to complete a session evaluation form!

Federal GIS Conference 2014

February 10–11, 2014 | Washington DC

esri

Networking Reception

Smithsonian National Museum of Natural History

Tuesday, 6:30 PM–9:30 PM

Bus Pickup located on L Street

Federal GIS Conference 2014

February 10–11, 2014 | Washington DC

esri

Print your customized Certificate of Attendance!

Printing stations located in Hall B
and the 140/150 Room Concourse.

Federal GIS Conference 2014

February 10–11, 2014 | Washington DC

esri

GIS Solutions EXPO, Hall B

Monday, 12:30 PM–6:30 PM
Tuesday, 10:45 AM–4:00 PM

- Exhibitors
- Hands-On Learning Lab
- Technical & Extended Support
- Demo Theater
- Esri Showcase

Federal GIS Conference 2014

February 10–11, 2014 | Washington DC

esri

Interested in diving deeper into Esri technology?

Add a day to your Fed GIS experience and register to attend the Esri DevSummit Washington DC. Stop by the registration counter to sign up.