AWS alignment with Motion Picture of America Association (MPAA) Content Security Model

The Motion Picture of America Association (MPAA) has added an additoinal set of best practices which is focused around applications and cloud security. These controls were added with the April 2015 MPAA update. For additional information on MPAA content security best practices refer to: http://www.fightfilmtheft.org/best-practice.html.

The table below was created by AWS to highlight the delta between the MPAA best practices published in 2013 and the MPAA best practices published in 2015.

- For any new control added to the 2015 MPAA best practices, see any rows highlighted in "green."
- For any control set which had a slight change between the 2013 MPAA best practices and the 2015 best practices, see any row highlighted in "blue."
- For any control set which was removed from the 2015 MPAA best practices, these controls were highlighted in "grey."
- Any control set which is not highlighted the requirements behind the controls were fundamentally unchanged

MPAA Best Practices 2015			MPAA Best Practices 2013			AWS comments on the differences between 2015 and 2013 version
Security Topic	No.	Best Practice	Security Topic	No.	Best Practice	
Development Lifecycle	AS-1.0	Build security into the entire Systems/Software Development Lifecycle (SDLC).				2015 MPAA added this control set.
	AS-1.1	Test security across the entire application and infrastructure.				
	AS-1.2	Perform fuzz testing and defect remediation to discover security loopholes in software, operating systems or networks by massive inputting of random data to the system in an attempt to make it crash (e.g., buffer overflow, cross-site scripting, denial of service attacks, format bugs, SQL injection).				
	AS-1.3	Perform bug tracking and defect remediation in conjunction with extensive black box testing, beta testing, and other proven debugging methods.				
	AS-1.4	Provide training and user guides on additions and changes to the application.				
Authentication & Access	AS-2.0	Implement secure authentication.				2015 MPAA added this control set.
	AS-2.1	Register user devices.				
	AS-2.2	Implement secure password recovery.				
	AS-2.3	Follow the principle of least privilege.				
	AS-2.4	Implement controls to prevent brute force attacks.				
	AS-2.5	Implement and document a process to secure key / cryptographic storage and ensure ongoing secure management.				
	AS-2.6	Enable an auto-expiration setting to expire all external links to content after a user-defined time.				
	AS-2.7	Use human verification tools such as CAPTCHA or reCAPTCHA with web applications.				
	AS-2.8	Provide clients with the ability to limit the number of times an asset may be downloaded or streamed by a particular user.				
	AS-2.9	Confirm the upload and download of all content and critical assets.				
	AS-2.10	Include a brief message on mobile applications to remind users to enable device passwords and to enable remote wipe and device location software.				
Secure Coding and Systems	AS-3.0	Perform penetration testing / web application security testing prior to production deployment, and at least quarterly thereafter. Validate vulnerabilities were remediated with a retest.				2015 MPAA added this control set.
	AS-3.1	Perform vulnerability testing at least quarterly.				
	AS-3.2	Utilize cookies in a secure manner, if they need to be used				
	AS-3.3	Validate user input and implement secure error handling.				
	AS-3.4	Implement secure logging procedures.				
	AS-3.5	Implement an SIEM (Security Information Event Management System) to aggregate and analyze the disparate logs.				
	AS-3.6	Encrypt all content and client data at rest.				
	AS-3.7	Encrypt all content and client data in transit.				
	AS-3.8	Implement controls for secure session management.				
	AS-3.9	Implement controls to prevent SQL injection.				
	AS-3.10	Implement controls to prevent unvalidated URL redirects and forwards.				
	AS-3.11	Implement controls to prevent connections from anonymity networks (e.g., Tor, Freenet, Netshade), if possible.				
	AS-3.12	Implement controls to prevent IP address leakage.				
	AS-3.13	Implement controls to prevent XSS (Cross-site scripting).				
	AS-3.14	Allow senders the option to include session-based forensic (invisible) watermarking for content.				
	AS-3.15	Implement a formal, documented content / asset lifecycle.				
	CS-1.0	Compliance with the MPAA Content Best Practices Common Guidelines is required. Where stronger controls exist within the Application Security and Cloud/Distributed Environment Guidelines, the stronger policy will prevail.				2015 MPAA added this control set.
	CS-1.1	Perform a third party security audit at least once per year (e.g., SSAE 16 Type 2, SOC 1, ISO 27000/27001, MPAA).				
	CS-1.2	Document and implement security and privacy policies that are aligned with security industry frameworks for Information Security Management (e.g., ISO-27001, ISO-22307, CoBIT).				
	CS-1.3	Document and implement information security baselines for every component of the infrastructure (e.g., Hypervisors, operating systems, routers, DNS servers, etc.).				
	CS-1.4	Document and implement personnel security procedures that align with the organization’s current information security procedures.				
	CS-1.5	Require all employees, contractors, and third parties to sign confidentiality / non-disclosure agreements when going through the onboarding process.				

MPAA Best Practices 2015			MPAA Best Practices 2013			AWS comments on the differences between 2015 and 2013 version
Security Topic	No.	Best Practice	Security Topic	No.	Best Practice	
Organization & Management	CS-1.6	Document and implement procedures for conducting security due diligence when offloading functionality or services to a third party.				
	CS-1.7	Document and implement segregation of duties for business critical tasks.				
	CS-1.8	Provide clients with information regarding locations for their content and data.				
	CS-1.9	Develop a documented procedure for responding to requests for client data from governments or third parties.				
	CS-1.10	Establish policies and procedures for labeling, handling, and securing containers that contain data and other containers.				
	CS-1.11	Establish procedures for the secure deletion of content/data, including archived and backed-up content/data.				
	CS-1.12	Establish, document and implement scenarios to clients in which client content/data may be moved from one physical location to another.				
	CS-1.13	Establish, document and implement additional key management features, controls, policies and procedures.				
	CS-1.14	Train personnel regarding all policies and procedures.				
	CS-1.15	Establish a process to notify clients when material changes are made to security/privacy policies.				
	CS-1.16	Plan, prepare and measure the required system performance to ensure acceptable service levels.				
	CS-1.17	Develop and maintain additional requirements for incident response and immediate notification to the client in the event of any unauthorized access to systems or content.				
Operations	CS-2.0	Secure datacenter utilities services and environmental conditions.				2015 MPAA added this control set.
	CS-2.1	Ensure the data center has appropriate perimeter and physical security controls.				
	CS-2.2	Develop, document and maintain additional requirements for business continuity planning.				
	CS-2.3	Develop, document and maintain additional change and configuration controls.				
	CS-2.4	Maintain a complete inventory of all critical assets, including ownership of the asset.				
	CS-2.5	Maintain an inventory of all critical supplier relationships.				
	CS-2.6	Develop and maintain service level agreements (SLA's) with clients, partners, and service providers.				
Data Security	CS-3.0	Implement a process to provide all relevant logs requested for good cause to clients in a format that can be easily exported from the platform for analysis in the event of a security incident.				2015 MPAA added this control set.
	CS-3.1	Consider providing the capability to use system geographic location as an additional authentication factor.				
	CS-3.2	Provide the capability to control the physical location/geography of storage of a client's content/data, if requested.				
	CS-3.3	Establish procedures to ensure that non-production data must not be replicated to production environments.				
	CS-3.4	Establish, document and implement a published procedure for exiting the service arrangement with a client, including assurance to sanitize all computing systems of client content/data once the client contract has terminated.				
	CS-3.5	Establish and document policies and procedures for secure disposal of equipment, categorized by asset type, used outside the organization's premises.				
	CS-3.6	Implement a synchronized time service protocol (e.g., NTP) to ensure all systems have a common time reference.				
	CS-3.7	Design and configure network and virtual environments to restrict and monitor traffic between trusted and untrusted connections.				
	CS-3.8	Design, develop and deploy multi-tenant applications, systems, and components such that client content and data is appropriately segmented.				
	CS-3.9	Use secure and encrypted communication channels when migrating physical servers, applications, and content data to/from virtual servers.				
	CS-3.10	Implement technical measures and apply defense-in-depth techniques (e.g., deep-packet analysis, traffic throttling, black-holing) for detection and timely response to network-based attacks associated with unusual ingress/egress traffic patterns (e.g., NAC spoofing and ARP poisoning attacks and/or DDOS attacks).				
	CS-3.11	Establish and document controls to secure virtualized environments.				