MOTION PICTURE ASSOCIATION OF AMERICA, INC.

MPAA Site Security Program

CONTENT SECURITY BEST PRACTICES

COURIER, DELIVERY AND FREIGHT SUPPLEMENTAL

Version 2.0

May 15, 2011

Document History

Version	Date	Description	Author
1.0	December 31, 2009	Initial Public Release	Deloitte & Touche LLP MPAA MPAA Member Companies
2.0	May 15, 2011	Updates and Revisions Consolidation into Common Guidelines and Supplementals	PwC LLP MPAA MPAA Member Companies

I. COURIER, DELIVERY AND FREIGHT OVERVIEW

General Description

Courier, Delivery and Freight facilities are responsible for transporting physical media (such as film, hard drives and DVDs) containing content from one point to another.

Facility

The following table describes the attributes of the content generally held at this facility type:

Type of Content
☑ Stills
☑ Script
☑ Audio Only
☑ Video and Audio

Video Attribute	Description
Completeness	☑ Full ☑ Partial
Resolution	☑ High ☑ Low
Quality	☑ Clean ☑ Watermarked ☑ Spoiled

Typical Risks

Typical security and content protection risks for this facility type include, but are not limited to, the following:

- Loss, interception, or theft of sensitive content such as:
  - Complete or partial video married with audio
  - All resolutions of film and files on data tape
  - Master audio files
  - High resolution files on HDD
  - Video tape dubs at varying resolutions
- Lack of comprehensive screening and background checks of courier, delivery, and freight personnel
- Ad-hoc processes around asset tracking and handling that may not be consistently followed
- Ad-hoc processes around notification of losses and theft of missing content that may not be consistently followed
- Lack of asset classification and education on handling highly sensitive content

II. Best Practice Supplemental Guidelines

MANAGEMENT SYSTEM		PHYSICAL SECURITY			DIGITAL SECURITY		
ORGANIZATION AND MANAGEMENT	COMPETENCY	FACILITY	ASSET MANAGEMENT	TRANSPORT	INFRASTRUCTURE	CONTENT MANAGEMENT	CONTENT TRANSFER

No.	Security Topic	Best Practice	Implementation Guidance
MS.S-3.0	Security Organization	Establish a security team that is responsible for proactively monitoring **information systems** and physical security to identify and respond to any suspicious activity	• Monitor **information systems** regularly throughout the day to detect possible incidents • Incorporate the **incident response** process to handle detected incidents • Consider implementing automatic notification to the team when suspicious activity involving **information systems** is detected • Implement a periodic review process to monitor the effectiveness of monitoring processes

No.	Security Topic	Best Practice	Implementation Guidance
MS.S-13.0	Third Party Use and Screening	Communicate to clients the use of third-party storage providers for physical assets	• Provide clients with **due diligence** reports for third party storage companies • Require clients to approve and sign-off on the use of third party storage companies
MS.S-13.1		Require international (to/from U.S.) transportation companies to be "Customs-Trade Partnership Against Terrorism" (CTPAT) certified	• Require international transportation companies to present proof of CTPAT certification upon first hire • Maintain a list of CTPAT certified transportation companies
MS.S-13.2		Re-assess transportation and packaging vendors annually and when the vendor changes its location and/or provides additional services	• Implement procedures to track which vendors have undergone **due diligence** for the year (e.g., database repository, certificates of completion)

No.	Security Topic	Best Practice	Implementation Guidance
PS.S-1.1	Entry/Exit Points	Lock and install alarms on all loading dock doors, and monitor loading dock doors while in use	• Unlock loading docks only for transactions that have a valid work order • Require the appropriate company personnel to be present at all times during loading
PS.S-13.1	Inventory Tracking	Lock up and log assets that are delayed or returned if shipments could not be delivered on time	• Establish a procedure for storing assets in an access-controlled area • Maintain documentation that logs the on-site storage of assets, including date and reason for storage

No.	Security Topic	Best Practice	Implementation Guidance
PS.S-16.1	Client Assets	Use an access-controlled cage for the staging area and always monitor the area with surveillance cameras	
PS.S-16.2		Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight	• Secure safe by bolting it to an immovable surface (e.g., floor, wall)

No.	Security Topic	Best Practice	Implementation Guidance
PS.S-19.1	Shipping	Require personnel picking up package(s) to verify the count against shipping document and obtain a signature from the shipping point	• Require recipients to reconcile that the shipped count matches their work orders • Report back any discrepancies or damage to shipped goods immediately
PS.S-19.3		Implement a formal process to record, monitor, and review travel times, routes, and delivery times for shipments between facilities	• Establish a baseline for delivery times between common shipping points and monitor actual times for variance • Investigate, report, and escalate major variances to appropriate personnel • Designate approved rest stops
PS.S-23.0	Transport Vehicles	Include the following security features in transportation vehicles (e.g., trailers): • Segregation from driver cabin • Ability to lock and seal cargo area doors • GPS for high-security shipments	• Use vehicles equipped with GPS or XDA tracking systems for delivery of sensitive content and high-value assets
PS.S-23.1		Apply numbered seals on cargo doors for shipments of highly sensitive titles	• Require security guards to apply, record, and monitor seals • Consider additional security measures for highly sensitive packages (e.g., locked/secured cargo area, locked pelican cases)
PS.S-23.2		Require security escorts be used for delivery of highly sensitive content in high-risk areas	• Hire security personnel capable of protecting highly sensitive content from hijacking, mugging, and other scenarios which could result in content theft

Appendix A — Mapping of Supplemental Controls to References

The following table provides a general mapping of the best practices to the ISO 27001/27002 and NIST 800-53 standards. These standards can be referenced for further information on the implementation of the provided security controls.

No.	Security Topic	ISO 27002 Reference	NIST Reference
MS.S-3.0	Security Organization	6.1.3	PE-6, PM-2, SI-4
MS.S-13.0	Third Party Use and Screening	6.2.1	
MS.S-13.2		6.2.3, 10.2.2	PS-3
PS.S-1.1	Entry/Exit Points	9.1.6	PE-3, PE-7, PE-16
PS.S-13.1	Inventory Tracking	9.2.1	MP-2, MP-4
PS.S-16.1	Client Assets	9.1.2	PE-3, PE-6
PS.S-16.2		9.2.1	MP-2, MP-4
PS.S-19.1	Shipping	10.8.2, 10.8.3	
PS.S-19.3		10.8.2	MP-5, PE-16
PS.S-23.1		10.8.3	

End of Document