Esri Software Security and Privacy

Esri is committed to delivering secure geospatial software and services that meet the needs of customers, from individuals to large organizations. While Esri has always taken the security of its products seriously, the importance of embedding security and privacy into the development life cycle has increased as Esri incorporates Artificial Intelligence capabilities in a responsible manner. This document summarizes key aspects of Esri's Secure Development Life Cycle (SDLC).

Governance

Security policies spanning the company are set at the corporate level by the corporate security team's Chief Information Security Officer (CISO), while privacy policies are set by the Chief Privacy Officer (CPO) within the Legal team. Esri's Human Resource team ensures that all employees are appropriately vetted before onboarding. Corporate security controls are inherited across Esri, while functional areas (such as engineering and operations) are responsible for specific security control families, as seen in figure 1 below.

The security of Esri products and services is overseen by the Chief Information Security Officer (CISO)-Products, who leads Esri's Software Security & Privacy team. This team is embedded within product operations and engineering, providing security guidance and validation while fostering a security & privacy champion program across the broad spectrum of product teams to help further embed security and privacy across Esri products.

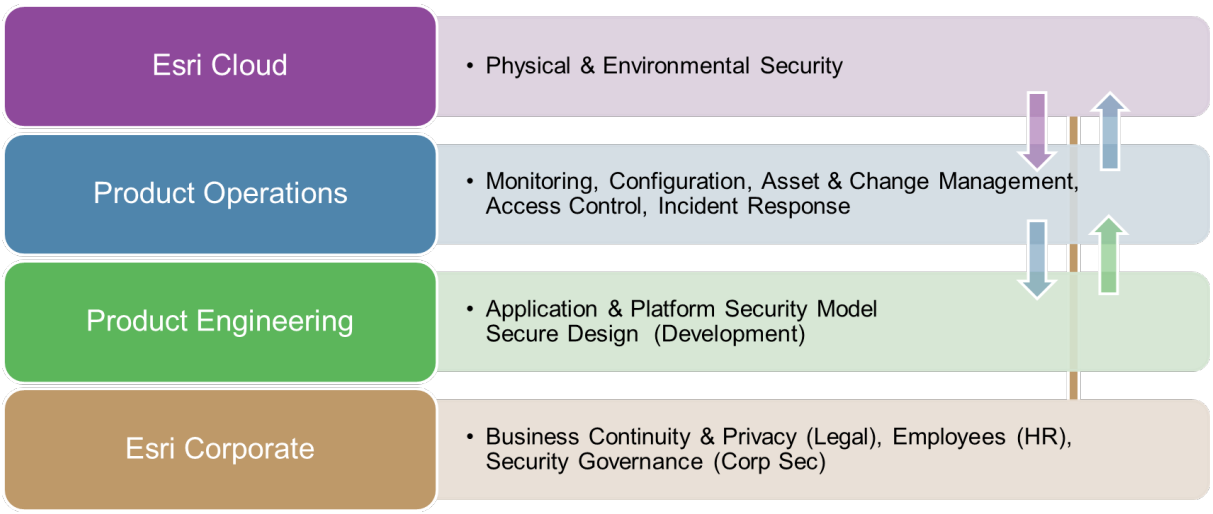

Figure 1—Product Security Responsibility by Functional Area

Secure Development Standards

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. BSIMM was utilized to create Esri's Product Security Baseline to assure basic security and privacy requirements are addressed. The amount of security validation incorporated during the life cycle for a product varies depending on the product's relative risk.

Esri designs security into ArcGIS to ensure a consistent, secure experience across your enterprise, whether it's providing role-based access control (RBAC), logging, authentication, or authorization. ArcGIS is also designed to integrate into your organization's security infrastructure through support of standards such as LDAP, SAML, OpenID, and even using your organization's identity store and security policies at the web level to facilitate single sign-on or public key infrastructure (PKI) support. Additional embedded product security capabilities are documented in the ArcGIS Trust Center (Trust.ArcGIS.com) as well as our online help.

Esri provides secure coding training based on Open Web Application Security Project (OWASP) guidelines and promotes awareness of the Common Weakness Enumeration (CWE/SANS) Top 25 most dangerous software errors. Esri provides teams with secure coding checklists to further reinforce the importance of key security items that all product teams should address. Basic items, such as malicious code discovery, have been incorporated into the build process for many years, utilizing multiple antivirus programs to minimize risk and false positive alerts.

Esri applies its most rigorous security measures for its foundational products of ArcGIS Enterprise, ArcGIS Online, and ArcGIS Pro. These products regularly undergo static code analysis, dynamic scans, third-party component analysis, and periodic third-party pen testing. Esri continues to expand the amount of security validation it performs against all ArcGIS products and seen in Figure 2 below.

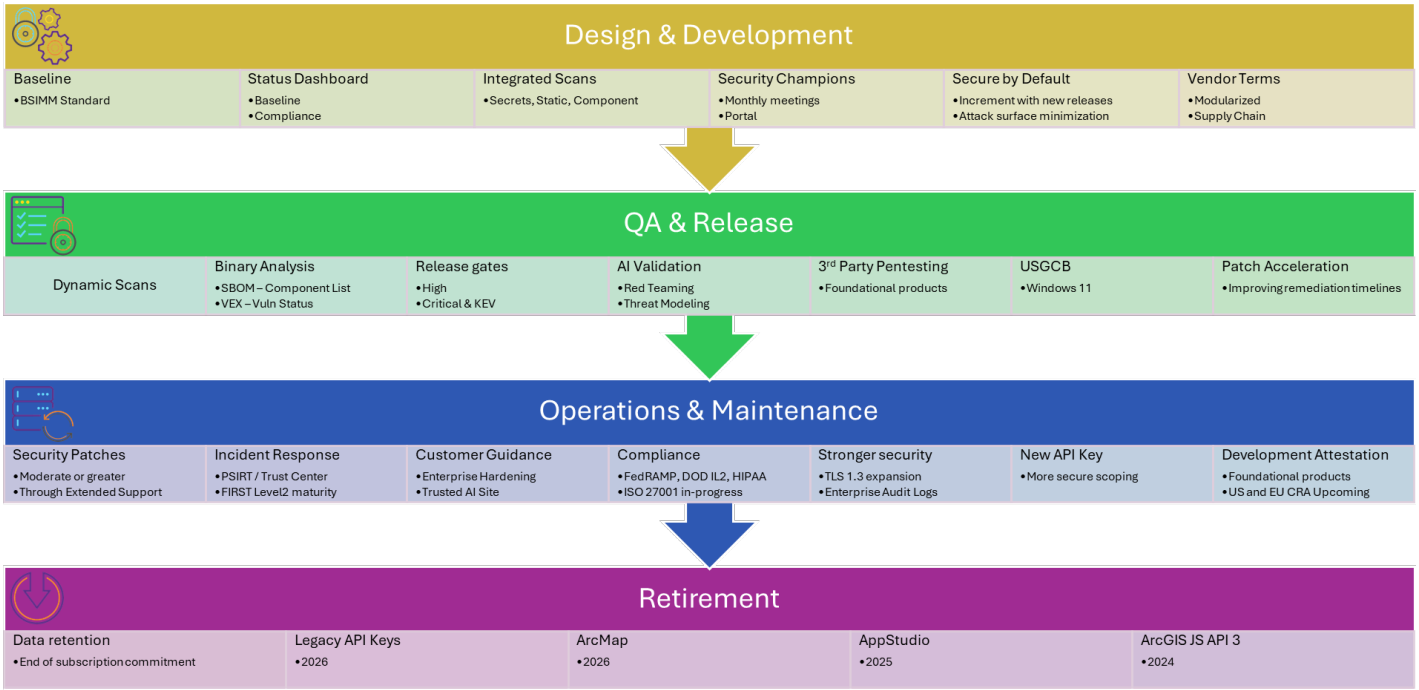

Figure 2— Key Attributes of Esri's Security & Privacy Development Lifecycle

Software-as-a-Service Security

ArcGIS Online is Esri's premier software-as-a-service (SaaS) geographic information system (GIS). Esri's security strategy for government-authorized offerings, such as ArcGIS Online, is based on an industry-standard defense-in-depth approach that provides security controls at every level including application, network, and facilities. ArcGIS Online is FedRAMP Moderate authorized by the US Government ensuring that security and risk management activities are integrated under a risk management framework. This includes annual third-party assessments / pen testing, and regular security validation efforts including the scans mentioned for ArcGIS Enterprise. The Esri Managed Cloud Services Advanced Plus offering is also FedRAMP authorized, providing single tenant ArcGIS Enterprise hosting for both commercial organizations and federal agencies. Esri is actively pursuing ISO 27001 certification of the European Union regional capabilities of ArcGIS Online and Location Platform.

Vulnerability and Breach Response

Esri has a Product Security Incident Response Team (PSIRT), which reports to the CISO-Products, to help shepherd security issues from cradle to grave, as shown in figure 3. Vulnerability concerns can be submitted via Esri's standard support process or Trust Center security concern page, where the PSIRT team will be engaged. To help prioritize efforts, Esri utilizes the Common Vulnerability Scoring System (CVSS) to determine the potential severity of the vulnerability and adjust for applicable environment factors. Ultimately, the resolution of a reported incident may require upgrades to products that are under active support from Esri. If an item requires a security patch, upon release, it is broadcast in the Trust Center "Announcements" section, which has an RSS feed that customers can subscribe to. Esri also announces patches through its Support site, blogs, and some end-user products—such as ArcGIS Pro—to notify the user of updates when starting the application.

If an event were to occur where a customer's data being managed by Esri was confirmed breached, Esri will contact the customer within 72-hours. Esri will coordinate with appropriate parties to investigate the security breach and perform remediation as necessary. Esri will provide updates to the customer with applicable information on a mutually agreed-on schedule. Esri does not inform any third party of a breach of a customer's information and data without first obtaining the customer's prior written consent, unless required by law or court order.

Figure 3—Product Security Incident Response Team (PSIRT) Workflow

Privacy

Esri values the privacy of its customers, distributors, and partners, as it is a principal component of establishing trust. Esri has created a general company Privacy Statement and a Products & Services Privacy Statement Supplement to ensure that customers receive the level of privacy they deserve and expect. The privacy statements describe how Esri collects data and uses information you provide to us and are independently validated.

Esri supports alignment with the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and has a Data Processing Addendum (DPA) containing Standard Contractual Clauses available within the ArcGIS Trust Center documents that customers can sign. Lastly, HIPAA eligible services are available for ArcGIS Online, which are backed by a Business Associate Agreement (BAA).

Trusted AI

Esri added a Trusted AI section to the ArcGIS Trust Center for customers to understand the security and privacy validation incorporated into our evolving AI capabilities as well as highlighting aspects customers should address in a shared responsibility model. Some of the AI specific checks we have incorporated into our SDLC are AI threat modeling and red team testing as shown in figure 2. We provide transparency of new AI features through AI Transparency Cards so customers can assess their risks, assess alignment with their operational needs and any associated mitigations to minimize risk.

esri | THE SCIENCE OF WHERE™

Esri, the global market leader in geographic information system (GIS) software, offers the most powerful mapping and spatial analytics technology available.

Since 1969, Esri has helped customers unlock the full potential of data to improve operational and business results. Today, Esri software is deployed in more than 350,000 organizations including the world's largest cities, most national governments, 75 percent of Fortune 500 companies, and more than 7,000 colleges and universities. Esri engineers the most advanced solutions for digital transformation, the Internet of Things (IoT), and location analytics to inform the most authoritative maps in the world.

Visit us at esri.com.

More Security & Privacy Information

Esri posts detailed product security, privacy, and compliance information to its Trust.ArcGIS.com website. In addition to guidance for each of these areas, there are security presentations, best practice technical papers, and in-depth answers to the Cloud Security Alliance (CSA) common security questions.

Esri Software
Security & Privacy Team
SoftwareSecurity@Esri.com

Contact Esri

380 New York Street
Redlands, California 92373-8100 USA

1 800 447 9778
T 909 793 2853
F 909 793 5953
info@esri.com
esri.com

Offices worldwide
esri.com/locations