Designing an Enterprise GIS Security Strategy

Michael E. Young
Agenda

- Introduction
- Esri’s Security Strategy
- Assessing Your Security Needs
- Security Trends
- Enterprise-wide Mechanisms
- Product Security
- Cloud Computing Security
- Summary
Introduction
Introduction

- Michael E Young
  - Esri Senior Enterprise Security Architect
  - Enterprise Implementation Services Team (EIST)
  - FISMA C&A Application Security Officer
  - Certified Information Systems Security Professional (CISSP)

- Application Security Risks Diagram – OWASP 2010
Introduction

• Question
  - Are you happy with your current security?

• 2009 DOE National Lab Security Maxim list
  - True 80-90% of time

  - The “So We’re In Agreement” Maxim
    - If you’re happy with your security, so are the bad guys

• Three DOE National Labs Hacked this year
Introduction

What Does Secure GIS Mean to You?

• Enterprise component integration?
  - Directory Services / LDAP / MS Active Directory

• Standards, Certifications & Regulations?
  - FDCC / FISMA / ISO 2700x / HIPPA

• User Interfaces?
  - ADF, MS Silverlight, Adobe Flex, JavaScript, Rich Clients

• Application vs. security products?
  - ArcGIS Token Service / 3rd Party Single-Sign-On products

• Process, Procedure, Governance?

*Don’t focus on trying to implement a security silver bullet*
Introduction

Designing an Enterprise GIS Security Strategy

- **Identify your Security Needs**
  - Assess your environment
  - Datasets, Systems
  - Sensitivity, Categorization, Patterns

- **Understand Security Options**
  - Enterprise GIS Resource Center
  - Enterprise-wide Security Mechanisms
  - Application Specific Options

- **Implement Security as a Business Enabler**
  - Improve appropriate availability of information
Introduction

Designing an Enterprise GIS Security Strategy

Security Risk Management Process Diagram - Microsoft
Esri’s Security Strategy
Esri’s Security Strategy

Reinforcing Trends

**Esri Products**

Discrete products and services with 3rd party security

**IT Trend**

Isolated Systems

Enterprise platform and services with embedded and 3rd party security

Integrated Systems with discretionary access
Esri’s Security Strategy

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

- **Secure GIS Solution Guidance**
  - Enterprise Resource Center
    - [http://resources.arcgis.com/](http://resources.arcgis.com/)
  - Esri security patterns
Esri’s Security Strategy

Foundational Security Principles

• CIA Security Triad
  - Confidentiality
  - Integrity
  - Availability

• Defense in Depth
  - Layers of security across your enterprise
Esri’s Security Strategy

Defense in Depth

- Authentication
- Authorization
- Filters
- Encryption
- Logging

- Technical Controls
- Policy Controls
- Physical Controls
- Data and Assets
Esri’s Security Strategy

Security Patterns

- Esri security implementation patterns
  - Best practice security guidance
- Leverage
  - National Institute of Standards and Technology (NIST)
- Based on risk level
  - First identify your risk level

To prioritize information security and privacy initiatives, organizations must assess their business needs and risks.
Identifying Your Security Needs
Identifying Your Security Needs

- Assess your environment
- Datasets, Systems, Users
- Sensitivity, Categorization
Identifying Your Security Needs

Assess Your Environment

- Choose a security standard
- Perform an assessment relative to standard metrics

*The 2010 State of Cybersecurity from the Federal CISO’s Perspective*
Identifying Your Security Needs

Identify Sensitive geospatial datasets

- **Legislation/Policies/Permits**
  - E.g Privacy Act - Individual identifiable, either directly by georeferenced information or indirect amalgamation

- **Confidentiality**
  - Data is considered confidential by an organization or its use can be economically detrimental to a commercial interest

- **Natural Resource Protection**
  - Information can result in the degradation of an environmentally significant site or resource

- **Cultural Protection**
  - Information can result in the degradation of an culturally significant site or resource

- **Safety and Security**
  - Information can be used to endanger public health and safety.

*Best Practices for Sharing Sensitive Environmental Geospatial Data*
Identifying Your Security Needs

Categorization, Patterns

• Formal
  - NIST Security Categorization Process

  ![Diagram](image.png)

• Informal
  - Simple scenarios Esri customers can relate to
Identifying Your Security Needs

Informal Pattern Selection

- **Basic**
  - No sensitive data – public information
  - All architecture tiers can be deployed to one physical box

- **Standard**
  - Moderate consequences for data loss or integrity
  - Architecture tiers are separated to separate systems
  - Potential need for Federated Services

- **Advanced**
  - Sensitive data
  - All components redundant for availability
  - 3rd party enterprise security components utilized
Identifying Your Security Needs

**Basic Security**

- **Common Attributes**
  - Utilize data and API downloads from public clouds
  - Secure services with ArcGIS Token Service
  - Separate internal systems from Internet access with DMZ
  - Reverse Proxy to avoid DCOM across firewalls
Identifying Your Security Needs

Standard Security Attributes

- Web Application Firewall on Reverse Proxy
- Dynamic ArcGIS Tokens
- Separate tiers w/VLANs - Web, Database and Management
- Multi-Factor authentication for External users
- Separate Management traffic connections
- Redundant components
- Local copies of all high-availability data
- Install API’s on Local ArcGIS Server for Internal Users
- Intrusion Prevention/Detection Systems
- Lock down ports, protocols, services (Hardening Whitepaper)
- Standardize system images (SMS Whitepaper)
- Host-based firewalls on systems
- Browser plug-in restrictions
Identifying Your Security Needs

Advanced Security Attributes

- Minimal reliance on external data/systems
- Separate datasets (e.g. Public, Employees, Employee Subset)
- Consider explicit labels
- Clustered Database w/Transparent Data Encryption
- Public Key Infrastructure (PKI) certs
- Local user access via Multi-Factor Authentication
- Remote user access via Hardware Token Multi-Factor
- Network connections redundant w/ IPSec between servers
- SSL/TLS between Clients and Servers (Web and Rich Clients)
- Network Access Control (NAC)
Security Trends

# Cyber Security Articles Over Time
Security Trends

Breaches

• 2011
  - Citigroup – 360,000 Credit card accounts
  - Sony – 100+ Million accounts – Recovery over $200 mill
  - RSA – The security company hacked
  - Lockheed – Compromise via discoveries from RSA hack
  - DOE – 3 National Labs This Year (Spearfishing)
  - FBI, CIA, PBS, Electronic Arts… and more…

• Security Expert Conclusion (SANS 7/6/2011)
  - Cost of successful attack against targets of choice has fallen dangerously low

• Why?
  - Financial Harm/Gain
  - Company Retribution
Security Trends

Types of Attacks

- 2010 CSI Survey
  - Continuing increase
  - Phishing
  - Malware infection
- Key solutions
  - Log Management
  - Dashboards
Security Trends

Security Technologies Utilized

- Anti-virus software: 97.0% (2010), 84.6% (2009)
- Firewall: 94.9% (2010), 79.1% (2009)
- Anti-spyware software: 66.2% (2010), 79.1% (2009)
- Virtual Private Network (VPN): 67.5% (2010), 79.1% (2009)
- Vulnerability / Patch Management: 62.4% (2010), 67.5% (2009)
- Encryption of data in transit: 66.2% (2010), 67.5% (2009)
- Intrusion detection system: 59.8% (2010), 67.5% (2009)
- Encryption of data at rest (in storage): 59.8% (2010), 59.4% (2009)
- Web / URL filtering: 59.4% (2010), 59.4% (2009)
- Application firewall: 58.5% (2010), 58.5% (2009)
Security Trends

Cybersecurity Evolving

• Compliance
  - Shift from compliance-based to continuous monitoring / prioritization
  - 20 Critical Security Controls excellent example

• Location / Privacy concerns
  - More applications utilizing current user location to deliver content
  - Proposed Bills Address Geo-Location Data Privacy (6/15/11)
    - Inform users about what type of information is being collected
    - Obtain permission from consumers before sharing geo-location data

• Geolocation Aggregation
  - Creepy - Pinpoints location of targeted individuals via geotagged pictures and social networking services
Security Trends

What is the response?

• Cybersecurity becoming a business process

• IT/Security teams must now know
  - Where data resides
  - Where it moves
  - How to protect it

• Requires comprehensive data security practice
  - Security teams will become business process experts to keep the bad guys disarmed while keeping the good guys productive
Enterprise-wide Security Mechanisms
Enterprise-Wide Security Mechanisms

- Authentication
- Authorization
- Filters
- Encryption
- Logging/Auditing
Enterprise-Wide Security Mechanisms

Authentication – 3 ArcGIS Server Schemes

• Web Traffic via HTTP
  1. Web Services
  2. Web Applications

• Intranet Traffic via DCOM
  3. Local Connections
Enterprise-Wide Security Mechanisms

**Authentication**

<table>
<thead>
<tr>
<th>Access Restricted</th>
<th>Authentication Method</th>
<th>Protocol</th>
<th>Description</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Service or Web Application</td>
<td>None</td>
<td>HTTP</td>
<td>Default Internet Connections</td>
<td>N/A</td>
</tr>
<tr>
<td>Web Service or Web Application</td>
<td>Basic Digest Windows Integrated</td>
<td>HTTP (SSL optional)</td>
<td>Browser built-in pop-up login dialog box.</td>
<td>Basic None, unless using SSL</td>
</tr>
<tr>
<td>Web Service or Web Application</td>
<td>Java EE Container</td>
<td>HTTP (SSL optional)</td>
<td>Web container provides challenge for credentials</td>
<td>Container Managed</td>
</tr>
<tr>
<td>Web Application Only</td>
<td>Client Certificates PKI Smart Cards</td>
<td>HTTPS</td>
<td>Server authenticates client using a public key certificate</td>
<td>PKI Managed</td>
</tr>
<tr>
<td>Web Application Only</td>
<td>.NET Form-based</td>
<td>HTTP (SSL optional)</td>
<td>Application provides its own custom login and error pages.</td>
<td>None, unless using SSL</td>
</tr>
<tr>
<td>Web Application Only</td>
<td>Java ArcGIS Managed</td>
<td>HTTP (SSL optional)</td>
<td>ArcGIS Server provides login page for Java Web App</td>
<td>None, unless using SSL</td>
</tr>
<tr>
<td>Web Only</td>
<td>Esri Token</td>
<td>HTTP (SSL optional)</td>
<td>Cross Platform, Cross API Authentication</td>
<td>AES-128bit</td>
</tr>
<tr>
<td>Local</td>
<td>Windows Integrated</td>
<td>DCOM</td>
<td>Default Local Connections OS Groups AGSUser AGSAdmin</td>
<td>OS Managed</td>
</tr>
</tbody>
</table>
Enterprise-Wide Security Mechanisms

Authentication – User and Role Storage Options

- **Java Options**
  - *Default* – Apache Derby
  - External Database
  - LDAP
  - MS Active Directory

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

Authorization – Role Based Access Control

- **Esri COTS**
  - Assign access with ArcGIS Manager
  - Service Level Authorization across web interfaces
  - Services grouped in folders utilizing inheritance

- **3rd Party**
  - RDBMS – Row Level or Feature Class Level
    - Versioning with Row Level degrades RDBM performance
    - Alternative - SDE Views

- **Custom - Limit GUI**
  - Rich Clients via ArcObjects
  - Web Applications
    - Sample code Links in ERC
    - Microsoft’s AzMan tool
Enterprise-Wide Security Mechanisms

Filters – 3rd Party

- Firewalls
- Reverse Proxy
  - MS free reverse proxy for IIS 7 (Windows 2008)
- Web Application Firewall
  - Open Source option ModSecurity
- Anti-Virus Software
- Intrusion Detection / Prevention Systems
- Limit applications able to access geodatabase
Enterprise-Wide Security Mechanisms

Filters – Firewall Friendly Scenario

- Web Application Firewall (WAF) in DMZ
- File Geodatabase (FGDB) in DMZ
  - One-way replication via HTTP(s)
  - Deployed to each web server for performance
  - Internet users access to subset of Geodatabase
Enterprise-Wide Security Mechanisms

Filters

• Why no Reverse Proxy in DMZ?
  - One-off component / no management, minimal filtering

• Multi-Function Web Service Gateways
  - Store SSL Certificates / SSL Acceleration
  - URL Rewrite
  - Web Application Firewall
Enterprise-Wide Security Mechanisms

Encryption – 3rd Party Options

- **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
  - ArcGIS Workflow Manager
    - Track Feature based activities
  - ArcGIS Server 10 Logging
    - “User” tag allows tracking of user requests

- **3rd Party**
  - Web Server, RDBMS, OS, Firewall
  - Consolidate with a SIEM

86% of victims had evidence of the breach in their logs, yet 61% of the breaches were discovered by a third party

*Verizon’s 2010 Data Breach Investigations Report*
Product Security Options

Rich Clients
Mobile
ArcGIS Server
Cloud Services
Rich Client Security
Rich Client Security

Desktop

- Client typically with most access to sensitive data
- Variety of system connections
  - Direct Connect – RDBMS
  - Application Connect – SDE
  - HTTP Service – GeoData Service
    - Integration with Token Service
    - Windows native authentication
  - SSL and IPSec Utilization
- ArcObject Development Options
  - Record user-initiated GIS transactions
  - Fine-grained access control
    - Edit, Copy, Cut, Paste and Print
Rich Client Security

**ArcGIS Explorer Communication**

- Explorers for different users or topics
- Focused data and functions in one place
- You manage and customize

---

**Explorers**

- Sales Explorer
- Marketing Explorer
- Your customers’ Explorer

**Frontend**


**Data Management**

- Centrally managed configurations
- G:\SalesData
- \MKT\data
Mobile Phone Security
Mobile Phone Security

• More
  - Platforms
    - ArcPad
    - ArcGIS Mobile
    - iPhone
    - Android
    - Windows 7
  - Functionality/Storage
  - User-base

• Leads to
  - Increased Hacker Attention
Mobile Phone Security

ArcGIS Mobile Security Touch Points

- SDE permissions
- Server authentication
- Service authorization
- Communication
- Device access
- Storage
- Project access
- Data access
Mobile Phone Security

ArcGIS Mobile

- Encrypt Communication
  - HTTPS (SSL) or VPN tunnel
- Web Service Authentication / Authorization
  - Windows Authentication or Token Service
  - Filter by OS / IP / Unique Device Identifier
- Encrypt data at Rest
  - Windows Mobile Crypto API
  - 3rd Party tools for entire storage system
- Mobile Device Management
  - Good Technology…
ArcGIS Server Security
ArcGIS Server Security

Common Questions/Issues

- **Is Communication Across Wire Secure by Default?**
  - No
    - Communication via ArcGIS Server and all clients is clear-text by default
    - Secure web communication with an SSL Certificate
    - Secure internal DCOM communication with IPSec
ArcGIS Server Security

Common Questions/Issues

- Is a reverse proxy required?
  - No
    - Some customers implement to eliminate DCOM traffic across firewalls
    - Used with Web Application Firewall improves security posture
ArcGIS Server Security

Common Questions/Issues

• Is there Security Hardening Guidance?
  - Yes
    - Check out the ERC Implementation Gallery
    - Next update expected in 2011 - Version 10 Win 2k8
ArcGIS Server Security

Common Questions/Issues

- Should I assign the Everyone group to the root in ArcGIS Manager?
  - Depends
    - Everyone will have access to your services by default
    - OK for Basic security risk environments
    - NOT recommended for any Standard or Advanced security
    - Deny by default used in higher risk environments
ArcGIS Server Security

Common Questions/Issues

- Can I provide security more granular than service level?
  - Yes
    - SDE Views or 3rd Party Software
    - Integrated security model
ArcGIS Server Security

Flowing web user identity down to the database

- **Integrated Security Model (ISM)**
- **Flow web user identity to database via proxy user**
  - Logging - Non-repudiation across all architecture tiers for high risk security environments
  - Row-Level Security - Database driven security model for high-risk security environments

- **Current Status**
  - Customer scenarios collected
  - Simple layer level security performance validation completed
    - 10-20% performance overhead
  - More complex scenarios to be validated next
  - Basic documentation online for Java ArcGIS Server
ArcGIS Server Security
ISM Initial Validation Configuration

- Web Server
  - MS IIS

- Application Server
  - Java ArcGIS Server 10
  - LDAP (Derby) Users & Groups Security Provider

- Oracle Database
  - Proxy user sessions
  - Table level access (Layer security)
Integrated Security Model

A Quick Peek At Row Level Security

Web Service User with Permissions to both High (Red) and Low (Green) Features
Integrated Security Model

Geospatial Security Paradox

As Expected: Web service user with Low access only shows Green (Low)
Paradox: Lack of information can be information. Road gaps above can be intuitively “filled in”
ArcGIS Server Security

Security Model
ArcGIS Server Security

User Local Access to SOM

- **Windows**
  - Access managed by operating system of SOM machine
- **Solaris and Linux**
  - Users managed by ArcGIS Server Manager
- **Add users to appropriate group**
  - Simplistic access levels (None, Read, Full)

<table>
<thead>
<tr>
<th>agsadmin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add, delete, or modify services</td>
</tr>
<tr>
<td>Start, stop, or pause services</td>
</tr>
<tr>
<td>Add, remove, or modify server directories</td>
</tr>
<tr>
<td>Create Web mapping applications</td>
</tr>
<tr>
<td>Add or remove SOC machines</td>
</tr>
<tr>
<td>View statistical information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>agsusers</th>
</tr>
</thead>
<tbody>
<tr>
<td>View and access services</td>
</tr>
</tbody>
</table>
ArcGIS Server Security

Server Data Access

• Share folders that contain GIS resources
  - Grant SOC account
    Read and/or Write permission
to the folder

• Add SOC as a user of your database
  - Grant SOC account
    Read and/or Write permission
to each geodatabase
ArcGIS Server Security

Management User Interface Access

• ArcGIS Services Directory
  - Available as part of ArcGIS Server installation
  - Typically not exposed for Standard security needs to public

• REST API Admin
  - Manages access to local ArcGIS Services Directory
  - Maintains REST cache
  - Requires membership in agsadmin group
  - Recommend to configure no public access

• ArcGIS Manager
  - Recommend to configure no public access
ArcGIS Server Security

GIS resource access

Local security

Service capabilities

Web security

Internet

Intranet

http://...

ArcGIS Server

No web editing
ArcGIS Server Security

Implementing Web Access Control

1. Implement SSL
2. Choose user/role store
3. Assign users to roles (as necessary)
4. Assign roles to resources
5. Enable security
ArcGIS Server Security

Authenticating to services with Token

• What is a token?

• Why do you need it?
  - Services don’t have a logon user interface

• How does it work?
  - ArcGIS Server Token Service

• Where do you get it?
  - Request a Token from Token Service
ArcGIS Server Security

Web Service API Security Options

- **Embed Token**

- **Bind token in a proxy page**

- **Write full logon access to the token service** (e.g., ArcGIS Desktop, custom application)

Diagram:

- Web Server
- ArcGIS SOAP/REST
- Proxy page
- Secured container
- Token
- Token
- User
  - Password
- Token
- https://...
ArcGIS Server Security

Version 10 Security Enhancements

• AGS Manager
  - Searchable user/roles
  - Application Level User Activity Logging

• Database level security option
  - Added to REST API
  - Passes user context to database
  - Control all data access at data tier

• Web Service Interface Security Improvements
ArcGIS Server Security

What lays ahead?

- ArcGIS Server 10.1
  - Say goodbye to DCOM
  - Adding a publisher role
  - Administrative API access
Geospatial Cloud Computing

Security
Geospatial Cloud Security

Is Cloud computing safe?
- Classic answer: It depends...

Security Benefits
- Virtualization / Automation
  - Expedite secure configurations with images
- Broad network access
  - Reduce removable media needs
  - Segmentation - Public data -> Cloud & sensitive -> Internal
- Potential economies of scale
  - Lower cost backup copies of data
- Self-service technologies
  - Apply security controls on demand
Geospatial Cloud Security

Risks

• Vendor Practice Dependence
  - Potential sub-standard security controls
  - Loss of governance over data

• Vendor Lock-In
  - Services termination data loss
  - Portability
  - Lost internal capabilities to support

• Sharing resources (Multi-tenancy)
  - Access to other’s data
  - Unclear security responsibilities
  - Increased data transmitted = Increased disclosure risk

• Deployment Model Threat Exposure Levels
  - Private = Lowest    Community = More    Highest = Public
Geospatial Cloud Security

Cloud platforms utilized by Esri

- **System Admin Access (IaaS)**
  - ArcGIS Server on Amazon EC2
  - Terremark Cloud (Now Verizon)
  - Private Cloud

- **Developer Access (PaaS)**
  - Esri Web Mapping APIs (JavaScript, Flex, Silverlight)
  - Microsoft Azure ArcGIS Applications

- **End User Solutions (SaaS)**
  - ArcGIS Online
  - Business Analyst Online
  - ArcGIS Explorer Online
Geospatial Cloud Security

Which Cloud Deployment Model?

• Cloud Deployment Location
  - Public (e.g. Amazon)
  - Private (e.g. Internal Corporate)

• Primary driver -> Security

• Organizations from midmarket up, will have a mix of public & private
  - June 2010 IDC IT Executive Survey
Geospatial Cloud Security

What are your Security Needs?

- **Assess your security needs**
  - Data sensitivity
    - Public domain, sensitive, classified
  - User types
    - Public, internal
  - Categorize security needs
    - Basic, standard, advanced

- **Most public cloud implementations are basic**
  - Security similar to social networking sites (Facebook)
  - Most GIS users have only basic security needs
Geospatial Cloud Security

Hot topics

• Data Location
  - International concerns with Patriot Act
  - Some Cloud providers don’t assure location

• Identity Management
  - Long-term vision formulating
    - National Strategy for Trusted Identities (Released 6/25/10)

• Shared Responsibility Model
  - Details not delineated
  - Regulatory compliance questionable
Geospatial Cloud Security

Cloud Best Practices by Platform

**SAAS**
- Don’t replicate your organization in the cloud
- Protect your API Keys

**PAAS**
- Protect private information before sending to cloud
- Do maintain an audit trail
- Protect your API Keys

**IAAS**
- Protect against rogue cloud usage
- Protect your API Keys

CSO: SaaS, PaaS, and IaaS: A security checklist for cloud models
Geospatial Cloud Security

IAAS Best practices

- Similar to internal ops
  - Break up tiers
  - Protect in transit
  - Protect at rest
  - Credential management
  - Built-in OS Firewalls
  - AGS App Security
Geospatial Cloud Security

ArcGIS Server on Amazon EC2

- Default
  - Web and App Tiers combined

- Scaling out
  - Elastic Load Balancing
  - What about supporting infrastructure?
Geospatial Cloud Security

ArcGIS Server on Amazon EC2

- Minimize your administrative attack surface
Geospatial Cloud Security

Amazon EC2 Security

• Secured physical facilities
• Logically secure EC2 instances
• Configurable firewall to control ingress access
• Standard ArcGIS Server security
• Optional multifactor authentication

• What about the users of EC2?
Geospatial Cloud Security

Utilize the security guidelines available

Researchers: AWS Users Are Leaving Security Holes

Researchers in Germany have found abundant security problems within Amazon's cloud-computing services due to its customers either ignoring or forgetting published security tips.

By Jeremy Kirk
Mon, June 20, 2011
Geospatial Cloud Security

Product Specific Guidance

• ArcGIS Server on Amazon EC2
  - AMI not hardened beyond Windows 2008 Server defaults
  - Creating security hardened AMI
    - Part of GeoCloud initiative
  - Basic Esri Online Help guidance
  - Amazon Security Best Practices (Jan 2011)

• ArcGIS Online Sharing Content
  - Online Help – Sharing Content / Participating in Groups
  - Recent SAS70 Type 2 review of Esri hosting services
Summary

Designing an Enterprise GIS Security Strategy

1. **Identify your Security Needs**
   - Assess your environment
   - Utilize patterns

2. **Understand Current Security Trends**

3. **Understand Security Options**
   - Enterprise GIS Resource Center
     - Enterprise-wide Security Mechanisms
     - Application Specific Options

4. **Implement Security as a Business Enabler**
   - Improve appropriate availability of information
Summary

- Security is NOT about 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
  - Professional Services Enterprise GIS Security Assessment

- Cloud Computing for GIS Has Arrived
  - Security is evolving quickly
  - Security in the cloud is a shared responsibility
Summary

Need more?

- **ArcGIS Server Application Security UC Sessions**
  - Building Secure Applications
    - Thurs 1:30-2:45

- **Professional Services Offering**
  - Enterprise GIS Security Review
  - [http://www.esri.com/services/professional-services/implementation/enterprise.html](http://www.esri.com/services/professional-services/implementation/enterprise.html)
Summary

Resources

- Esri Enterprise GIS Resource Center (Security)
  - http://resources.arcgis.com/content/enterprisegis/10.0/security
  - http://gocsi.com/survey
- Web Browser Security Test Results Summary: Q1 2010
  - http://nsslabs.com/test-reports/NSSLabs_Q12010_BrowserSEM_Summ_FINAL.pdf
- Windows on Amazon EC2 Security Guide
  - http://developer.amazonwebservices.com/connect/entry.jspa?externalId=1767
- Selected Documents on Confidentiality and Geospatial Data
- SaaS, PaaS, and IaaS: A Security Checklist
Summary

Resources

• NIST Information Security Publication Website
  - http://csrc.nist.gov/publications/PubsSPs.html

• Providing SSO To Amazon EC2 From An On-Premises Windows Domain

• DOE Argonne National Labs Security Maxims

• GAO Guidance Needed with Implementing Cloud Computing

• FY 2010 Report to Congress on Implementation of FISMA
  - http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf

• Best Practices for sharing sensitive environmental geospatial data (2010)
Summary

Contact Us At:
Enterprise Security esinfo@esri.com
Michael Young myoung@esri.com

Where Do You Need More Security Guidance From Esri?

Don’t Forget To Fill Out Your Survey at:
www.esri.com/sessionevals