Adobe security for digital government

Bringing serious security practices, processes and certifications to today's digital government environment

Table of contents

Adobe is the global leader in digital marketing and digital media solutions. Our tools and services allow agencies to create groundbreaking digital content, deploy it across media and devices, and measure and optimize it over time to achieve greater success. We help government make, manage, measure and mobilize content across every channel and screen.

Since the company was founded in 1982, Adobe has been responsible for technological breakthroughs like PostScript—which expanded publishing beyond printing presses and into the offices and homes of everyday people in the 80s—and PDF—which facilitated the exchange of documents anytime, anywhere and on any device in the 90s. Adobe continues to innovate while fully embracing cloud technologies of the 21st century. From the acquisition of Omniture—a company with over 15 years of experience offering cloud services—and integration of those products into the Adobe Marketing Cloud to the complete transition of popular desktop products like Adobe Photoshop and Adobe Acrobat to the cloud—Adobe Creative Cloud and Adobe Document Cloud, respectively—Adobe has been fully committed to providing powerful, secure and cost-effective solutions. Adobe cloud solutions for government include:

- **Adobe Connect**—Used for online meetings and collaboration by Department of Defense (DoD) users worldwide. Connect is supported by Adobe as a managed service, with over one million users on both Non-classified Internet Protocol Router Networks (NIPRNets) and Secret Internet Protocol Router Networks (SIPRNets).
- **Adobe Experience Manager forms**—Used at the Centers for Medicare and Medicaid Services (CMS) in support of the Affordable Care Act (ACA) with a Federal Information Security Management Act (FISMA) moderate Authority to Operate (ATO).

Adobe received Federal Risk and Authorization Management Program (FedRAMP) ATO for Adobe Connect and Experience Manager forms in August of 2015. These certifications represent the latest of our continuous efforts to maximize Adobe security for digital government.

Security strategy

At Adobe, we take the security of your digital assets seriously. From the rigorous integration of security into our internal software development process and tools to our cross-functional incident response teams, we strive to be proactive and nimble. What's more, our collaborative work with partners, researchers and other industry organizations helps us understand the latest threats and security best practices, as well as continually build security into the products and services we offer.

Application security to cloud security and certifications

At Adobe, we've evaluated security for our application and services development from both top-down and bottom-up perspectives. Initially, to protect our applications from the software layer down, we implemented the Adobe Secure Product Lifecycle (SPLC)—a rigorous set of several hundred specific security activities spanning software development practices, processes and tools integrated into multiple stages of the product lifecycle, including supply chain security.

As we moved to the cloud, we took a new look at protection from the physical layer up. To do this, we implemented a foundational framework of security processes and controls to protect our infrastructure, applications and services, as well as help us comply with a number of industry-accepted best practices, standards and certifications that we call the Adobe Common Controls Framework (CCF).

Adobe Common Controls Framework

Adobe reviewed the criteria for the most common security certifications and found a number of overlaps. To create the CCF, we analyzed more than 1,000 requirements from relevant cloud security frameworks and standards, rationalizing them down to approximately 200 Adobe specific controls. These controls provide specific requirements that meet the expectations of Adobe stakeholders and customers for implementing controls.

Adobe Secure Product Lifecycle

Adobe Secure Software Engineering Team (ASSET) security researchers provide specific SPLC guidance for each key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices and the threat landscape.

Adobe SPLC activities include, depending on the specific product component, some or all of the following recommended best practices, processes and tools:

- Security training and certification for product teams
- Product health, risk and threat landscape analysis
- Secure coding guidelines, rules and analysis
- Service roadmaps, security tools and testing methods that guide the Adobe Analytics security team to help address:
  - Open Web Application Security Project (OWASP) Top 10 Most Critical Web Application Security Risks
  - Common Weakness Enumeration/System Administration, Audit, Networking and Security Institute (CWE/SANS) Top 25 Most Dangerous Software Errors
- Security architecture review and penetration testing
- Source-code reviews to help eliminate known flaws that could lead to vulnerabilities
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Full readiness review, response plans and release of developer education materials

As part of the SPLC, Adobe conducts ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services. Employees participating in the Adobe Software Security Certification Program attain certification levels by completing security projects.

The program has four levels, each designated by a colored belt—white, green, brown or black. Adobe updates training on a regular basis to reflect new threats and mitigations, as well as new controls and software languages.

- **White and green levels**—Achieved by completing computer-based training courses.
- **Brown and black level**s—Achieved by completing months- or year-long, hands-on security projects. Employees attaining brown and black belts become security champions and experts within their product teams.

Security tactics

Apart from strategic top-down and bottom-up evaluations of security for application and services development, Adobe follows tactical industry standards and categorizes security operations into prevention, detection and incident response. The following sections highlight some pertinent security measures within each category with respect to digital government.

Prevention

Prevention is the first line of defense in Adobe's efforts to optimize security.

Penetration testing

Adobe approves and engages with leading third-party security firms to perform penetration testing that can uncover potential security vulnerabilities and improve the overall security of Adobe products and services. Upon receipt of the third-party report, Adobe documents the vulnerabilities, evaluates their severity and priority, and then creates a mitigation strategy or remediation plan.

Internally, our security teams perform a risk assessment of all components prior to every release. Conducted by highly trained security staff trusted with securing the network topology and infrastructure and applications, the security teams look for insecure network setup issues across firewalls, load balancers and server hardware, as well as application-level vulnerabilities. The security touchpoints include exercises like threat modeling, along with vulnerability scanning and static and dynamic analysis of the application. The security team partners with technical operations and development leads to help ensure that all high-risk vulnerabilities are mitigated prior to each release.

Leveraging the community

Since 2010, Adobe has been an active member of the Cloud Security Alliance (CSA) and OWASP, two of the leading industry organizations for cloud security certifications and standards. Adobe is also a founding and current charter member of Software Assurance Forum for Excellence in Code (SAFECode), an organization focused on advancement of effective software assurance methods. Other founding members include Microsoft, EMC and Cisco. In addition, Adobe has a well-developed, expansive security training program for all product development professionals. This program and its materials now comprise the SAFECode core security training program for developers.

Strong cryptography and authentication

Adobe has a rich history with public key infrastructure (PKI) and encryption, including support for standards like Joint Interoperability Test Command (JITC) and National Institute of Standards and Technology (NIST) Public Key Interoperability Test Suite (PKITS) for digital signatures and Federal Information Processing Standard (FIPS) 140-2 for document encryption. Adobe leverages this history to provide PKI-based authentication services with our solutions. For instance, when clients—Adobe Acrobat DC and Adobe Acrobat Reader DC—communicate with the Adobe Experience Manager server, the Hypertext Transfer Protocol Secure (HTTPS) protocol is used. To authenticate the end user, several methods are provided. While many organizations leverage their own authentication system—which the clients can leverage via Kerberos and Security Assertion Markup Language (SAML) single sign-on (SSO)—Experience Manager also supports username/password, one-time password (OTP), and TLS mutual authentication.

Physical security

Every Adobe corporate office location is protected 24x7 by on-site security guards. Adobe employees access company buildings using a keycard ID badge. Visitors enter through the front entrance, sign in and out with the receptionist, display a temporary visitor ID badge and are escorted at all times by an Adobe employee. All server equipment, development machines, phone systems, file and mail servers and other sensitive systems are locked at all times in environment-controlled server rooms that are accessible only by appropriate, authorized staff members.

Virus protection

Adobe scans all inbound and outbound corporate email for known malware threats.

Employee access to customer data

Adobe maintains segmented development and production environments, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems—employees with no legitimate business purpose are restricted from accessing these systems.

Background checks
Adobe obtains background check reports for employment purposes. The typical report includes educational background; work history; court records, including criminal conviction records; and references obtained from professional and personal associates, each as permitted by applicable law. These background check requirements apply to regular U.S. new-hire employees, including those who will be administering systems or have access to customer information. New U.S. temporary agency workers are subject to background check requirements through the applicable temporary agency, in compliance with Adobe background screening guidelines. Outside the United States, Adobe conducts background checks on certain new employees in accordance with Adobe background check policies and applicable local laws.

Employee termination
When an employee leaves Adobe, the employee's manager submits an exiting worker form. Once approved, Adobe People Resources initiates an email workflow informing relevant stakeholders to take specific actions leading up to the employee's last day. In the event that Adobe terminates an employee, Adobe People Resources sends a similar email notification to relevant stakeholders, including the specific date and time of the employment termination.

Adobe Corporate Security then schedules the following actions to help ensure that, upon conclusion of the employee's final day of employment, he or she can longer access Adobe confidential files or offices:

- Email access removal
- Remote VPN access removal
- Office and data center badge invalidation
- Network access termination

Upon request, managers may ask building security to escort a terminated employee from the Adobe office or building.

Detection
Adobe employs a variety of detection methods and programs to help thwart potential security breaches.

Threat landscape monitoring
Adobe continuously monitors the threat landscape and invests in primary security research and telemetry information to help ensure fast responses to threats that target our products, services or the Adobe cloud infrastructure. In addition to subscribing to industry-wide vulnerability announcement lists like those from the United States Computer Emergency Readiness Team (US-CERT), Bugtraq and SANS, Adobe subscribes to the latest security alert lists issued by major security vendors.

Intelligence sharing
Adobe works with customers, researchers and partners to exchange information about potential threats and vulnerabilities. As new threats emerge, we share this intelligence across Adobe product teams to mitigate the threats and adapt our processes accordingly, enabling us to develop stronger security capabilities in all Adobe products and services.

MAPP partnership
Our partnership with the Microsoft Active Protections Program (MAPP) facilitates advance information sharing of product vulnerabilities with security software providers—like antivirus and intrusion detection and prevention vendors—helping them reduce the risk of malicious coders exploiting the vulnerability.

Continuous monitoring
As part of our risk management framework and to help ensure the confidentiality, integrity and availability of information, Adobe Managed Services operates an information security continuous monitoring process. From a government compliance and management perspective, the Adobe security program most closely aligns with the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program. The CDM program is a dynamic, future-state approach to fortifying the cybersecurity of federal networks and systems. The CDM program leverages capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts and enable cybersecurity personnel to mitigate the most significant problems first.

Adobe provides continuous monitoring of all events occurring within the scanned environments—including within individual FedRAMP instances—and correlates them on a continuous basis to identify potential risk events or combinations of events. Adobe takes appropriate action based on threat assessments of the identified correlation of events, which are prioritized based on the potential impact to Adobe environments. In effect, Adobe is already firmly operating in the desired future-state of the DHS CDM program.

Incident response

When a significant announced vulnerability puts any of our solutions at risk, the Adobe Product Security Incident Response Team (PSIRT) communicates the vulnerability to the appropriate team to coordinate the mitigation effort. Adobe centralizes incident response, decision-making and external monitoring in our Security Coordination Center (SCC), providing cross-functional consistency and fast resolution of issues. When an incident occurs with an Adobe product or service, the SCC works with the involved Adobe product incident response and development teams to help identify, mitigate and resolve the issue using the following proven process:

- Assess the status of the vulnerability
- Mitigate risk in production services
- Quarantine, investigate and destroy compromised nodes (cloud-based services only)
- Develop a fix for the vulnerability
- Deploy the fix to contain the problem
- Monitor activity and confirm resolution

Forensic analysis

For incident investigations, teams adhere to the Adobe forensic analysis process that includes complete image capture or memory dump of an impacted machine(s), evidence safe-holding and chain-of-custody recording.

Summary

Adobe's proactive approach to security and stringent procedures described in this paper help protect the security of our solutions and your confidential data. At Adobe, we take the security of your digital experience very seriously. We continuously monitor the evolving threat landscape to stay ahead of malicious activities and help ensure the security of your data. With an ongoing commitment to providing powerful, secure and cost-effective solutions, Adobe will continue its efforts to maximize secure solutions for today's digital government.

For more information

Adobe Genuine software program: *www.adobe.com/genuine.html*
Adobe Privacy Center: *www.adobe.com/privacy.html*
Adobe Product Security Incident Response Team (PSIRT) Blog: *blogs.adobe.com/psirt*
Adobe security training: *www.adobe.com/content/dam/Adobe/en/security/pdfs/adobe-security-training-wp-web.pdf*
Adobe supported standards: *www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/standards.html*
Notifying Adobe of security issues: https*://helpx.adobe.com/security/alertus.html*
SAFECode security engineer training: *https://training.safecode.org/*
Security bulletins and advisories: *https://helpx.adobe.com/security.html*
Adobe security resources: *www.adobe.com/security/resources.html*
Security @ Adobe blog: *blogs.adobe.com/security*

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com