ArcGIS Online: Security and Compliance

Michael Young – CISO Products

Randall Williams – Sr. Security Engineer

Esri's Software Security & Privacy Team

Agenda

- Security Priority
- Shared Responsibility Model
  - Esri Responsibilities
  - Customer Responsibilities
- Summary
- Open Q&A Discussion

Security Priority

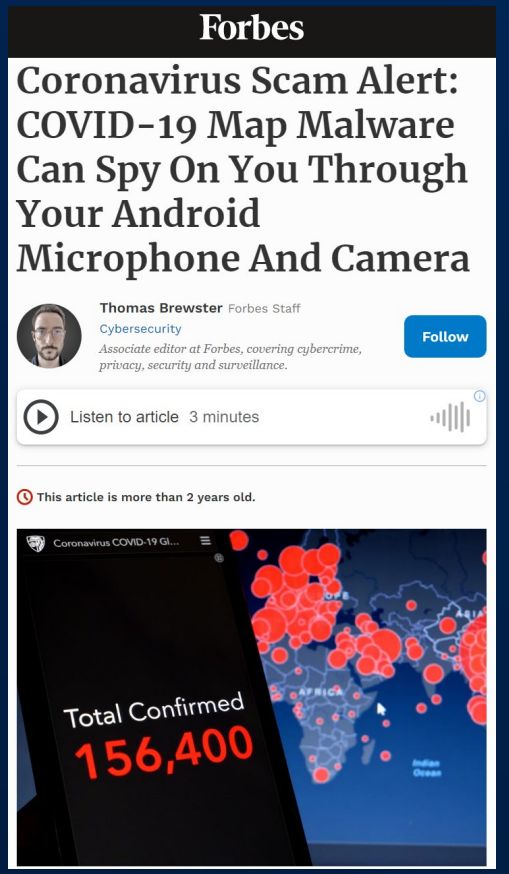
Security Priority

- Security demands affect customer geospatial deployments AND how Esri builds products
  - Recent US Government demand changes stem from
    - 2021 Presidential EO on Improving the Nation's Cybersecurity
    - 2022 FedRAMP Authorization Act

- Geospatial deployments typically no longer operate in isolation and are interconnected with customer operations and cloud-based services
  - Customers shutdown geospatial systems if there is not adequate assurance within hours (Log4j)

- Geospatial datasets are central to media viral stories (Climate, COVID, Racial)
  - Misinformation is rampant, GIS security required to ensure integrity

- GIS datasets are breached as part of cyberattacks or misconfiguration


Forbes

Coronavirus Scam Alert: COVID-19 Map Malware Can Spy On You Through Your Android Microphone And Camera

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.
Follow

Listen to article 3 minutes

This article is more than 2 years old.

Importance of a Secure GIS has Increased Significantly

Shared Responsibility Model

Shared Responsibility

- We've all heard the phrase, "Security is everybody's responsibility"
  - Sometimes this can lead to an incorrect assumption that someone else is responsible for aspects of an organization's security posture
  - How do we realize the goal of this phrase?

- Today we will briefly talk about how the shared responsibility model applies to our offerings
  - Diving deeper into what we address
  - What our customers need to address

Shared Responsibility

- Anything missing for On-Premises responsibilities?

Responsibility	ArcGIS On-Premises	ArcGIS Cloud Images	EMCS Advanced+ *FedRAMP Moderate*	ArcGIS Online *FedRAMP Tailored Low*
Data Classification &Accountability				
Client & End-Point Protection				
Identity and Access Management				
Application Level Controls				
Network Controls				
Physical Security				

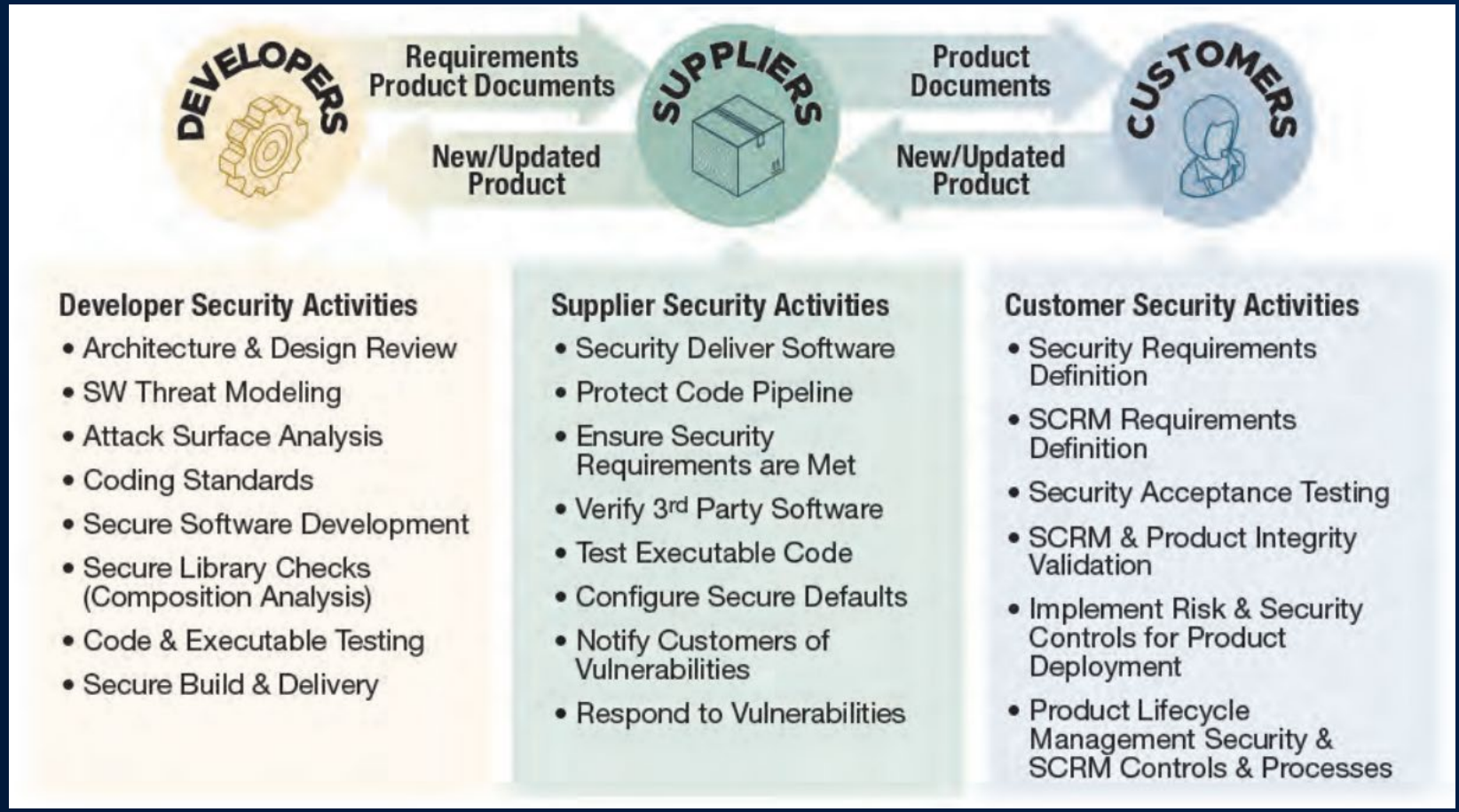
Customer Managed

Cloud Provider Managed

Esri Managed

Shared Responsibility

- For both On-Premises and Cloud scenarios, Esri is responsible for delivering secure products
  - Requirements for measuring a secure product are evolving
  - Expanding to cover full software supply chain
  - See Presidential Executive Order 14028 – May 2021



Esri Security Responsibilities

Esri Responsibilities

DEVELOPMENT

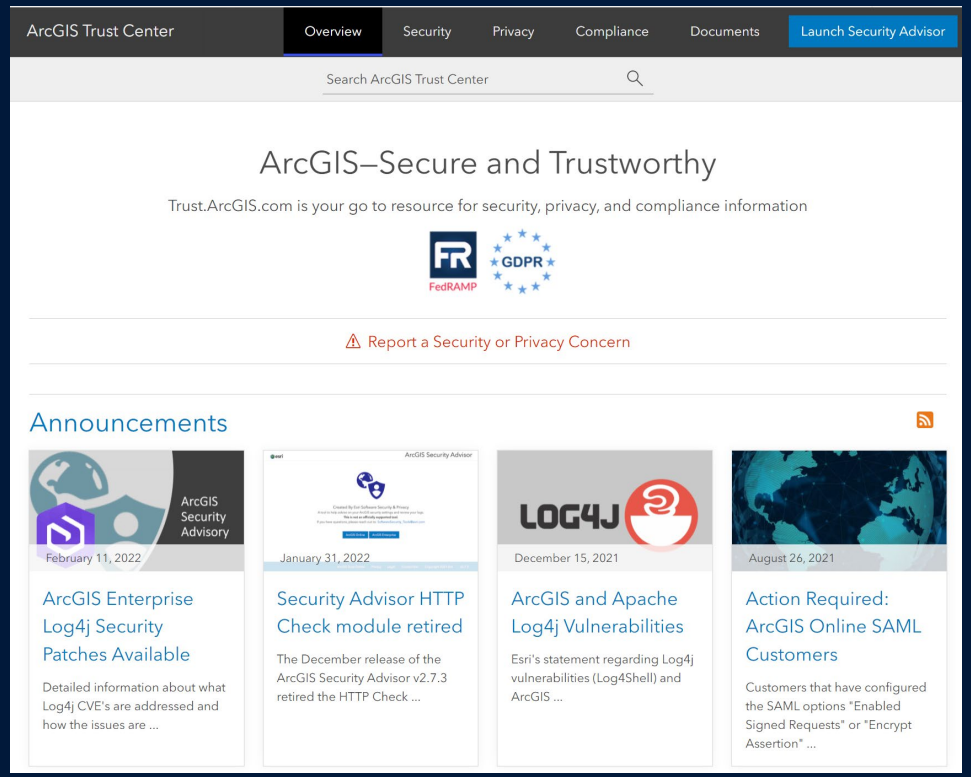
VALIDATION

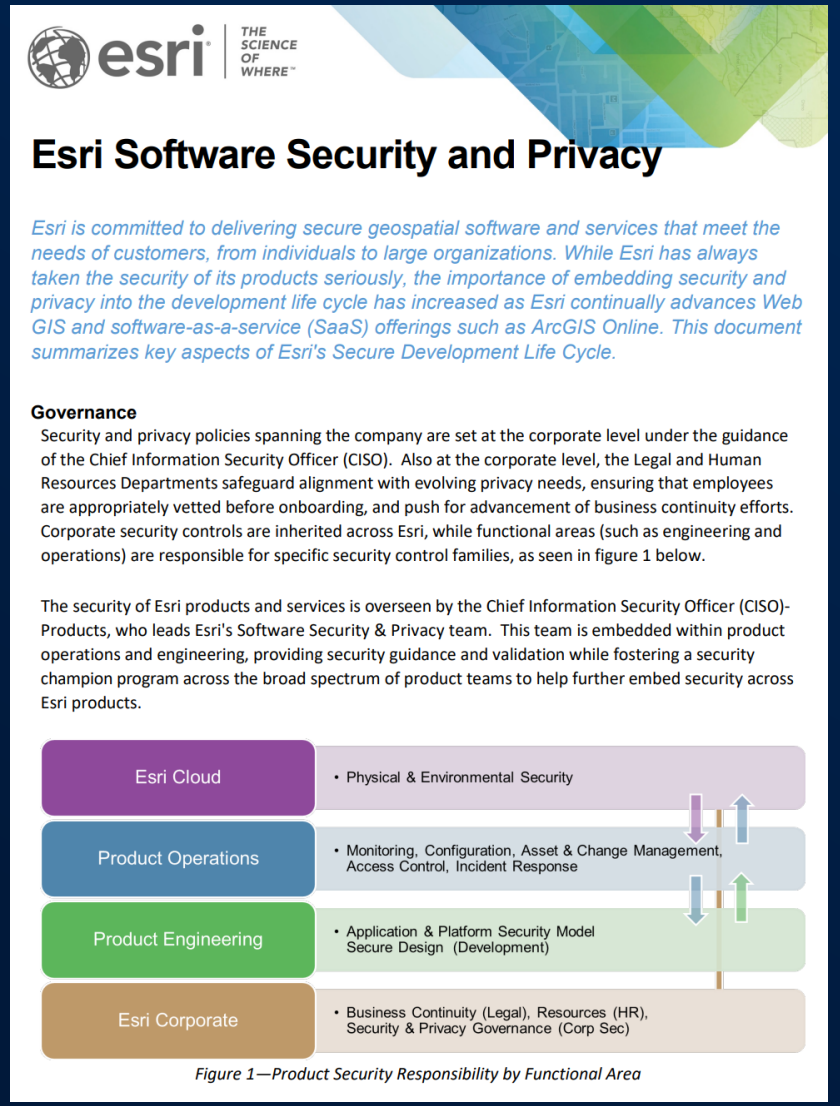
GUIDANCE

Esri Responsibilities

Development

- Overview of Esri Secure Development Lifecycle
  - Trust.ArcGIS.com

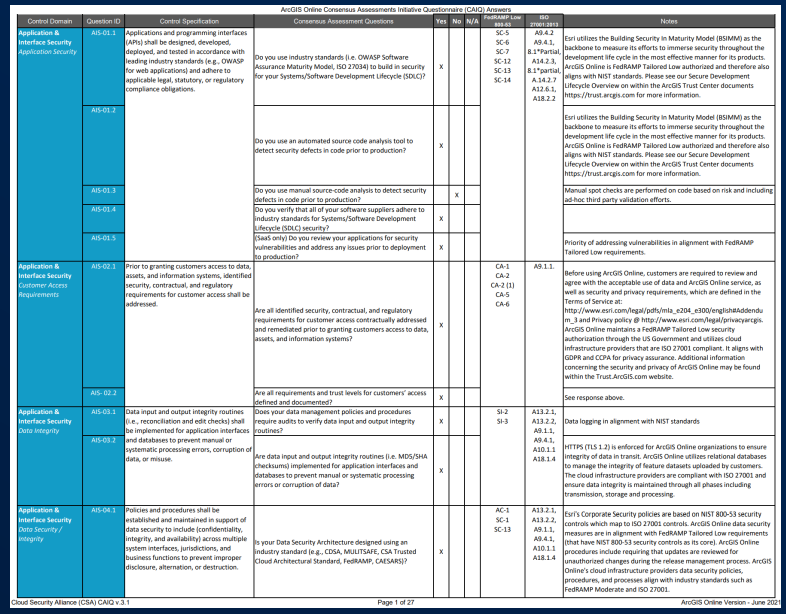




Esri Responsibilities

Validation

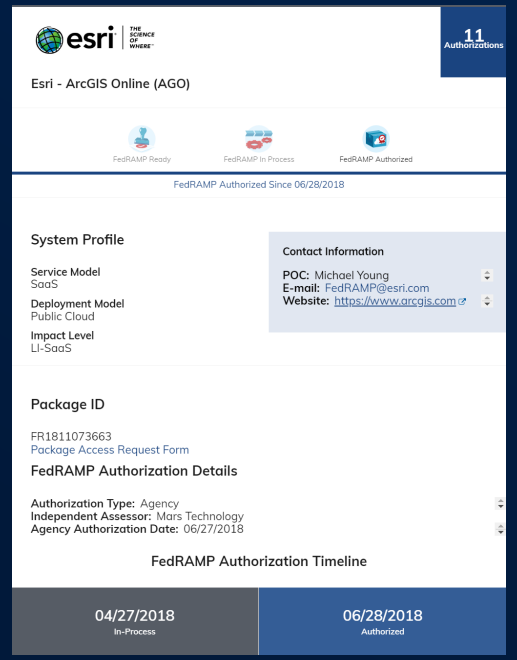
- Publicly available
  - ArcGIS Trust Center
  - Cloud Security Alliance CAIQ – 27 pages
- HIPAA eligible Geocoding service
  - BAA available – Restrictions listed on Trust Center Privacy page
  - Upcoming FedRAMP Moderate and customer feedback allows us to consider additional services based on demand
- Available to Agencies from FedRAMP Marketplace
  - ArcGIS Online FedRAMP package
  - Tailored Low package available now
  - Moderate materials available soon



ArcGIS Online Consensus Assessments Initiative Questionnaire (CAIQ) Answers

Control Domain	Question ID	Control Specification	Consensus Assessment Questions	Yes	No	N/A	FedRAMP Low 800-53	ISO 27001:2013	Notes
Application & Interface Security *Application Security*	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	x			SC-5 SC-6 SC-7 SC-12 SC-13 SC-14	A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2	Esri utilizes the Building Security In Maturity Model (BSIMM) as the backbone to measure its efforts to immerse security throughout the development life cycle in the most effective manner for its products. ArcGIS Online is FedRAMP Tailored Low authorized and therefore also aligns with NIST standards. Please see our Secure Development Lifecycle Overview on within the ArcGIS Trust Center documents https://trust.arcgis.com for more information.
	AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	x					Esri utilizes the Building Security In Maturity Model (BSIMM) as the backbone to measure its efforts to immerse security throughout the development life cycle in the most effective manner for its products. ArcGIS Online is FedRAMP Tailored Low authorized and therefore also aligns with NIST standards. Please see our Secure Development Lifecycle Overview on within the ArcGIS Trust Center documents https://trust.arcgis.com for more information.
	AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?		x				Manual spot checks are performed on code based on risk and including ad-hoc third party validation efforts.
	AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	x					
	AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	x					Priority of addressing vulnerabilities in alignment with FedRAMP Tailored Low requirements.
Application & Interface Security *Customer Access Requirements*	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	x			CA-1 CA-2 CA-2 (1) CA-5 CA-6	A9.1.1,	Before using ArcGIS Online, customers are required to review and agree with the acceptable use of data and ArcGIS Online service, as well as security and privacy requirements, which are defined in the Terms of Service at: http://www.esri.com/legal/pdfs/mla_e204_e300/english#Addendum_3 and Privacy policy @ http://www.esri.com/legal/privacy#arcgis. ArcGIS Online maintains a FedRAMP Tailored Low security authorization through the US Government and utilizes cloud infrastructure providers that are ISO 27001 compliant. It aligns with GDPR and CCPA for privacy assurance. Additional information concerning the security and privacy of ArcGIS Online may be found within the Trust.ArcGIS.com website.
	AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	x					See response above.
Application & Interface Security *Data Integrity*	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Does your data management policies and procedures require audits to verify data input and output integrity routines?	x			SI-2 SI-3	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4	Data logging in alignment with NIST standards
	AIS-03.2		Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	x					HTTPS (TLS 1.2) is enforced for ArcGIS Online organizations to ensure integrity of data in transit. ArcGIS Online utilizes relational databases to manage the integrity of feature datasets uploaded by customers. The cloud infrastructure providers are compliant with ISO 27001 and ensure data integrity is maintained through all phases including transmission, storage and processing.
Application & Interface Security *Data Security / Integrity*	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	x			AC-1 SC-1 SC-13	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4	Esri's Corporate Security policies are based on NIST 800-53 security controls which map to ISO 27001 controls. ArcGIS Online data security measures are in alignment with FedRAMP Tailored Low requirements (that have NIST 800-53 security controls as its core). ArcGIS Online procedures include requiring that updates are reviewed for unauthorized changes during the release management process. ArcGIS Online's cloud infrastructure providers data security policies, procedures, and processes align with industry standards such as FedRAMP Moderate and ISO 27001.

Cloud Security Alliance (CSA) CAIQ v.3.1 — Page 1 of 27 — ArcGIS Online Version - June 2021



Esri Responsibilities

Validation – ArcGIS Online FedRAMP Moderate

- Security controls shifted from FedRAMP Tailored Low to Moderate in 2022
- 3rd-party assessment materials summitted to initial authorizing agency (DOI) and FedRAMP for review
- Agency FedRAMP Moderate authorization expected by Q2 2023
- No migration is required, this was an in-place upgrade of security controls
- Authorized services remains the same through this transition, more service authorizations planned
- Start alignment with customer responsibility matrix now to ease transition
- When moderate authorization is in place, customers should consider expanded use cases involving sensitive information sets that can be discussed with your security team

FedRAMP

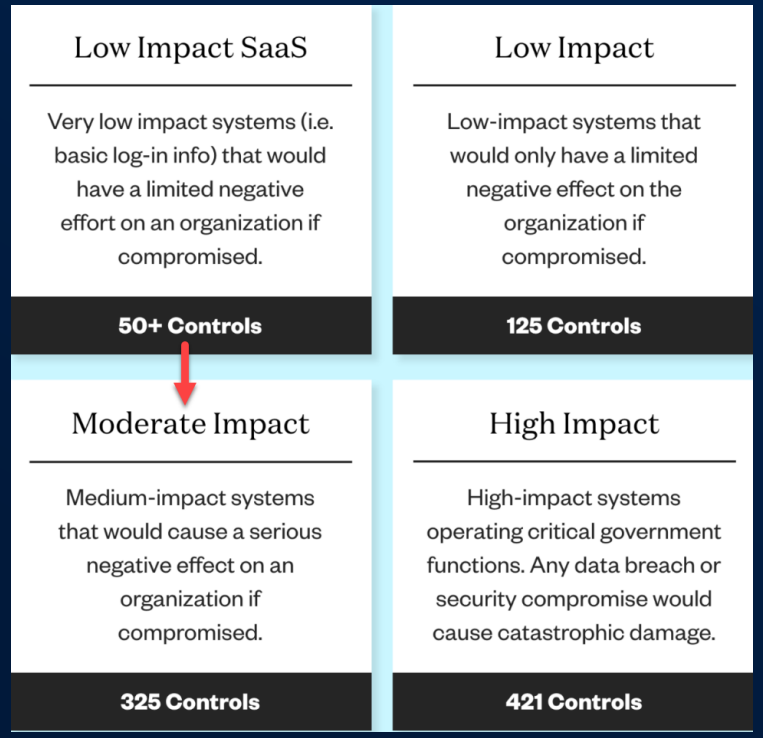
Security already advanced, assessment complete, waiting for agency authorization

Esri Responsibilities

Validation – ArcGIS Online FedRAMP Moderate

- Remains an **agency** authorized offering
  - DOI serving as initial authorizing agency
  - Other agencies have already started reviewing Moderate package
  - Communication so far from customers is JAB vs Agency based authorization does not matter

- Remains a **public** cloud offering
  - Customers gain benefit of FedRAMP moderate security without additional Gov Cloud costs/limitations



Esri Responsibilities

Validation – FedRAMP – Broader US Government Coverage

- National Defense Authorization Act (NDAA) signed at the end of 2022 incorporates FedRAMP Authorization Act
  - Formalizes FedRAMP requirement for cloud services utilized by U.S. government
  - Includes reciprocity enabling agencies to certify SaaS offerings like ArcGIS Online more easily

- What about US Defense usage?
  - DISA supports reciprocity between FedRAMP Moderate and DoD IL2 without separate authorization paperwork
    - See DISA Cloud SRG page 37
  - DOD IL2 allows for non-critical mission information and public data to be hosted when Moderate authorization is in place

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	CSP PERSONNEL REQUIREMENTS & INVESTIGATION EQUIVALENCY
2	PUBLIC	FedRAMP Moderate Baseline (MBL)	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	Tier 1 (T1)
4	CUI (FOUO, PII, PHI) or Non-CUI	Level 2 + CUI-Specific Tailored Set OR FedRAMP HBL	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 (IT-1) Tier 5 (T5)
5	CUI (FOUO, PII, PHI), U-NSI/NSS	Level 4 + NSS-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 (IT-2) Tier 3 (T3) Non-Disclosure Agreement (NDA)
6	Classified SECRET NSS	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated T5 & SECRET Clearance NDA

Esri Responsibilities

Validation – Upcoming - Cyber Supply Chain Validation

- Esri is actively maturing our cyber supply chain
- ISO 20243 assessment in progress
  - Addresses Supply Chain / Development Security
  - ArcGIS Online self-attestation by Q2 2023
- FedRAMP NIST 800-53 R5
  - Adds Supply Chain control family
  - Expected in 2024
- Broader International ISO 27001 Certification
  - Scope: ArcGIS Online EU Region
  - Expected mid-2024

Family	Group
Supply Chain Security	Risk Management
	Physical Security
	Access Controls
	Employee and Supplier Security and Integrity
	Business Partner Security
	Supply Chain Security Training
	Information Systems Security
	Trusted Technology Components
	Secure Transmission and Handling
	Open Source Handling
	Counterfeit Mitigation
	Malware Detection
Product Development and Engineering	Software/Firmware/Hardware Design Process
	Configuration Management
	Well-defined Development/Engineering Method Process and Practices
	Quality and Test Management
	Product Sustainment Management
Secure Development and Engineering	Threat Analysis and Mitigation
	Run-time Protection Techniques
	Vulnerability Analysis and Response
	Product Patching and Remediation
	Secure Engineering Practices
	Monitor and Assess the Impact of Changes in the Threat Landscape

Esri Responsibilities

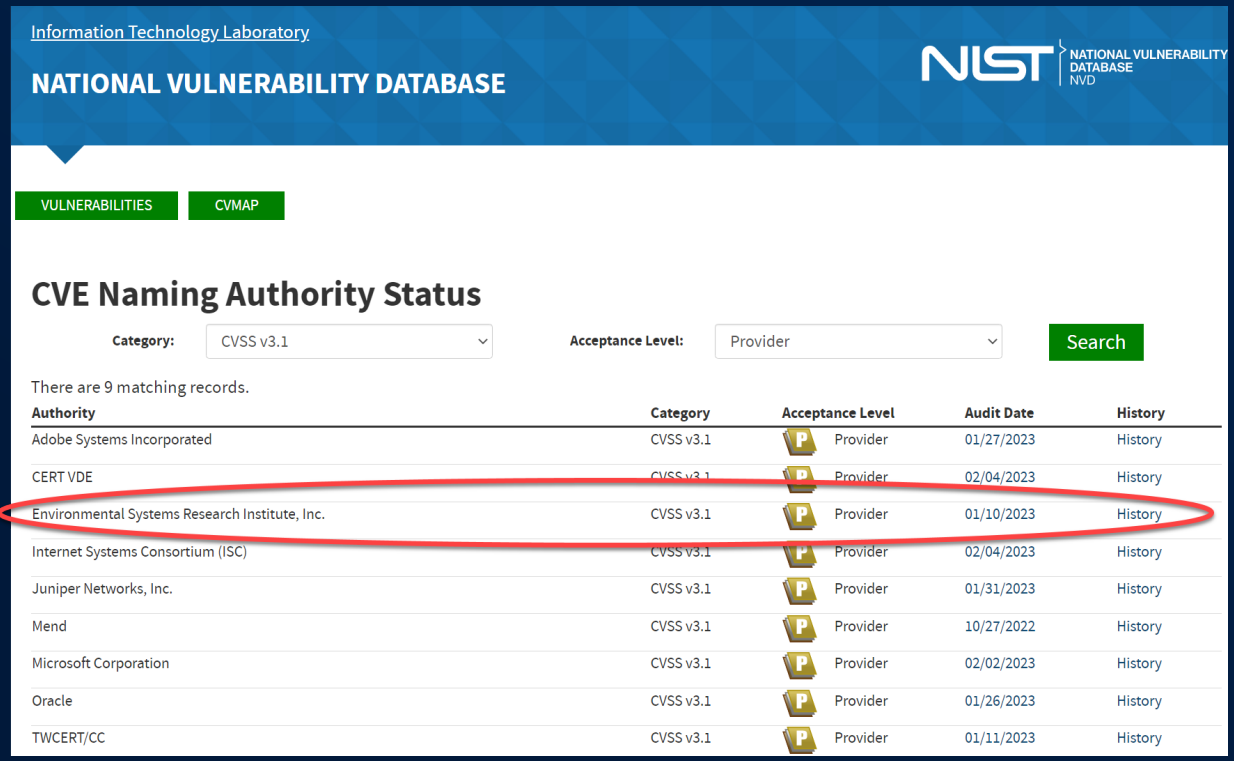
Validation – Upcoming – EO 14028 National Cybersecurity Improvement

- Response to large-scale events (Colonial Pipeline & SolarWinds attacks)
- Broad executive order with aspects we will address today

- Secure Software Development Attestations
  - FedRAMP addresses ArcGIS Online
  - Government final terms expected by June
  - Core product coverage Sept 2023

- Software Bill of Material (SBOM) validation ongoing
  - Validating minimum EO specs met with SPDX
  - Incorporating checks for no critical KEV's as part of release

- Vulnerability Disclosure Program Leadership
  - Esri is a CVE Numbering Authority
  - Audited by NIST as top 1% for accuracy of information



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES | CVMAP

CVE Naming Authority Status

Category: CVSS v3.1 | Acceptance Level: Provider | Search

There are 9 matching records.

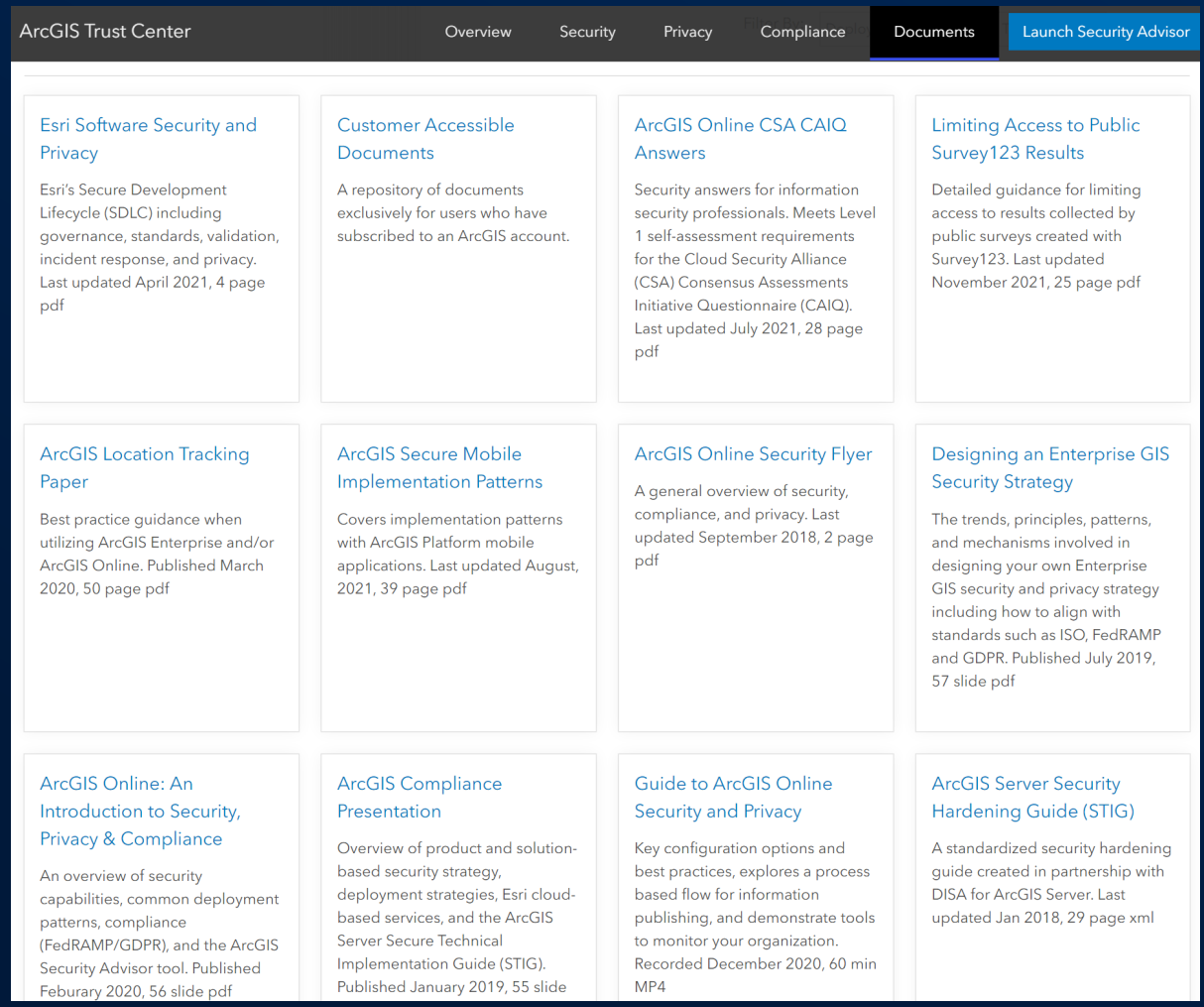
Authority	Category	Acceptance Level	Audit Date	History
Adobe Systems Incorporated	CVSS v3.1	Provider	01/27/2023	History
CERT VDE	CVSS v3.1	Provider	02/04/2023	History
Environmental Systems Research Institute, Inc.	CVSS v3.1	Provider	01/10/2023	History
Internet Systems Consortium (ISC)	CVSS v3.1	Provider	02/04/2023	History
Juniper Networks, Inc.	CVSS v3.1	Provider	01/31/2023	History
Mend	CVSS v3.1	Provider	10/27/2022	History
Microsoft Corporation	CVSS v3.1	Provider	02/02/2023	History
Oracle	CVSS v3.1	Provider	01/26/2023	History
TWCERT/CC	CVSS v3.1	Provider	01/11/2023	History

Esri Responsibilities

Guidance

- Tons of guidance within Trust Center today
  - Security & Privacy Advisor Tool
  - Location Sharing Privacy paper
  - Mobile
  - Surveys

- Upcoming guidance
  - ArcGIS Enterprise Security Hardening Guide
    - Critical Software Security Measures Alignment
    - Zero Trust touchpoints to be addressed
  - Welcome beta document feedback



Esri Responsibilities

Guidance – FedRAMP Authorized

- Validate authorized services
  - See Trust Center Customer Exclusive Docs
  - Trust.ArcGIS.com
- See what's next (Planned)
- Shift away from deprecated products
- Don't use retired products

FedRAMP

FedRAMP

ArcGIS Online FedRAMP Authorized Services

✓ = Authorized - service is included in audit scope and has been authorized

= Planned - service on roadmap for future authorization

! = Deprecated – service support will soon be ending and removed from the FedRAMP boundary

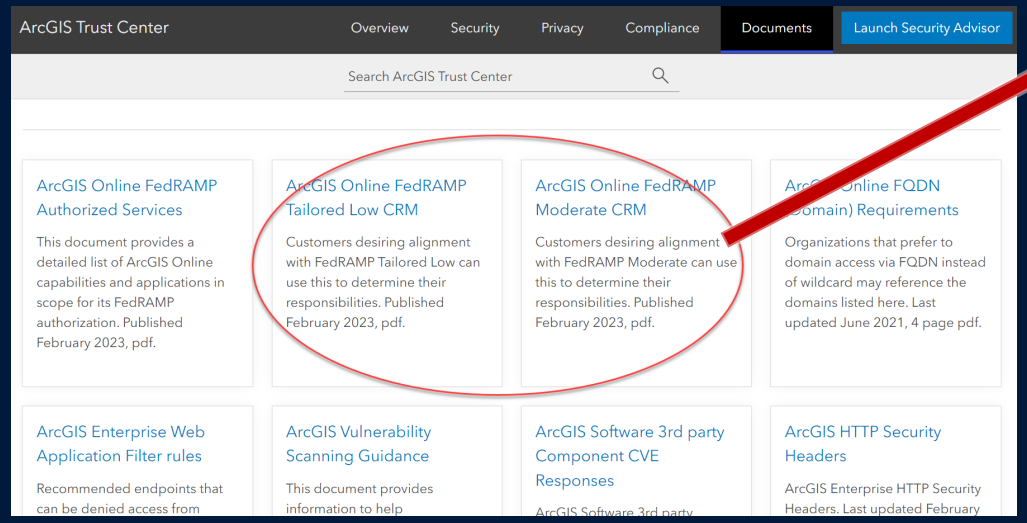
✗ = Retired – service not supported and no longer FedRAMP authorized

Service	Status
Organization Home	✓
Public Home	✓
ArcGIS Maps SDK for JavaScript	✓
ArcGIS Configurable Apps	✓
Customer Content (Items)	✓
Utility Service - Geocoding	✓
Utility Service - Geoenrichment	✓
Utility Service - Directions & Routing	✓
Hosted Feature Layers	✓
Hosted Tile Layers	✓
Analysis Tools	✓
Vector Tile Basemaps	✓
ArcGIS Web AppBuilder	✓
Scene Viewer	✓
Map Viewer	✓
ArcGIS QuickCapture (API) **	✓
ArcGIS Experience Builder	✓
ArcGIS Dashboards	✓
ArcGIS Solutions for ArcGIS Online *	✓
ArcGIS Hub (Basic & Premium)	✓
ArcGIS StoryMaps	✓
ArcGIS Field Maps (API, Web App) **	✓
ArcGIS Survey123 (API, Web App)	✓
ArcGIS Survey123 (Website, Web Designer)	✓
ArcGIS Instant Apps	
Location Sharing Services	
Classic Story Maps	!
ArcGIS Dashboards Classic	✗
ArcGIS Collector (API)	✗

Esri Responsibilities

Guidance – FedRAMP CRM

- Align with Customer Responsibility Matrix
  - Same Trust Center location
  - Both Tailored Low and Moderate available
  - Example Responsibility
    - Utilize a SAML provider (IDP) with ArcGIS Online and enforce account lockouts after 3 attempts for 15 minutes with IDP



AGO FedRAMP Tailored LI-SaaS Customer Responsibility Matrix (CRM) Worksheet

Control ID	Specific Inheritance and Customer Agency/CSP Responsibilities
AC-02 (f)	**Customer:** Responsible for the management and monitoring of their AGO organization accounts. Customer responsible for utilizing their SAML IDP for managing their accounts. Customers manage two main account types, administrator and user level access to their ArcGIS Online organization.
AC-03	**Customer**: Responsible for managing access to their AGO Organization and for managing the AGO roles defined and any custom roles that are created by that Customer. The Customer is also responsible for providing a SAML 2.0 Identity Provider for identity integration with the application, according to their policies and procedures to meet authentication requirements.
AC-07	**Customer**: Utilize a SAML IDP with ArcGIS Online and enforce account lockouts after 3 attempts for 15 minutes with their IDP. This capability is available within the online help here: https://doc.arcgis.com/en/arcgis-online/administer/enterprise-logins.htm Built-in AGO accounts not managed by an IDP are locked after 5 attempts, for 10 minutes. This
AC-17 (a)	**Customer**: Connect to AGO via the following allowed methods of remote access: web interface via a web browser. These customers are responsible for ensuring that the connection is secure by supporting TLS 1.2 connections.
AC-17 (b)	**Customer**: Responsible for authorizing remote access to their AGO Organization.
AC-22 (a)	**Customer**: Sharing occurs in alignment with the Customer's policies and procedures for the dissemination of content. AGO is a Services offering that gives the Customer the ability to share content with others within the Customer's Organization, to external organizations, or to the public. The Customer is responsible for the information they share to the public or externally.
AC-22 (b)	**Customer**: Sharing occurs in alignment with the Customer's policies and procedures for the dissemination of content. AGO is a Services offering that gives the Customer the ability to share content with others within the Customer's Organization, to external organizations, or to the public. The Customer is responsible for the information they share to the public or externally.
AC-22 (c)	**Customer**: Sharing occurs in alignment with the Customer's policies and procedures for the dissemination of content. AGO is a Services offering that gives the Customer the ability to share content with others within the Customer's Organization, to external organizations, or to the public. The Customer is responsible for the information they share to the public or externally.
AC-22 (d)	**Customer**: Sharing occurs in alignment with the Customer's policies and procedures for the dissemination of content. AGO is a Services offering that gives the Customer the ability to share content with others within the Customer's Organization, to external organizations, or to the public. The Customer is responsible for the information they share to the public or externally.
AU-03	**Customer**: Have the ability to audit their AGO organization by downloading the AGO Activity Log. The customers can specify the timeframe they want to audit from this activity log. Customers using SAML 2.0 compliant IdP are responsible for auditing these logs.
AU-05 (a)	**Customer**: Customers using SAML v2.0 IDP are responsible for auditing account creation, modification, disabling, and deletion events for their Identity Provider infrastructure as these events also pertain to AGO access. For these events, these customers are responsible for alerting designated organizational officials in the event of an audit processing failure
AU-05 (b)	**Customer**: Customers using SAML v2.0 IDP are responsible for auditing account creation, modification, disabling, and deletion events for their Identity Provider infrastructure as these events also pertain to AGO access. For these events, these customers are responsible for alerting designated organizational officials in the event of an audit processing failure
AU-06 (a)	**Customer**: * Monitoring the use of all customer-controlled accounts within AGO. * Reviewing and analyzing ArcGIS Online (AGO) audit logs through the AGO Status Dashboard related to activity generated by their Organization. In addition, the customer is responsible for reporting findings of inappropriate or unusual activity within AGO. * The SAML audit log content, review and analysis for account creation, modification, disabling, and deletion events for their Identity Provider infrastructure. * Monitoring and alerting designated organizational officials in the event of an audit processing failure related to events generated by their SAML Identity Provider (account creation, modification, disabling, deletion events, etc).
AU-06 (b)	**Customer**: * Monitoring the use of all customer-controlled accounts within AGO. * Reviewing and analyzing ArcGIS Online (AGO) audit logs through the AGO Status Dashboard related to activity generated by their Organization. In addition, the customer is responsible for reporting findings of inappropriate or unusual activity within AGO. * The SAML audit log content, review and analysis for account creation, modification, disabling, and deletion events for their Identity Provider infrastructure. * Monitoring and alerting designated organizational officials in the event of an audit processing failure related to events generated by their SAML Identity Provider (account creation, modification, disabling, deletion events, etc).
CP-09 (a)	**Customer**: Are responsible for backing up their organization's dataset's via daily incrementals and weekly full backups.
IA-02 (12)	**Customer**: Responsible for supplying a SAML 2.0 compatible federated identity provider for integration with AGO. This enables the Customer to support multi-factor authentication of approved CAC, PIV, Smartcard, MFA token, or Biometric.
IA-07	**Customer**: Government customers are responsible for ensuring that client software is configured to only establish sessions using FIPS 140-2 compliant protocols. This can be accomplished by restricting access to the government customer's SAML implementation to only internal network traffic. This will force government customers attempting to connect to ArcGIS Online to VPN into the customer's network or directly be on the network at the time of authentication. When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates USGCB baselines including browser settings to require FIPS 140-2 connections.
IA-08 (01)	**Customer**: Responsible for accepting and electronically verifying FICAM-approved third-party credentials.
PL-02 (a)	**Customer**: Please identify who the agency security stakeholders that the AGO Security Team should coordinate efforts such as Contingency and Incident Response testing, and monthly continuous monitoring report.
PS-03 (b)	**Customer**: Government customers are responsible for determining screening requirements and implementing the PS-3(b) requirements for their own personnel before they grant them access to the system.
RA-02 (a)	**Customer**: Responsible for their own security categorization of the information that is hosted on the AGO system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance. Since the baseline security categorization for the AGO system is Low, government customers are responsible for ensuring that no information with a security impact level greater than low is stored, processed, or transmitted vis the service provided to them by AGO. Because AGO does not have control over the information customers store within the system, government customer agencies/departments must separately categorize their data in agreement with FIPS 199 and NIST 800-60 to ensure that the security category of information types collected, processed, or stored in AGO does not exceed Low impact for confidentiality, integrity, and/or availability
RA-02 (c)	**Customer**: Responsible for their own security categorization of the information that is hosted on the AGO system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance. Since the baseline security categorization for the AGO system is Low, government customers are responsible for ensuring that no information with a security impact level greater than low is stored, processed, or transmitted vis the service provided to them by AGO. Because AGO does not have control over the information customers store within the system, government customer agencies/departments must separately categorize their data in agreement with FIPS 199 and NIST 800-60 to ensure that the security category of information types collected, processed, or stored in AGO does not exceed Low impact for confidentiality, integrity, and/or availability
SA-04 (10)	**Customer**: Government customers using SAML are responsible for accepting and electronically verifying Personal Identity Verification (PIV)credentials.
SC-12	**Customer**: Responsible for: * Ensuring that personal computing devices (client systems) are configured to request FIPS 140-2 encryption ciphers and protocols for all network sessions before connecting to AGO. * Ensuring that its users are using secure browsers and properly patched information systems to access ArcGIS Online (AGO). * Protecting against malicious code on its user's information systems that access ArcGIS Online (AGO).
SC-13	**Customer**: Government customers will ensure that personal computing devices (client systems) are configured to request FIPS-140-2 encryption ciphers and protocols for all network sessions. Commercial customers may also choose to use FIPS 140-2 ciphers and protocols when connecting to AGO.

Customer Security Responsibilities

Randall Williams

Customer Responsibilities

COMPLIANCE

CONFIGURE

PROCESSES

Customer Responsibilities

Compliance – Considerations for FedRAMP Moderate Use Cases

- ArcGIS Online's Tailored Low authorization centered around hosting only non-sensitive information in the SaaS
  - Drove a common pattern of *sensitive* data/services hosted in *ArcGIS Enterprise* and non-sensitive information hosted in ArcGIS Online ("Hybrid Pattern")

- ArcGIS Online's FedRAMP Moderate Auth allows agencies to consider storing PII and CUI
  - Customers can now balance the hosting location of datasets (ArcGIS Online/ArcGIS Enterprise) more on operational effectiveness and less than sensitivity level, allowing for a much larger number of uses cases
  - Allows agencies to meet *Cloud First* / *Cloud Smart* initiatives, allowing for more use cases

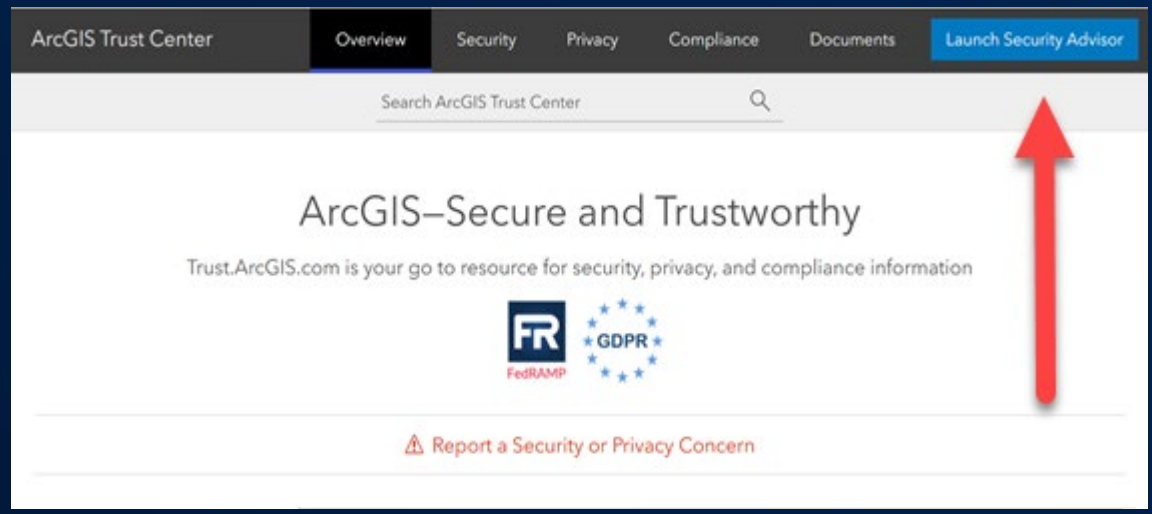
- **Customers battling stringent remediation timelines should consider SaaS**
  - CISA Operational Directive mitigations typically implemented within days
  - Critical issues mitigated within 7 days

Customer Responsibilities

Configure

- Ensure your systems are configured in alignment with best practices

- How? Use the ArcGIS Security & Privacy Advisor
  - Where? The ArcGIS Trust Center home page
  - What? Scan ArcGIS Online or Enterprise
  - Who? Requires Admin role to use
  - Cost? Free!
  - Setup? None for ArcGIS Online, minimal for Enterprise
  - Time? Less then 1 minute to scan Org



- Any items highlighted red (Dangerous), should be addressed immediately
  - Can be used to help align with FedRAMP Moderate requirements

Quickly and easily validate the security and privacy status of your Orgs

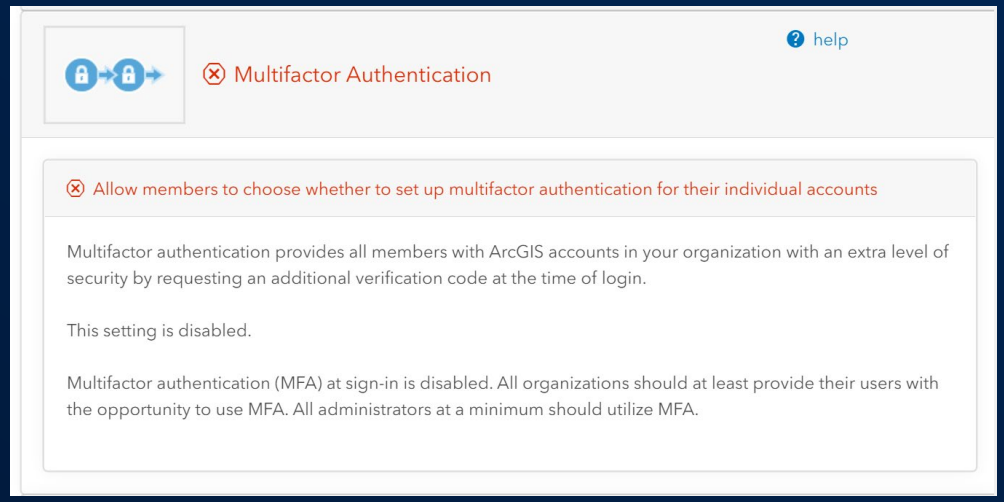
Customer Responsibilities

Configure

- What specific ArcGIS Online security **control**:
  1. Blocks more then 99.9% of account hacking attempts
  2. Is likely *not enabled* across your entire GIS yet

- Answer

  -**Multi-Factor authentication (MFA)**



*MFA is not a silver-bullet – It is a **minimum requirement** for a secure GIS*

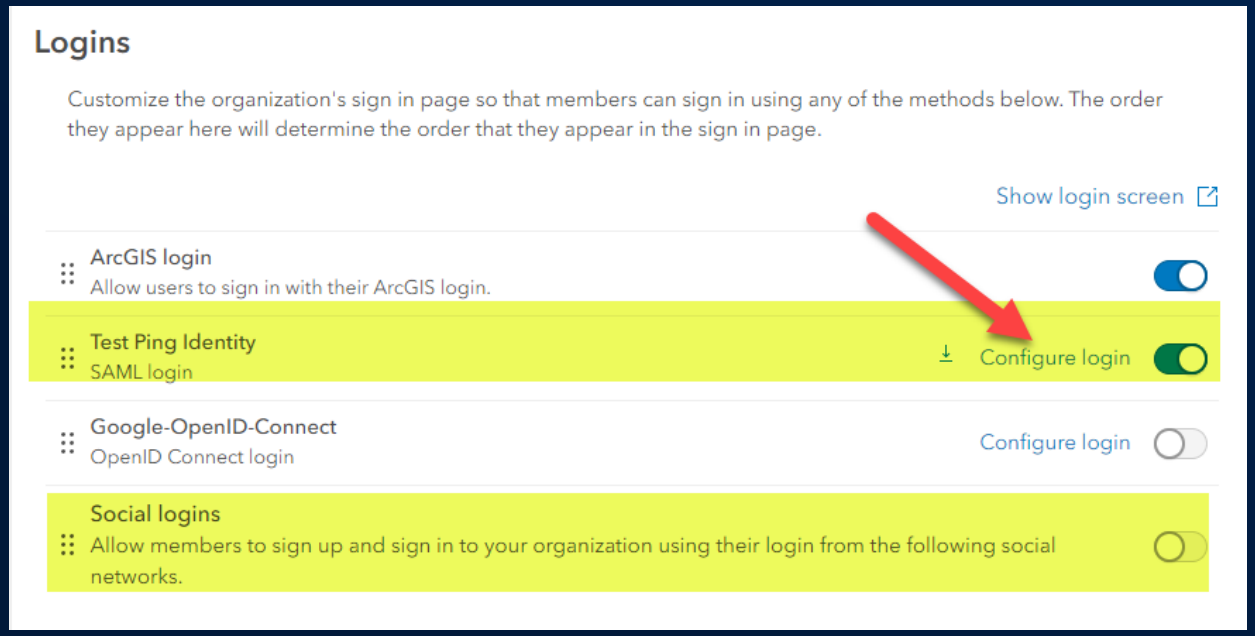
Customer Responsibilities

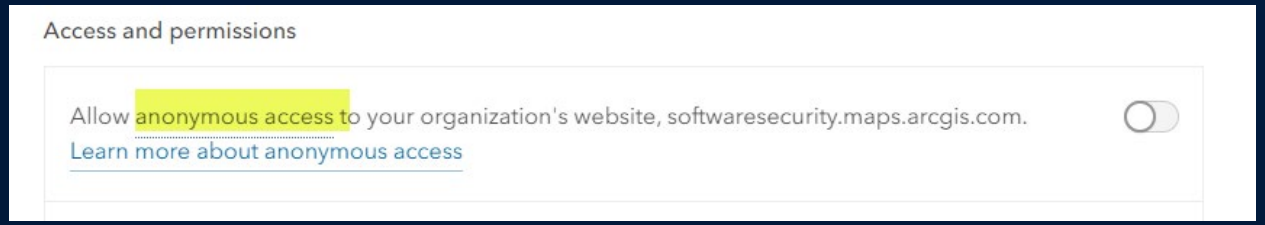
Configure – Consider your use case and adjust

- Use SAML for centralized user management
  - Manage users and groups with your domain tools
- Disable use of Social Media credentials to authenticate to Org
  - Allows access and audit of authentication controls using domain and/or AGO logs
- Configure custom roles for separation of duties
  - Use roles you define to delegate responsibilities and prevent privilege creep
- Disable Anonymous Access
  - Limit access to the AGO home app to authorized users. Share content via apps

Customer Responsibilities

Configure – Consider your use case and adjust





ArcGIS is Highly Configurable

Customer Responsibilities

Configure – More settings to consider

- Prevent users from sharing publicly
  - #1 source of privacy and data spillage is not an attacker – it's customers
- Prevent bio edits/visible profiles
  - Limit employee personal data exposure
- Remove social media links
  - Helps prevent data leaks via social media
- Participate in Organization Verification Program
  - Identify your organization as authoritative – be the source of truth!

Customer Responsibilities

Configure – Diving Deeper into Best Practices

- Using the Security & Privacy Advisor Tool is a great start, but not all capabilities/best practices are addressed by one tool

  - Portal for ArcGIS & ArcGIS Server best practice scanners come with ArcGIS Enterprise

  - A holistic table of security & privacy setting recommendations is included within the Location Sharing Privacy paper updated December 2022

Topic / *Recommended Option*	ArcGIS Enterprise - 11 Base Deployment						ArcGIS Online				Criticality / Impact	
HTTPS and Encryption	*Provided by Esri*	*Default*	*Configurable*	Portal Scan	Server Scan	Security Advisor	*Provided by Esri*	*Default*	*Configurable*	Security Advisor	*Privacy*	*Security*
Sitewide HTTPS TLS 1.2 and 1.3 Only	Yes	Yes	Yes	PS04	SS01	Yes	Yes	Yes	Yes	Yes	Danger	Danger
Enforce HTTPS via HSTS	Yes	No	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
Configure Preferred Encryption Algorithms	Yes	Yes	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
Website endpoint CA Certificates	No	No	Yes	-	-	-	Yes	Yes	No	-	Danger	Danger
CA Certificates used by Organization specific Identity Provider	No	No	Yes	-	-	-	No	No	Yes	-	Info	Info
Enforce data storage encryption (1)	No	No	Yes	-	-	-	Yes	Yes	No	-	Danger	Danger
Remove self signed certs	Yes	No	Yes	PS08	SS14	-	Yes	Yes	No	-	Warning	Info
LDAP Identity Store communication encrypted	Yes	No	Yes	PS07	SS13	-	N/A	N/A	N/A	N/A	Info	Info
Web Adaptor server uses HTTPS (2)	Yes	Yes	Yes	-	SS10	-	N/A	N/A	N/A	N/A	Danger	Danger
HTTP Header Config												
X-Content-Type-Options: NOSNIFF	Yes	Yes	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
X-XSS-Protection	Yes	Yes	No	-	-	-	No	No	No	-	Info	Info
X-Frame-Options: SameOrigin	Yes (3)	Yes	No	-	-	-	Yes	Yes	No	-	Warning	Warning
Interfaces												
Disable ArcGIS Services Directory	Yes	No	Yes	-	SS07	-	No	No	No	-	Warning	Warning
Disable ArcGIS Portal Directory	Yes	No	Yes	PS03	-	-	Yes	Yes	No	-	Warning	Warning
Limit access to ArcGIS Server Admin Resources via Web Adaptor	Yes	No	Yes	-	-	-	N/A	N/A	N/A	N/A	Warning	Warning
Understand Dynamic Workspace usage	Yes	Yes	Yes	-	SS09	-	No	No	No	-	Warning	Warning
Secure System Services	Yes	Yes	Yes (4)	-	SS06	-	Yes	Yes	No	-	Danger	Danger
Standardized Filtering												
Enforce Standardized Queries	Yes	Yes	Yes	-	SS02	Yes	Yes	Yes	Yes	Yes	Danger	Danger
Filter Web Content Enabled	Yes	Yes	Yes	-	SS05	-	Yes	Yes	No	-	Danger	Danger
Authentication and Authorization												
Utilize Enterprise Logins via SAML instead of Built-in	No	No	Yes	-	-	Yes	No	No	Yes	Yes	Warning	Warning
Block members joining org with social network credentials	No	No	No	-	-	Yes	Yes	No	Yes	Yes	Warning	Warning
Define a password Complexity Policy	Yes	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Warning	Danger
Use Organinization Specific user store with account lockout policy	Yes	Yes	Yes	-	-	-	Yes	Yes	Yes	-	Warning	Warning
Configure a shorter token Expiration Period	Yes	Yes	Yes	-	-	-	Yes	Yes	Yes	-	Warning	Warning
Configure Multi-factor Authentication	Yes (5)	No	Yes	-	-	Yes	Yes	No	Yes	Yes	Danger	Danger
Disallow user account self-creation	Yes	Yes	Yes	PS05	-	-	Yes	Yes	Yes	-	Warning	Danger
Define Custom Roles	Yes	No	Yes	-	-	-	Yes	No	Yes	-	Warning	Warning
Disable Anonymous Access to Portal home app	Yes	No	Yes	PS06	-	Yes	Yes	No	Yes	Yes	Danger	Warning
Configure role based access control	Yes	Yes	Yes	-	-	-	Yes	Yes	Yes	-	Danger	Danger
Disable Primary Site Administrator account (ArcGIS Server)	Yes	No	Yes	-	SS11	-	N/A	N/A	N/A	N/A	Warning	Warning
Disable Initial Admin Account (Portal for ArcGIS)	Yes	No	Yes	-	-	-	N/A	N/A	N/A	N/A	Warning	Warning
Disallow token generation in via GET	Yes	Yes	Yes	PS02	SS03	-	Yes	Yes	No	-	Danger	Danger
Disallow token generation w/ creds in query parameter via POST	Yes	Yes	Yes	PS02	SS04	-	Yes	Yes	No	-	Danger	Danger
SAML: Check if encrypted assertions and signed requests are enabled	Yes	No	Yes	PS13 (6)	-	-	Yes	No	Yes	-	Danger	Danger
ArcGIS Enterprise Web Tier Technologies												
Use a WAF/Web Filter	No	No	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
Utilize load balancer instead of Web Adaptor	No	No	Yes	-	-	-	Yes	Yes	No	-	Info	Warning
Web Adaptor utilized for IWA only inside organization	Yes	Yes	Yes	-	-	-	No	No	No	-	Info	Info
Remove Technology identifiers and banners	Yes	Yes	Yes (7)	-	-	-	Yes	Yes	No	-	Info	Info
Use Data Loss Prevention (DLP)	No	No	Yes	-	-	-	Yes	-	-	-	Warning	Warning
Data Ownership & Privacy												
Prevent users from sharing publicly	Yes	Yes	Yes	PS12	-	Yes	Yes	Yes	Yes	Yes	Warning	Warning
Disallow biography edits and visibile profiles	Yes	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Warning	Info
Limit search to your organization only	Yes	Yes	Yes	-	-	Yes	Yes	No	Yes	Yes	Info	Info
Remove social media links in item details/group pages	Yes	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Warning	Info
Do not allow members of other organizations to sign in	No	No	No	-	-	-	Yes	No	Yes	-	Warning	Warning
Define specific allowed Portals that your Portal may access	Yes	No	Yes	-	-	-	Yes	No	Yes	Yes	Warning	Warning
Validate Distributed Collaborations	Yes	No	Yes	-	-	-	Yes	No	Yes	-	Warning	Danger
Disable Esri User Experience Improvement Program (EUEI)	No	No	No	-	-	-	Yes	No	Yes	Yes	Warning	Info
Identify Authoritative Content (8)	No	No	No	-	-	-	Yes	No	Yes	-	Warning	Info
Configure Access Notice	Yes	No	Yes	-	-	-	Yes	No	Yes	-	Info	Warning
System Services Shared as portal item	Yes	Yes	Yes	-	SS15	-	-	-	-	-	Info	Info
Validate Public Feature Services with update or delete permissions	Yes	Yes	Yes	-	SS12	-	Yes	Yes	Yes	Yes	Warning	Warning
Server Trust Relationships												
Define servers for web tier authentication	Yes	No	Yes	-	-	-	Yes	No	Yes	Yes	Warning	Warning
Define allowed proxy hosts	Yes	No	Yes	PS01	-	-	Yes	No	No	-	Warning	Warning
Define Cross Origin Policy	Yes	No	Yes	PS09	SS08	-	Yes	No	Yes	Yes	Warning	Warning
Federated server administrative URL	Yes	No	Yes	PS10	-	-	N/A	N/A	N/A	N/A	Warning	Danger
Federated server services URL	Yes	No	Yes	PS11	-	-	N/A	N/A	N/A	N/A	Info	Info
Sharing Best Practices (9)												
Create and document content review policy	No	No	Yes	-	-	-	No	No	Yes	-	Danger	Warning
Create and document sharing review policy	No	No	Yes	-	-	-	No	No	Yes	-	Danger	Warning
Validate need for editable layers	Yes	No	Yes	-	-	-	Yes	No	Yes	-	Danger	Warning

Review the many documents available in the ArcGIS Trust Center

Customer Responsibilities

Configure – FedRAMP Alignment

- To achieve FedRAMP moderate alignment for your ArcGIS Online organization, you'll need configure it based on the Customer Responsibility Matrix (CRM)

  - The good news: Implementing these best practice recommendations we just discussed aligns with the FedRAMP Moderate recommendations in the CRM

  - The Security & Privacy Advisor can help automate validation of alignment many CRM items that require technical configuration settings

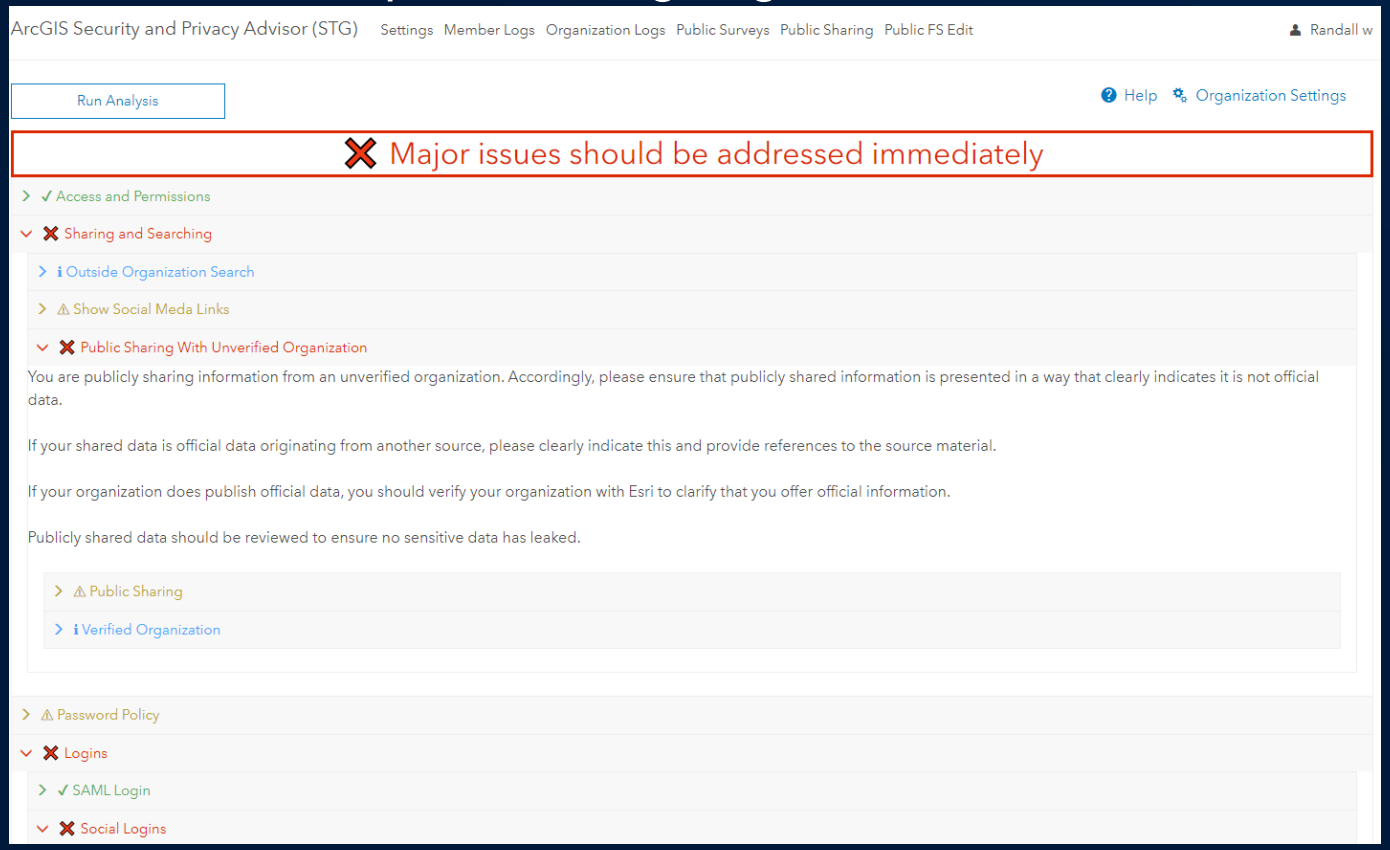
  - This allows for ease of ongoing validation and prevention of potential configuration "Drift" issues

FedRAMP alignment is both an Esri responsibility AND a Customer responsibility

How do I validate my configuration options again?

ArcGIS Security and Privacy Advisor! – https://trust.arcgis.com

- Supports ArcGIS Online and ArcGIS Enterprise!
- Enhancements planned/ongoing – check out the new BETA!



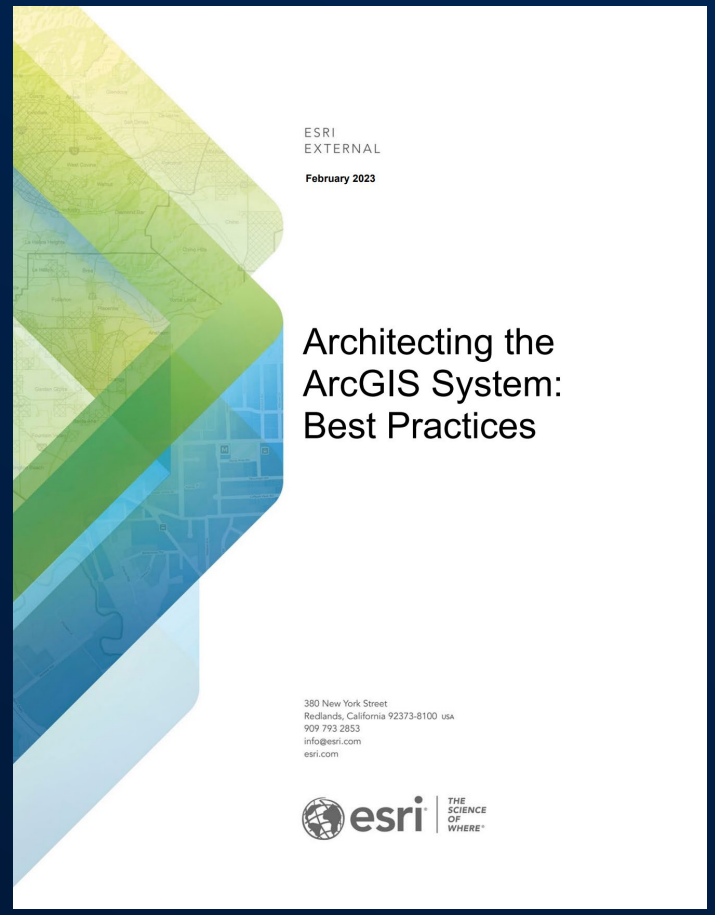
Provide feedback on the new Beta version!

Customer Responsibilities

Processes

- Architecting the ArcGIS System: Best Practices

- Practices with strong security value include
  - Leverage Automation Tools
    - Flag when configuration drifts away from best practices
  - Environment Isolation
    - Separate production, staging, and development environments
  - Identity management
    - Without MFA, accounts will be compromised
  - Publication strategy
    - Without a strong/enforced publication process, data will be breached



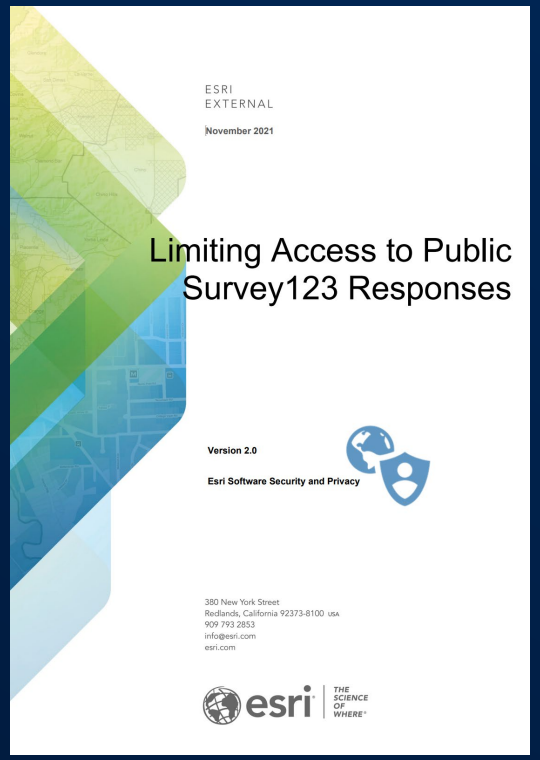
*Hold on…Data **will** be breached?*

Customer Responsibilities

Processes

Question: What GIS security **process**:

1. Drastically reduces the likelihood of the most common GIS data breach
2. Is frequently bypassed when enforcement controls are not in place



- Answer
  - A Strong GIS **data publication management** process

- Most common breach of GIS data
  - Occurs when customers accidentally publish sensitive data publicly, such as Survey123 results
  - Resulted in Esri publishing extensive guidance and providing stronger in-app warnings
  - Best analogy is the customer accidental over-exposure of AWS S3 datasets

Don't bypass rigorous GIS publication processes

Summary

Summary

ArcGIS Online Security & Compliance requires strong due diligence by Esri and customers

SECURE DEVELOPMENT

TRUST CENTER

FEDRAMP MODERATE

SECURITY & PRIVACY ADVISOR

MULTI-FACTOR AUTHENTICATION

RIGOROUS PUBLICATION

Questions? *SoftwareSecurity@Esri.com*