

AIS SECURITY SEAL VENDORS AND GUIDELINES

Introduction

The companies listed below have been identified as potential sources of tamper-resistant security seals. This list is provided as a reference. It is neither intended to be all-inclusive nor is it considered as a list of endorsed products.

1. **WELDON, WILLIAMS & LICK**
P.O. Box 168
Fort Smith, AR 72902
(800) 242-4995
(501) 783-4113
2. **BAY AREA LABELS**
1980 Lundy Ave.
San Jose, CA 95131
(800) 229-1980 (N. CA only)
(408) 432-1980
3. **MODERN DATA INDUSTRIES**
P.O. Box 26159
San Diego, CA 92196
(858) 566-9300
4. **TAPE & LABEL
CONVERTERS**
8231 Allport Avenue
Santa Fe Springs, CA 90670
(888)285-2462 (CA only)
(562) 945-3486
5. **GM NAMEPLATE, INC.**
2095 O'toole Ave
San Jose, CA 95131
(408) 435-1666
6. **SETON NAME PLATE COMPANY**
P.O. Box 819
Branford, CT 06405
(203) 488-8059
7. **LYNN PEAVEY COMPANY**
14865 W. 105th Street
Lenexa, KS 66215
(800) 255-6499
8. **OPSEC ADVANTAGE, INC.**
1809 Olde Homestead Lane
Lancaster, PA 17601
(717) 293-4110 Ext. 221
9. **AVERY DENNISON**
685 Howard St.
Buffalo NY 14240
(800) 542-8379
10. **AVERY DENNISON**
8500 Leesburg Pike, Suite 7600
Vienna, VA 22182
(703) 288-0324
11. **DESIGNER DECAL, INC.**
East 1120 First Avenue
Spokane, WA 99202
(800) 622-6333
(509) 535-0267

Guidelines

The ISSM (Information System Security Manager) must ensure that the following seal-related guidelines are implemented and identified in their System Security Plan (SSP).

1. Must be placed on the access points of each device.
 - Over seams
 - Over Screws
2. Must be consecutively numbered or individually identifiable.
3. Should bear a unique identification.
4. Must be safeguarded before use.
5. Must be accounted for and logged in when used.
6. Must serve its purpose.
 - Test acquired seals. If once applied can they be peeled off and reapplied without showing evidence? If so, find other seals.
 - Seals will deteriorate over a period of time. Fragibility will vary depending on the surface it's applied on. For example, on metal it may last five years, on plastic only a few months.

Procedures

Prior to the IS being upgraded, every seal must be inspected for tampering. If tampering is suspected, the ISSM must be notified so that a thorough inspection of the equipment can be conducted prior to classified processing. This must be part of the User's Upgrading action and documented in the Upgrading Action Log/record.

Remember that seals are to assist in detecting unauthorized tampering of the accredited components of the information system (IS) while in an unclassified state.

Seals, if used as a minimum level of unauthorized detection of unclassified components of the IS, all components must have seals applied.

- NSA Type One Devices do not require seals with the exception of the Secure Terminal Equipment (STE)
- You do not need to place a seal on a mouse.

SEALS ARE NOT AUTHORIZED TO PROTECT CLASSIFIED DEVICES.

Seal Placement, Markings, Security Audit Log/Record



Tamper Resistant Seal Log				
Seal Number	IS Component Applied to	Who Applied	Date Applied	Remarks
001	Printer	ISSO	9 Aug 02	IS System 1
002	CPU Box	ISSO	9 Aug 02	IS System 1
003	CPU Box	ISSO	9 Aug 02	IS System 1
004	Keyboard	ISSO	9 Aug 02	IS System 1
005	Display Screen	ISSO	9 Aug 02	IS System 1
006	Printer	ISSO	10 Sep 02	IS System 2
007	CPU Box	ISSO	10 Sep 02	IS System 2
008	CPU Box	ISSO	10 Sep 02	IS System 2
009	Keyboard	ISSO	10 Sep 02	IS System 2
010	Display Screen	ISSO	10 Sep 02	IS System 2

Sample Log

**001 John J. Jones
29 Aug 2002**

Place seal(s) over one or more seams and/or screws. Seal is applied where it must be violated to enter a component of the IS