GIS

The Geographic Approach for the Nation

ESRI Federal User Conference

Washington, D.C. • February 17–19, 2010

Enterprise GIS:
Delivering Secure GIS Solutions

CJ Moses
Michael E Young

Version 2.3

Agenda

- Intro
- What does Secure GIS mean to you?
- ESRI's Security Strategy
- Enterprise-Wide Security Mechanisms
- Application Security
- Cloud Computing Security
- NEW Integrated Security Model
- ESRI Security Compliance
- Summary and Next Steps

Intro

Michael E Young

- ESRI Senior Enterprise Architect
- FISMA C&A Application Security Officer
- Certified Information Systems Security Professional (CISSP)

CJ Moses

- AWS Senior Manager
- Cloud Computing Security Expert
- Extensive Career within Federal Government (FBI / US AFOSI)

What does Secure GIS mean To You?

What Does Secure GIS Mean to You?

- What about
  - Integration with other enterprise components?
    - Directory Services / LDAP / MS Active Directory
  - Meeting security standards requirements?
  - Security Certifications & Accreditations?
    - FDCC / FISMA / DITSCAP
  - User Application Interfaces?
    - ADF, MS Silverlight, Adobe Flex, JavaScript, Rich Clients
  - How much should be embedded in applications vs. security products?
    - ArcGIS Token Service / 3rd Party Single-Sign-On products

Don't focus on trying to implement a security silver bullet

Take a step back and focus on the bigger picture first

ESRI's Security Strategy

ESRI's Security Strategy

Reinforcing Trends

ESRI Products

Discrete products and services

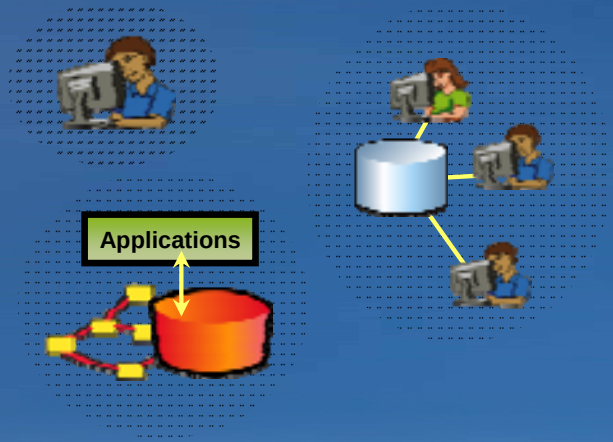
… exploiting 3rd party security functionality

Enterprise platform and services

… exploiting embedded and 3rd party security functionality

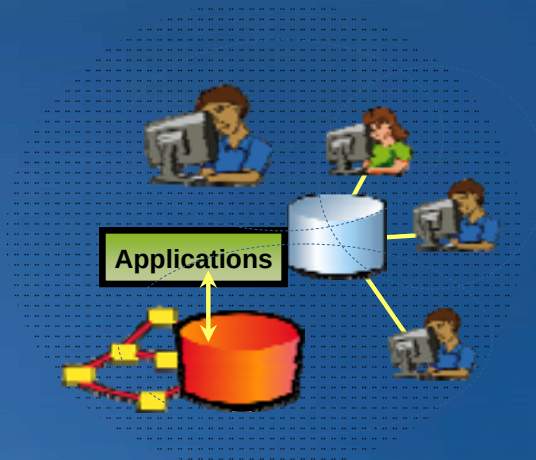
IT/Security Compliance

Isolated Systems



… relying on solution C&A

Integrated systems with discretionary access



… relying on product and solution C&A

ESRI's Security Strategy

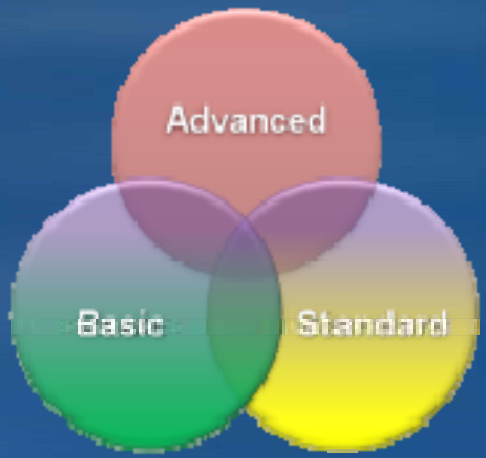
- Secure GIS Products
  - Incorporate security industry best practices
  - Trusted geospatial services across the globe
  - Meet both individual user needs and entire organizations

- Secure GIS Solution Guidance
  - Enterprise Resource Center Website
  - ESRI security patterns

ESRI's Security Strategy

Security Patterns

- ESRI provides security implementation patterns
  - Best practice security guidance
- Leverages National Institute of Standards and Technology (NIST)
- Patterns based on risk level
  - Basic Security
  - Standard Security
  - Advanced Security



- Identify *your* risk level
  - Formal process – NIST 800-60
  - Informal process

To prioritize information security and privacy initiatives, organizations must assess their business needs and risks

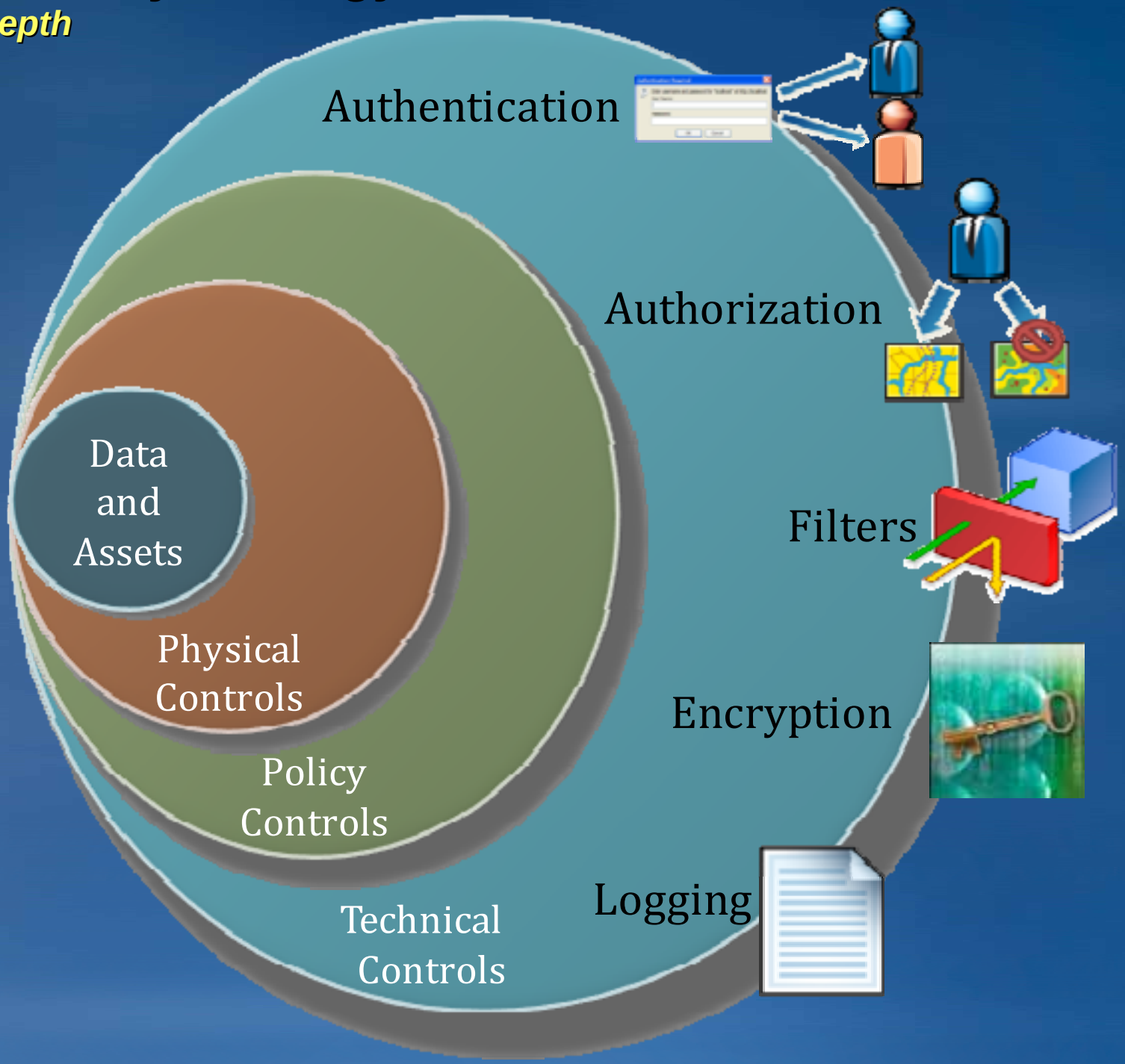
ESRI's Security Strategy

Foundational Security Principles

- CIA Security Triad
- Defense in Depth

ESRI's Security Strategy

Defense in Depth

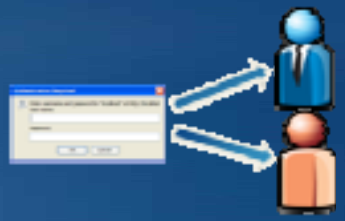


Enterprise-wide Security Mechanisms

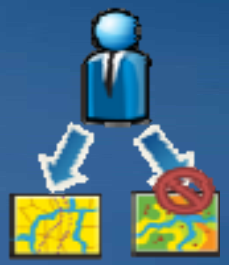
Enterprise-Wide Security Mechanisms

Overview

- Authentication



- Authorization



- Filters

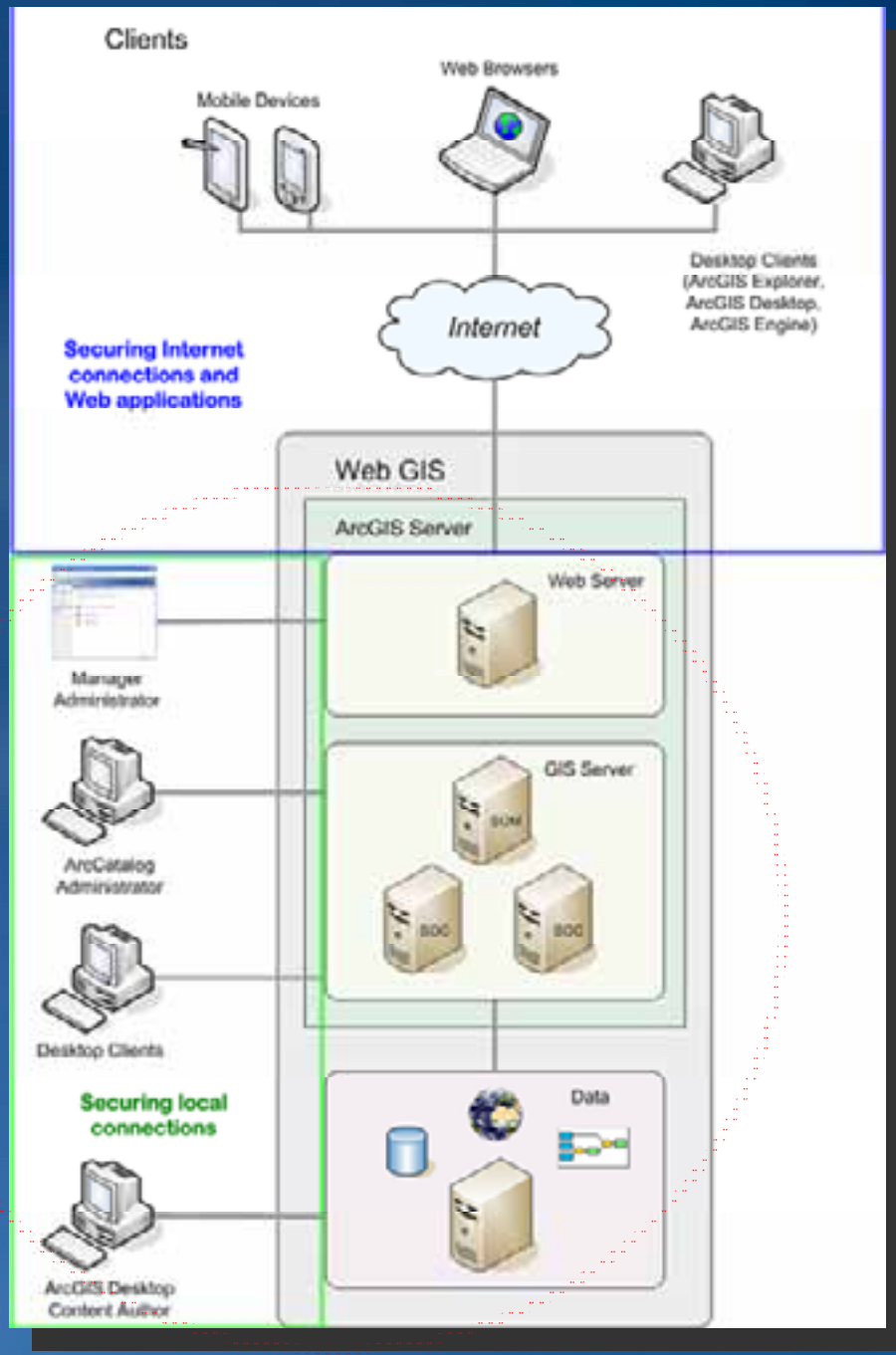
- Encryption

- Logging/Auditing

Enterprise-Wide Security Mechanisms

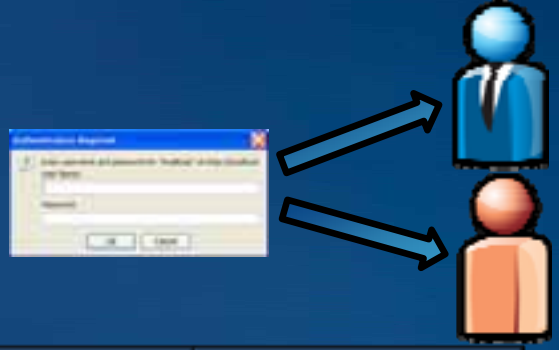
Authentication

- Three ArcGIS Authentication Schemes
  - Web Traffic via HTTP
    1. Web Services
    2. Web Applications
  - Intranet Traffic via DCOM
    3. Local Connections



Enterprise-Wide Security Mechanisms

Authentication



Authentication Method	Protocol	Description	Credential Encryption	Access Restriction Mechanism
None	HTTP	Default Internet Connections	N/A	Web Service or Web Application
Windows Integrated	DCOM	Default Local Connections	Managed by OS	OS Groups AGSUsers/ AGSAdmin
Basic Digest Windows Integrated	HTTP (SSL optional)	Browser built-in pop-up login dialog box	Basic None, unless using SSL	Web Service or Web Application
.NET Form-based	HTTP (SSL optional)	Application provides its own custom login and error pages.	None, unless using SSL	Web Application
Java ArcGIS Managed	HTTP (SSL optional)	ArcGIS Server provides login page for Java Web Application	None, unless using SSL	Web Application
Java EE Container	HTTP (SSL optional)	Web container provides challenge for credentials	Managed by Container	Web Service or Web Application
Client Certificates PKI Smart Cards	HTTPS	Server authenticates the client using a public key certificate	Managed by PKI	Web Service or Web Application
ESRI Token	HTTP (SSL optional)	Cross Platform, Cross API Authentication	AES-128bit	Web Service

Enterprise-Wide Security Mechanisms

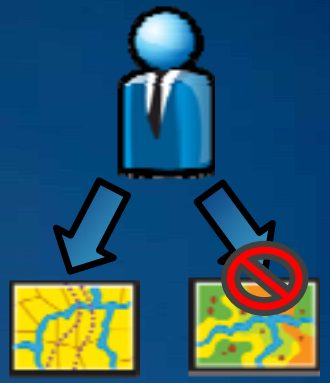
Authentication

- Enterprise Security Store Integration Options
  - Also called Principle Store
  - Contains Users & Roles
- Java Security Store Options
  - *Default* – Apache Derby
  - External Database
  - LDAP
  - MS Active Directory

- .NET Security Store Options
  - *Default* - Windows Users and Groups
  - MS SQL Server Express
  - Custom Provider
    - Instructions for Active Directory and Oracle Providers available

Enterprise-Wide Security Mechanisms

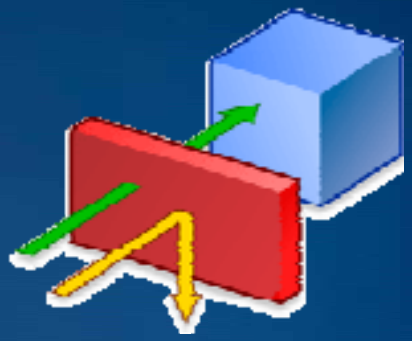
Authorization



- Role Based Access Control (RBAC)
  - ESRI COTS
    - Service Level Authorization across products
    - ArcGIS Manager web application used to assign access
    - Services grouped in folders utilizing inheritance
  - 3rd Party
    - RDBMS – Row Level or Feature Class Level
      - Multi-Versioned instances may significantly degrade RDBM performance
      - Alternative is SDE Views
  - Custom - Limit GUI
    - Rich Clients via ArcObjects
    - Web Applications
      - Check out sample code - Google: EDN Common Security
      - Try out Microsoft's AzMan tool

Enterprise-Wide Security Mechanisms

Filters

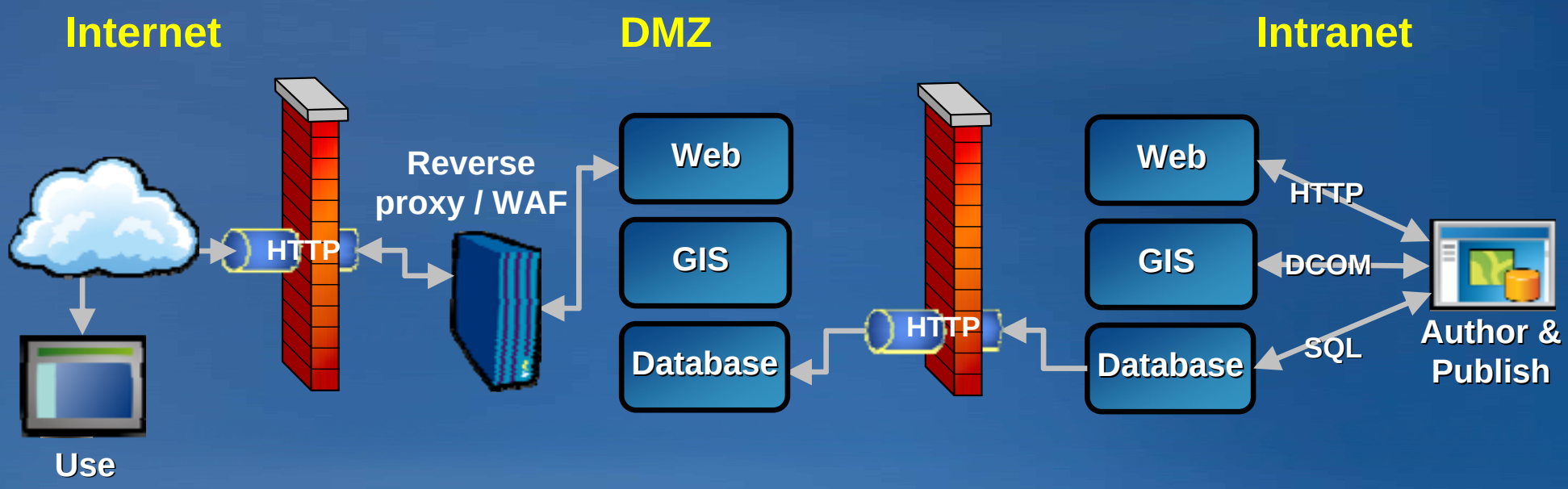


- 3rd Party
  - Firewalls
  - Reverse Proxy
    - Common implementation option
    - MS now has free reverse proxy code for IIS 7 (Windows 2008)
  - Web Application Firewall
    - ModSecurity Can Significantly Reduce Attack Surface
  - Anti-Virus Software
  - Intrusion Detection / Prevention Systems
  - Limit applications able to access geodatabase

Enterprise-Wide Security Mechanisms

Filters – Firewall Friendly Scenario

- Reverse proxy obfuscates internal systems
  - Add Web Application Firewall (WAF) for better protection
  - Communication between proxy and web server can be any port
- File Geodatabase in DMZ
  - One-way replication via HTTP(s)
  - Deploy on each web server for optimal throughput/performance
  - Internet users only have access to a subset of entire Geodatabase



Enterprise-Wide Security Mechanisms

Encryption

- 3rd Party
  - Network
    - IPSec (VPN, Internal Systems)
    - SSL (Internal and External System)
  - File Based
    - Operating System – BitLocker
    - GeoSpatially enabled PDF's combined with Certificates
    - Hardware (Disk)
  - RDBMS
    - Transparent Data Encryption
    - Low Cost Portable Solution - SQL Express 2008 w/TDE

Enterprise-Wide Security Mechanisms

Logging/Auditing

- ESRI COTS
  - Geodatabase history
    - May be utilized for tracking changes
  - Job Tracking for ArcGIS (JTX)
    - Track Feature based activities
  - ArcGIS Server Logging
- Custom
  - ArcObjects component output GML of Feature based activities
- 3rd Party
  - Web Server
  - RDBMS
  - OS
  - Firewall

Application Security

Application Security

Overview

- Rich Clients
- Mobile
- Web Applications
- Web Services
- Online Services

Application Security

Rich Clients

- Authentication / Authorization
  - Web Service integration with Token Service
  - SSO with Windows Integrated authentication
- Encrypting Communication
  - Direct Connect
    - Utilize database vendor client SSL or IPSec
  - Application Connect
    - IPSec Tunnel for SDE Port 5151
  - Web Services
    - SSL - HTTPS
- Custom Development
  - Fine-grained GUI access control
    - Edit, Copy, Cut, Paste and Print
  - LDAP integration

Application Security

Mobile

- ArcPad
  - AXF Data file - Password protect and encrypt
  - Memory Cards – Encrypt
  - ArcGIS Server users and groups - Limit who can publish ArcPad data
  - Internet connection – Secure ArcPad data synchronization traffic
- ArcGIS Mobile
  - GeoData Service - HTTPS (SSL) or VPN tunnel
  - Utilization of Token Service
  - Web Service Credentials
  - Consider utilization of Windows Mobile Crypto API
  - Third party tools for entire storage system

Application Security

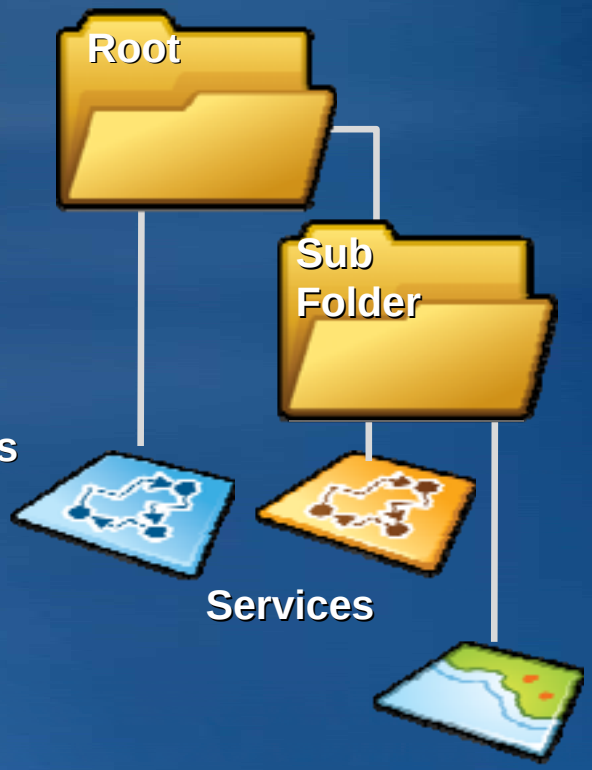
Web Applications

- ArcGIS Server Manager
  - Automates ASP.NET and Java EE web app security
    - E.g. Modifies web.config file of ASP.NET
- Application Interfaces
  - .NET and Java ADF's
    - Out of the box integration with Token Security service
  - REST API's (JavaScript, Flex, Silverlight)
    - Can embed in URL – Simple
    - Better solution is dynamically generate token
    - Don't forget to protect access to your client code

Application Security

Web Services

- ArcGIS Server Manager
  - Permission Inheritance
    - Folder Level
    - Individual Service Level
  - Service Level Security Restrictions
    - Internet / Web connections only
  - Secures all web service interfaces
    - REST
      - Service directory on by default (Disable as necessary)
    - SOAP
      - WS-Security addressed by 3rd party XML/SOAP gateways
    - OGC
      - COTS Simple/Common – Basic Authentication/SSL
      - 3rd Party Advanced – ConTerra Feature Level Security



- Removing Local Connection Access
  - Empty AGSUsers group

Application Security

Online Services

- ArcGIS Online Search and Share
  - Central resource for easily accessing, storing and sharing maps
  - A membership system
    - You control access to items you share
    - You are granted access to items shared by others
    - You join and share information using groups
    - Organizations self-administer their own users and groups
  - Site security similar in approach with other social networking sites

Application Security

Online Services

- Ready to try Public Cloud Computing?
- New ArcGIS Server For Amazon
  - ESRI built ArcGIS Server Amazon Machine Image (AMI)
  - Deploy to Amazon Elastic Compute Cloud (EC2) instance
- Addressing Security
  - Current AMI not hardened beyond Windows 2008 Server defaults
  - Typical Firewall Entries for Cloud implementations
    - ArcGIS Server
      - Port 80/443 for IIS
      - Remote desktop
    - Enterprise GeoDB AMI
      - Port 5151
- Biggest Cloud Computing Concern is Security and Privacy…

Brief Cloud Computing Security Discussion

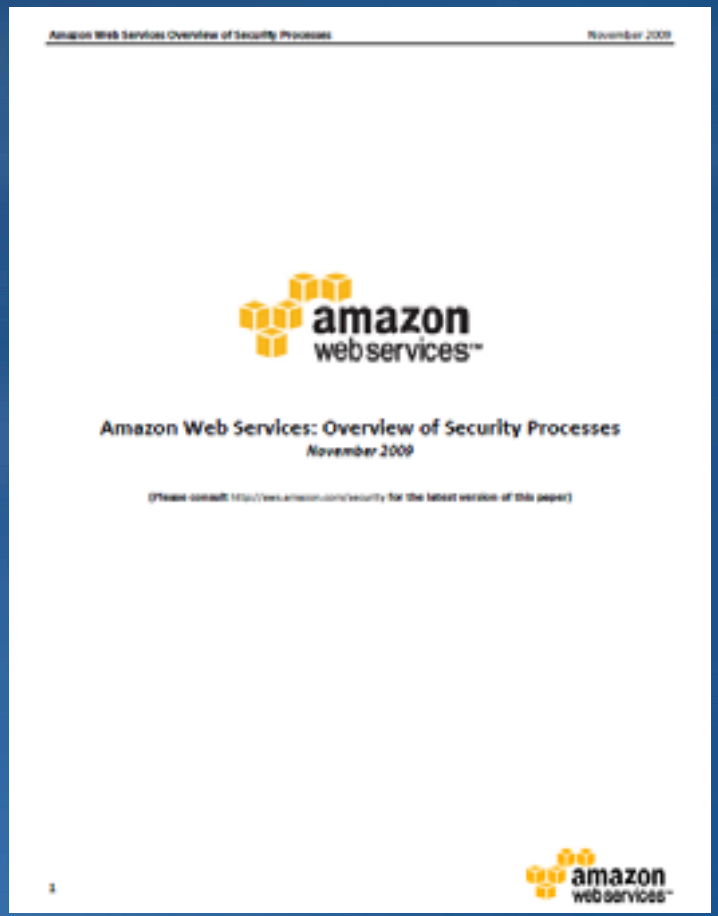
CJ Moses, Senior Manager

AWS Enterprise & Federal

cmoses@amazon.com

AWS Security Resources

- http://aws.amazon.com/security/
- Security Whitepaper
- Latest Version 11/09
- Updated bi-annually
- Feedback is welcome



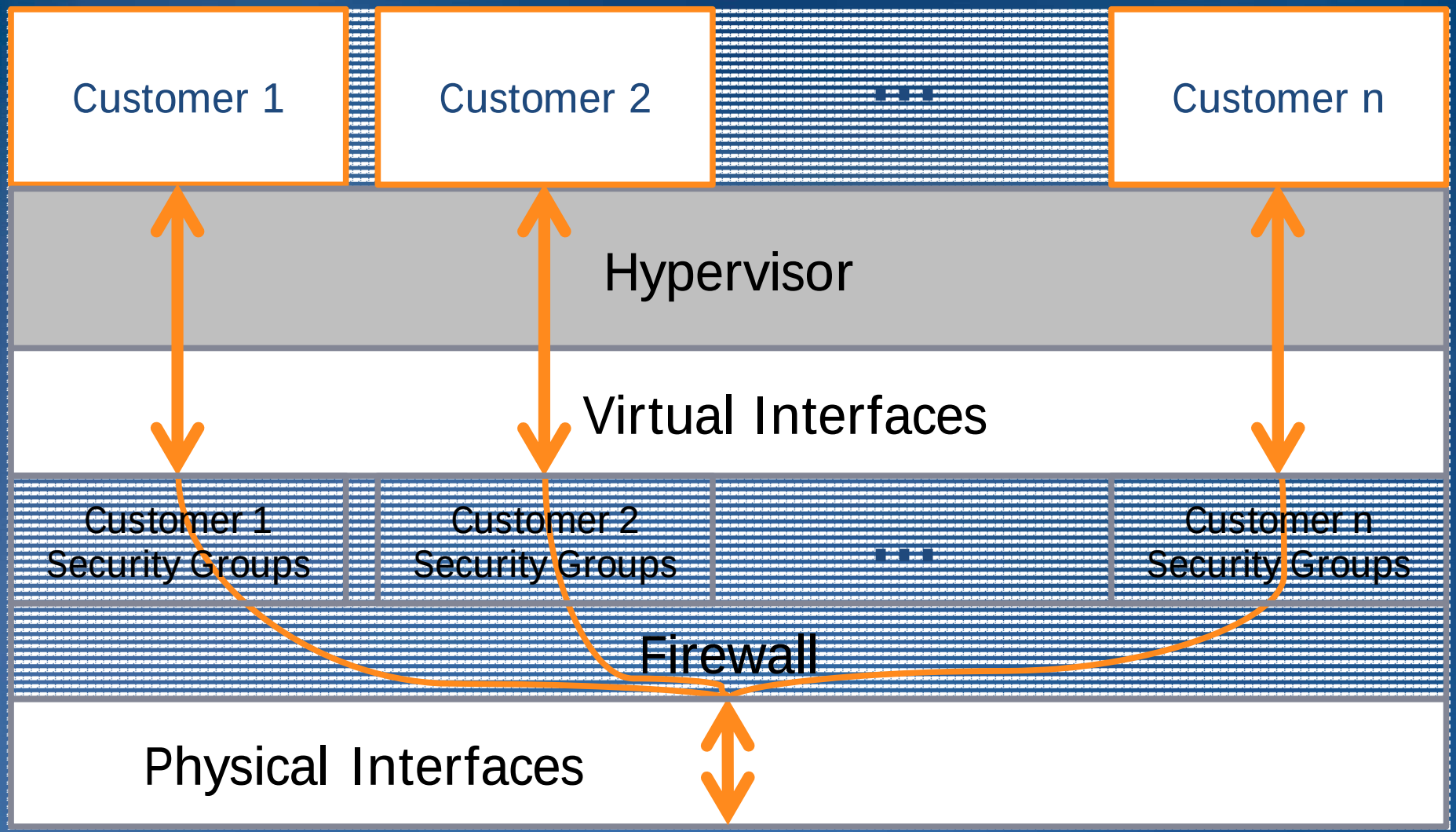
AWS Certifications

- Shared Responsibility Model
- Sarbanes-Oxley (SOX)
- SAS70 Type II Audit
- Working on FISMA (NIST)C&A
- Pursuing additional certifications
- Customers have deployed various compliant applications such as HIPAA (healthcare) and PCI DSS (credit card)

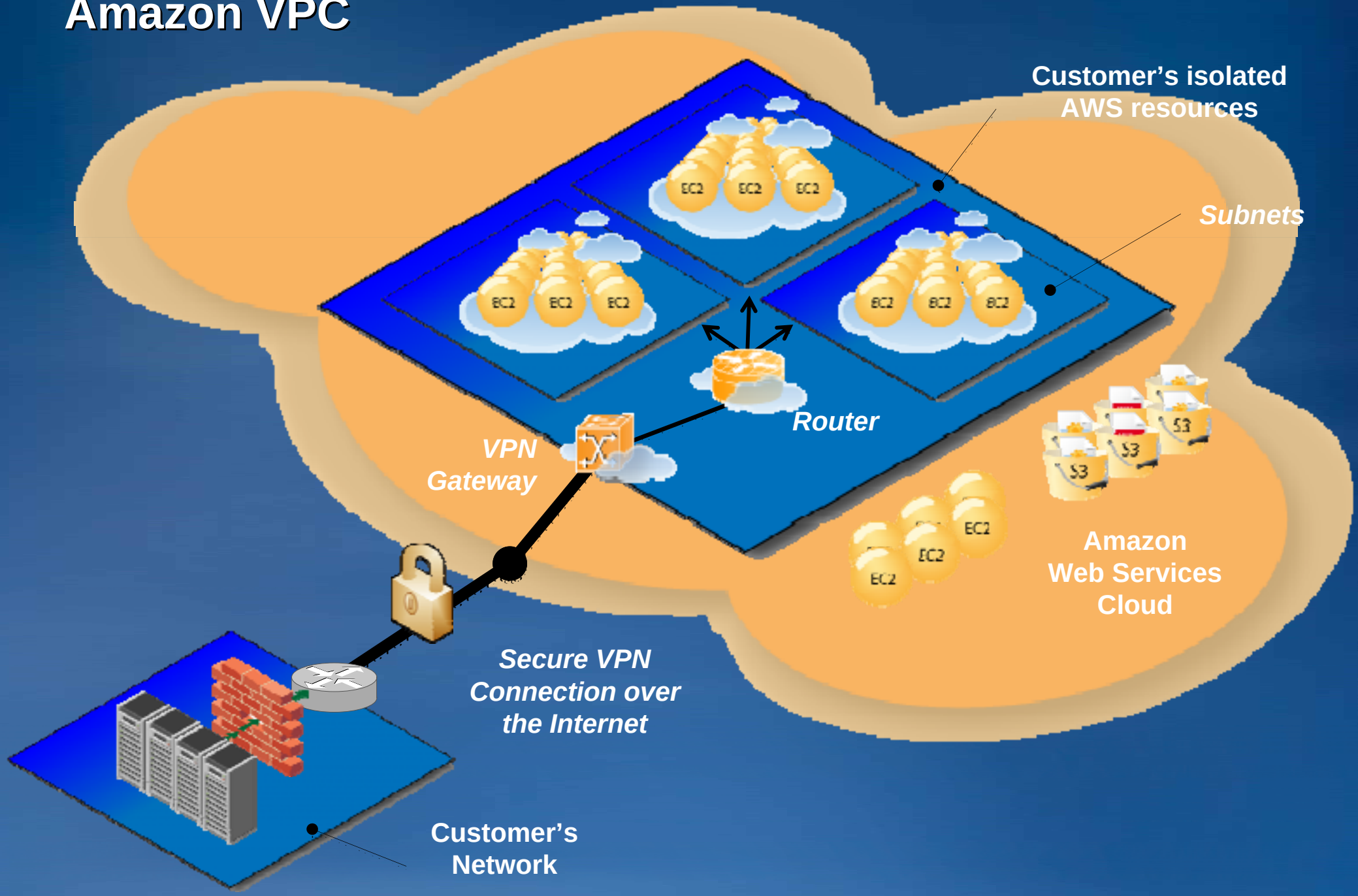
Amazon EC2 Security

- Host operating system
  - Individual SSH keyed logins via bastion host for AWS admins
  - All accesses logged and audited
- Guest operating system
  - Customer controlled at root level
  - AWS admins cannot log in
  - Customer-generated keypairs
- Stateful firewall
  - Mandatory inbound firewall, default deny mode
- Signed API calls
  - Require X.509 certificate or customer's secret AWS key

Amazon EC2 Instance Isolation



Amazon VPC


Customer's isolated
AWS resources
Subnets
EC2
Router
VPN
Gateway
S3
Amazon
Web Services
Cloud
Secure VPN
Connection over
the Internet
Customer's
Network

Amazon VPC Capabilities

- Create an isolated environment within AWS
- Establish subnets to control who and what can access your resources
- Connect your isolated AWS resources and your IT infrastructure via a VPN connection
- Launch AWS resources within the isolated network
- Use your existing security and networking technologies to examine traffic to/from your isolated resources
- Extend your existing security and management policies within your IT infrastructure to your isolated AWS resources as if they were running within your infrastructure

Thank You

Please reserve additional questions for the end of the presentation

aws.amazon.com

cmoses@amazon.com

NEW Integrated Security Model

New Integrated Security Model

- New configuration option
  - Identity of end user flows through all architecture tiers

- What's the Big Deal?
  - Provides Fine Grained Access Control / Row-level security capabilities
  - DCOM Local Connections can now be restricted at service level via ArcGIS Manager

- Looking for customers to provide additional validation
  - Validation / recommendations can lead to Production Support
  - Performance, Scalability and Usefulness are key outstanding concerns

New Integrated Security Model

Current Use-Case Architecture

Web Server

- MS IIS
- Windows Integrated Authentication
- Java and .NET ADF Applications

Application Server

- .NET ArcGIS Server 9.3 SP1 or later
- Windows Users & Groups Security Provider

Oracle Database

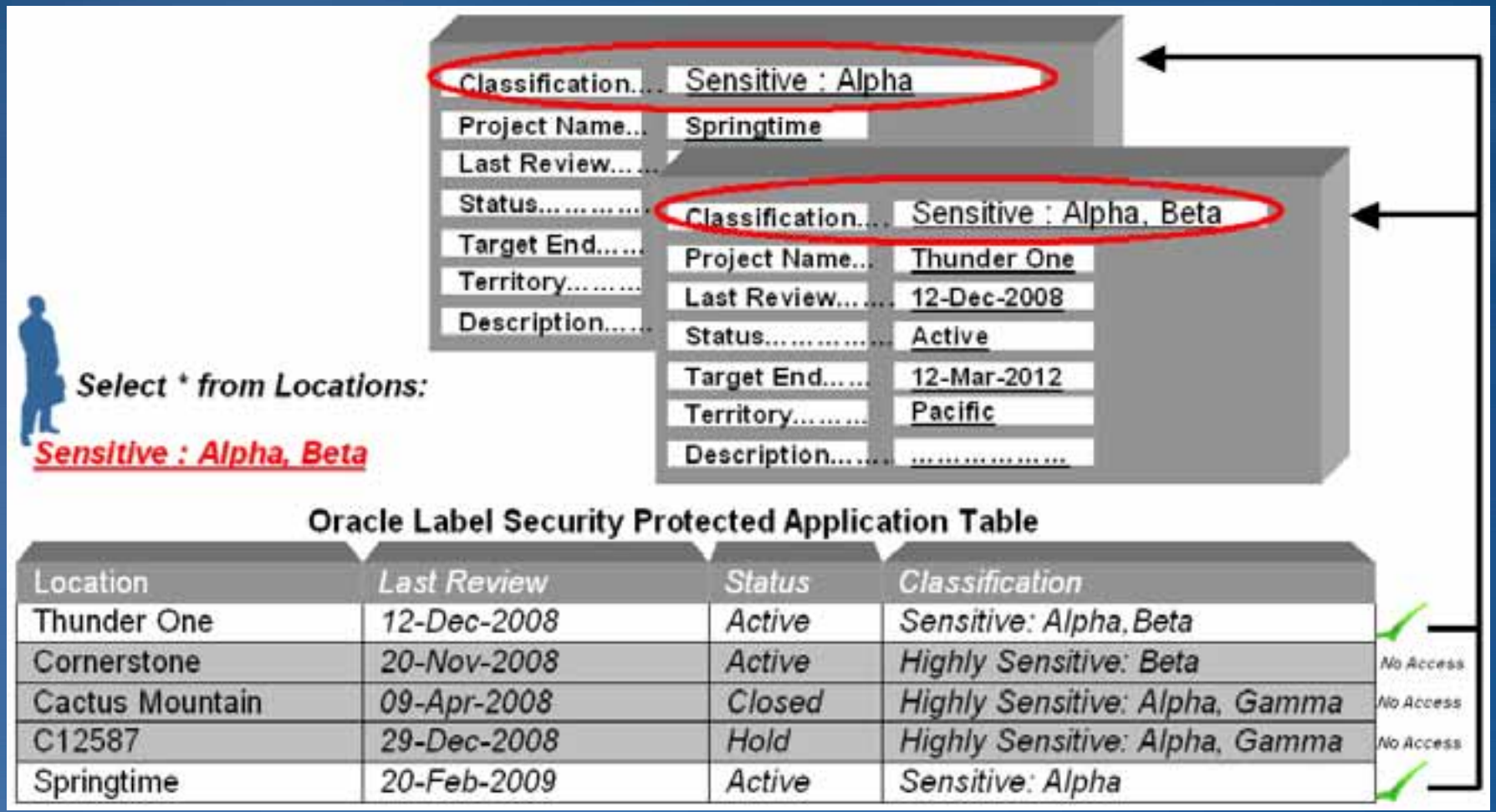
- Virtual Private Database
- Proxy user sessions
- Oracle Label Security (Optional)

Additional Configurations Pending Customer Demand

New Integrated Security Model

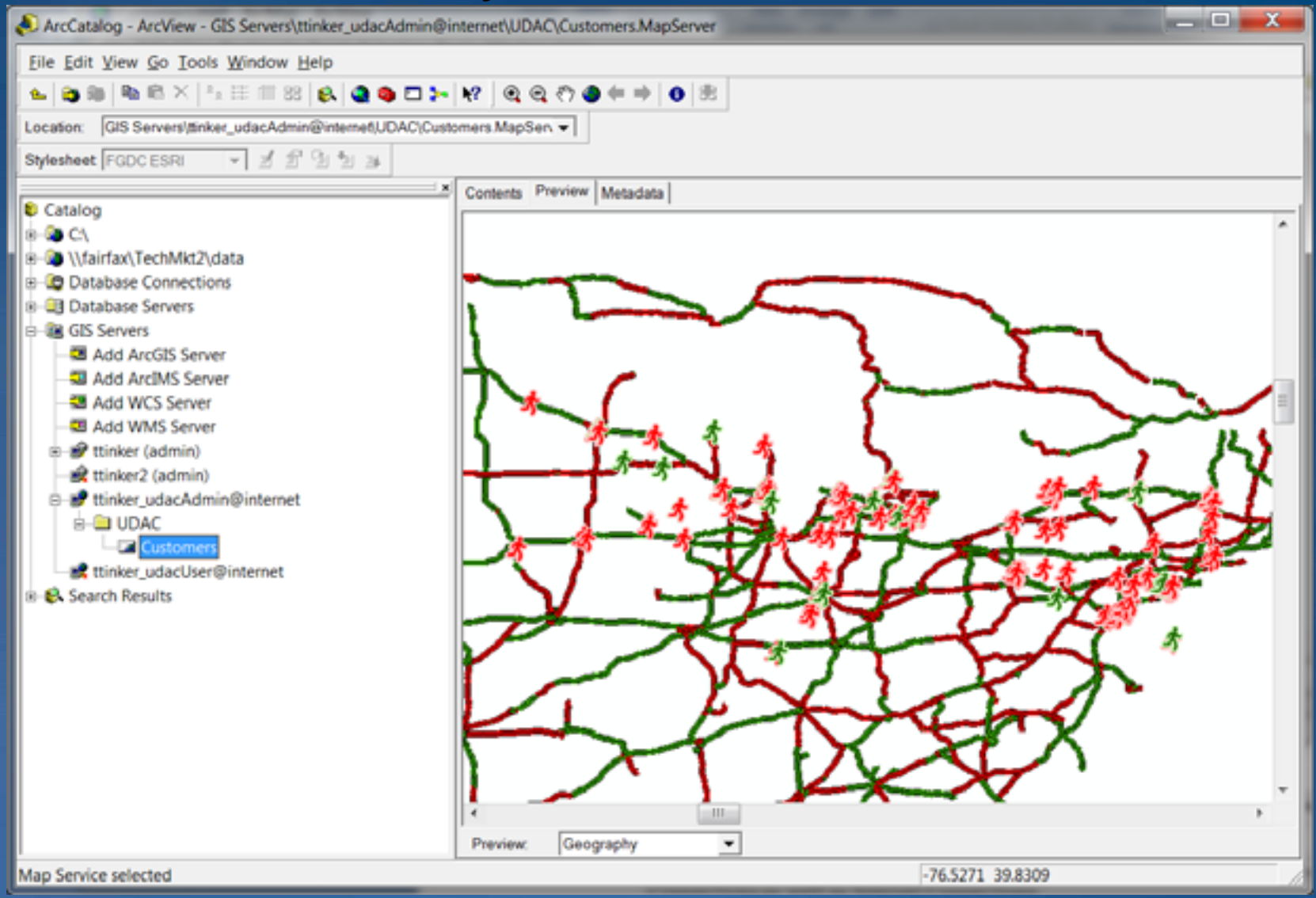
Utilizing Row-Level Security

- **Virtual Private Database (VPD)**
  - Transparently modifies requests
  - Presents partial table view
- **Oracle Label Security (OLS)**
  - Optional add-on
  - Provides interface for row-level security



New Integrated Security Model

A Quick Peek At Row Level Security

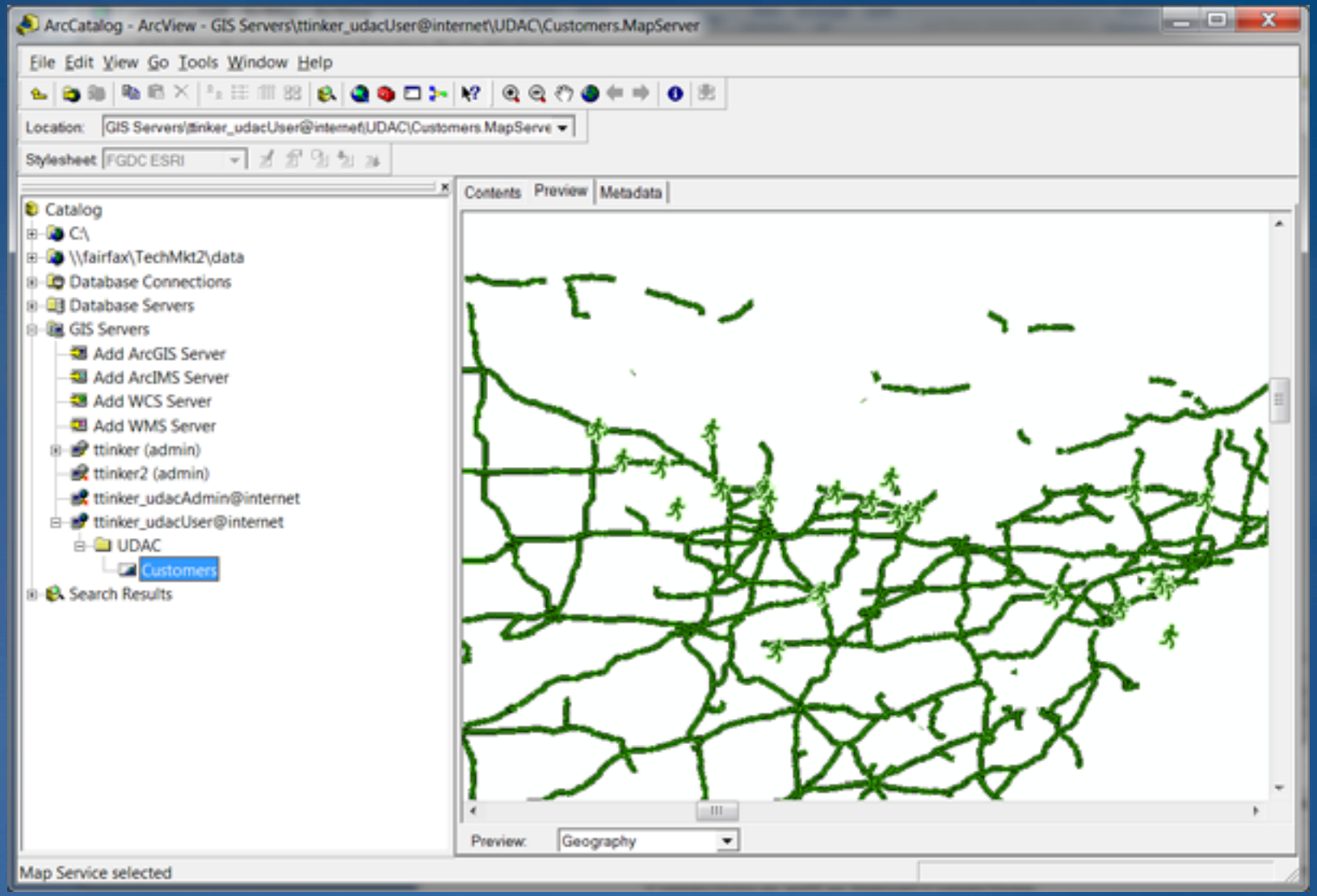


Web Service User with Permissions to both

High (Red) and Low (Green) Features

New Integrated Security Model

Geospatial Security Paradox



***As Expected**, a web service user with Low access only shows Green (Low)*

***Paradox** - Lack of information in some areas can actually be information*

Gaps in road features above can be intuitively "filled in"

ESRI Security Compliance

ESRI Security Compliance

Compliance and Certifications

- FDCC (Federal Desktop Core Configuration)
  - ESRI fully supports and tests product compatibility since 9.2
- FISMA certification and accreditation
  - ESRI hosts low risk category environments
- ESRI's Security Patterns
  - Based on NIST/FISMA guidance
  - Not provided as full certification compliance representations
- High risk security environments
  - Many successful ESRI software product deployments
- Classified environment products and systems
  - ESRI does not certify, function is performed by the system owner
- Additional compliance / certifications
  - ESRI continues to evaluate customer needs

ESRI Security Compliance

Regulations and Standards

- **ESRI Security Patterns**
  - **Based on NIST guidance**
  - **Contain backbone of most security regulations and standards**
- **Managing each regulation/standard individually is ineffective**
  - **Unified approach to information security compliance**
  - **NIST Standards operate as baseline**
  - **Layer in applicable laws, regulations for industry compliance**

TABLE 1. SUGGESTED SAFEGUARDS

SECURITY PRACTICE (E.G., ISO 17799 OR NIST 800)	HIPAA STANDARDS	GLBA (FTC REGULATIONS)	21 C.F.R. PART 11	PCI DSS	LAWS OR NOTICE OF SECURITY BREACH GUIDELINES)
ADMINISTRATIVE SAFEGUARDS					
Security Management Process (e.g., risk analysis, risk management, periodic reviews of effectiveness)	✓	✓	✓	✓	✓
Assigned Security Responsibility (e.g., partial or complete assignment of responsibility for protection of information)	✓	✓	X	✓	✓
Workforce Security (e.g., authorization and/or supervision of workforce or contractors, clearance and termination procedures)	✓	✓	✓	✓	✓
Management of Information Access	✓	✓	✓	✓	✓
Security Incident Procedures	✓	✓	X	✓	✓
Contingency Planning (e.g., data backup plan, disaster recovery plan, emergency mode operation plan, testing and revision procedures, applications and data criticality analysis)	✓	✓	X	✓	✓
Evaluation (e.g., opinion of compliance)	✓	X	X	✓	X
Contracts (e.g., extension of information security through contracts or other written arrangement)	✓	✓	X	✓	✓
Security Awareness and Training (e.g., security reminders, training on malicious software protection, log-in monitoring and password management)	✓	✓	✓	✓	✓
PHYSICAL SAFEGUARDS					
Facility Access Controls (e.g., contingency operations, facility security plan, access control and validation procedures, maintenance records)	✓	✓	X	✓	✓
Workstation Use and Security	✓	✓	X	✓	✓
Device and Media Controls (e.g., disposal, media reuse, accountability)	✓	✓	X	✓	✓
TECHNICAL SAFEGUARDS					
Access Controls (e.g., unique user identification, emergency access procedure, automatic logoff, encryption and decryption)	✓	✓	✓	✓	✓
Audit Controls	✓	✓	✓	✓	✓
Integrity Controls (e.g., mechanism to authenticate data)	✓	✓	✓	✓	✓
Person or Entity Authentication	✓	✓	✓	✓	✓
Transmission Security (e.g., integrity controls or encryption)	✓	✓	✓	✓	✓

ESRI Security Compliance

Summary

- ESRI provides security due diligence with our products and solutions, but is not a security software company
- ESRI recognizes every security solution is unique
- Ultimately, certifications and accreditations are based on a customers mission area and circumstance

Summary and Next Steps

Summary

- Security is NOT about implementing just a technology
  - Understand your organizations GIS risk level
  - Utilize Defense-In-Depth
- Secure Best Practice Guidance is Available
  - Check out the Enterprise GIS Resource Center!
  - Drill into details by mechanism or application type
- Cloud Computing for GIS Has Arrived
  - Security is evolving quickly
  - Security in the cloud is a shared responsibility

Next Steps Supporting Secure Solutions

- **Your Feedback and Insight Today is Essential**
  - **Current Security Issues**
  - **Upcoming Security Requirements**
  - **Feedback on New Integrated Security Model**
  - **Suggestions for the Enterprise Resource Center**
  - **Areas of concern Not addressed Today**

Contact Us At:

Enterprise Security esinfo@esri.com

Michael Young myoung@esri.com

CJ Moses cmoses@amazon.com

Session Evaluation Reminder

Session Attendees:

Please turn in your session evaluations.

. . . Thank you