

# Security Kit Interface Board Instruction Sheet

## INTRODUCTION

Use the following instructions when installing the Security Kit interface board in CP2000/M/MR, CP2000-h/i, S/SB, X/XB and CP2000-ZX models. The purpose of the Security Kit is to ensure the content on the interface board is protected. Image decryption keys on the Security Kit interface board are erased if it is tampered with in any way. The Security Kit interface board is constantly monitored even when it is not installed in a projector.

## SECURITY KIT PART NUMBERS

All previous boards have been upgraded to the new Gore enclosure, which contains the glue cable. They are all now Type 5 boards.

Security Kit Part Number	Description
003-120460-05	NEW HDCP-1TK SEC Kit "Glue Cable board" (Type 5)
004-120460-05	Refurb HDCP-1TK SEC Kit "Glue Cable board" (Type 5)
004-120383-11	Upgrade SEC Kit - 1CP (HDCP) "Glue Cable board" (Formerly Type 4)
004-100031-11	Upgrade SEC Kit - 1SR (Secure Ready) "Glue Cable board" (Formerly Type 2)
004-100170-11	Upgraded SEC Kit - 1S (Upgraded 1SR) (Secure) "Glue Cable board" (Formally Type 3)
004-100171-11	Upgraded SEC Kit - 1RH (RoHS Hybrid) (Formally Type 3)
004-100119-11	Upgraded SEC Kit - 1R (RoHS) "Glue Cable board" (Formally Type 3)

**NOTE:** Type 2, 3 and 4 listed above have been upgraded to security kit.

## WARNING AND SAFETY GUIDELINES

**⚠ WARNING** Always power down and disconnect/disengage all power sources to the projector before servicing or cleaning.

**NOTICE:** Observe all electrostatic precautions. Use a grounded wrist strap when handling electronics.

- DO NOT remove the security cover from the interface board. It is not field serviceable.
- Press in the ejector tabs to insert the interface board from the cardcage. During insertion ensure the tabs are pressed inline with the hinge.
- Exercise caution when installing the Security Kit interface board to avoid scratching or flexing the security cover.
- DO NOT use chemicals to clean the security cover. If necessary, only use a dry cloth.

## OVERVIEW OF SECURITY KIT

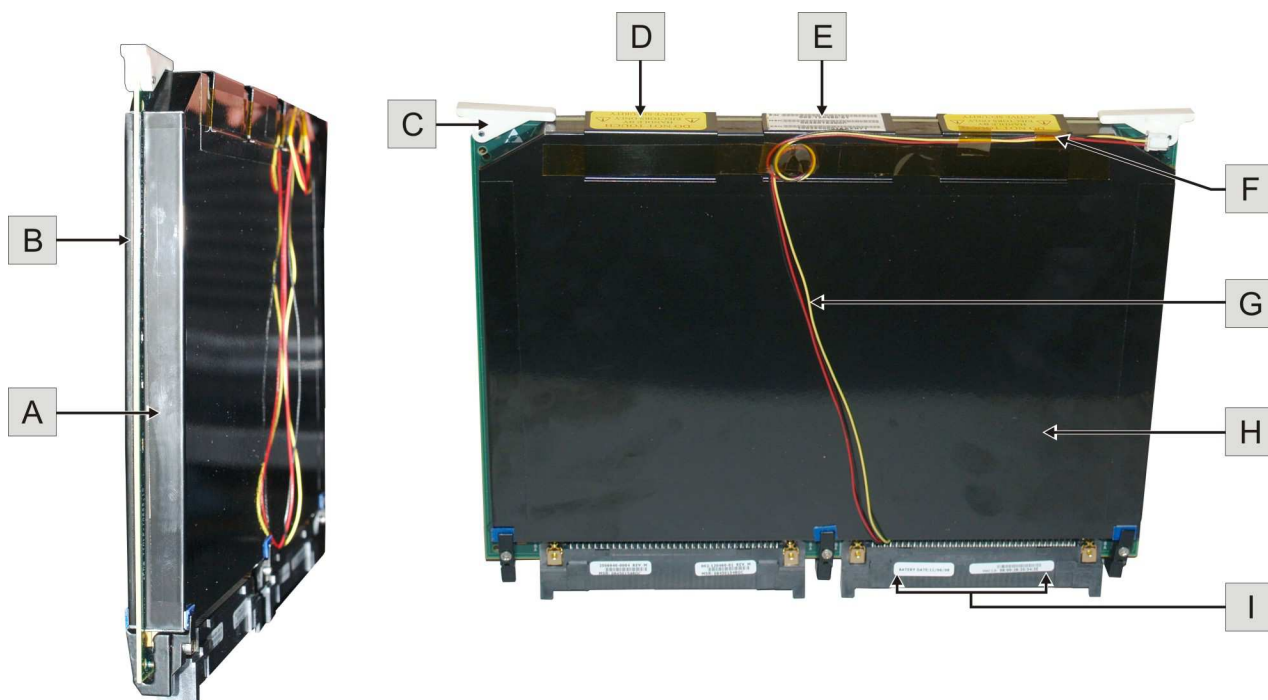


Figure 1 Security Kit

<b>A</b>	Component Side	<b>F</b>	Battery Harness Tape
<b>B</b>	Non-component Side	<b>G</b>	Battery Harness
<b>C</b>	Ejector Tab	<b>H</b>	Security Kit Cover
<b>D</b>	Metal Clips	<b>I</b>	Manufacturer and Electronic Serial Numbers
<b>E</b>	Manufacturer and Electronic Serial Numbers		

## INSTRUCTIONS

Make sure you have read and understood all instructions before handling and installing the Security Kit Interface Board.

### UNPACKING

**WARNING! Remove all hand jewelry before handling the board. Ensure all packaging is saved for shipping non-secured interface boards back to the factory.**

### INSTALLATION

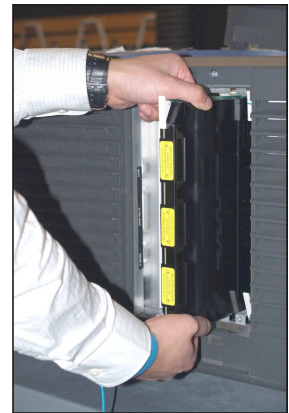
#### **FOR CP2000-ZX, CP2000-M/MR MODELS ONLY**

1. **BEFORE** removing the non-secure interface board, upgrade the DLP<sup>®</sup> projector software to v14.2.50 (or higher). This is required to run the projector with the new Security Kit interface board. PCM 3.0 (or higher) is mandatory to ensure the proper status reports are logged. For software upgrade instructions, refer to [Software Upgrade, on page 6](#). Remove the PCM cover, unlock and remove the projector's front lid and remove the PCM PCB.

2. Wearing a grounded wrist strap, remove the non-secure interface board. First release the ejector tabs on board, then gently pull on the tabs to remove the board slightly from the cardcage. Handling the board along its taped edges only, carefully remove it from the cardcage and place it into a protective ESD sleeve. **(Figure 2).**

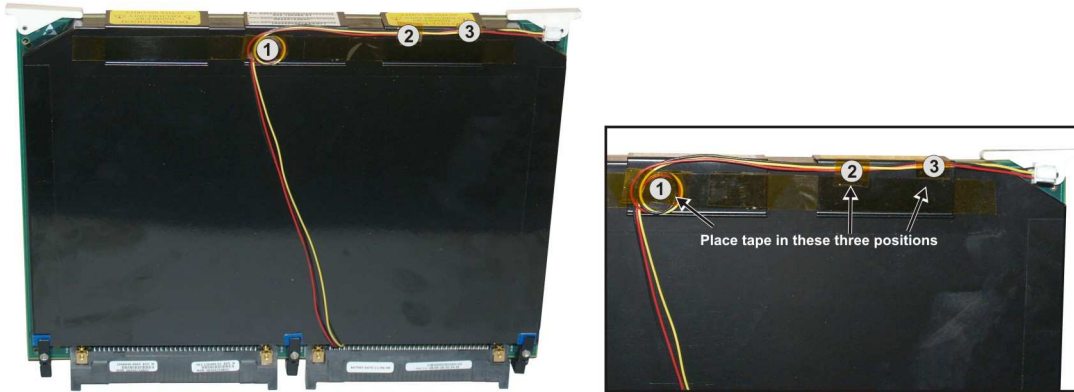
**NOTE:** Pack the non-secure board using the shipping material that came with the new board. Send it back to the factory according to standard RMA procedures.

3. Following the safe handling details provided in the Warning and Safety Guidelines section, remove the Security Kit interface board from its packaging. **NOTE:** Record the Manufacturers Serial Number (MSN), Electronic Serial Number (ESN) of the board, and the serial number of the projection head. These numbers must be added to the Network Operator Center (NOC) ticket call log.



**Figure 2 Board Removal**

4. Ensure the battery harness is routed, as shown in **Figure 3**. If the battery harness is not routed in this way, coil the wire and position the harness as shown, and secure the harness to the metal clips using tape.



**Figure 3 Routing Battery Harness**

5. Align the board with the guide rails in the cardcage.
6. Push on the **outer edge of both ejector tabs** to fully seat the board in the cardcage.
7. Visually inspect the alignment of the ejector tabs on the newly installed security interface board with the other boards in the cardcage. All tabs should be flush with each other. (**Figure 4**)
8. Reinstall the PCM cover, front lid and the PCM PCB.



**Figure 4 Install Board**

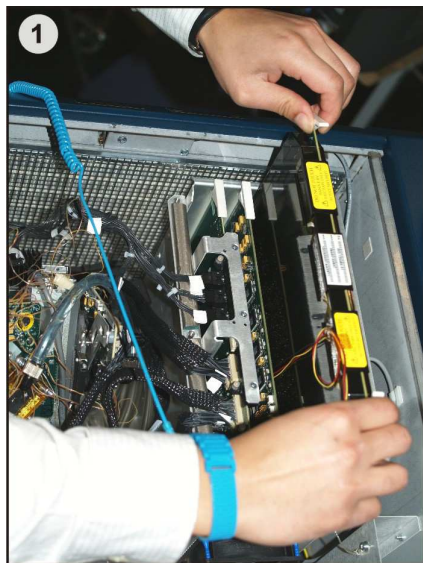
**FOR CP2000-h,i,S/SB,X/XB MODELS ONLY**

Installing the Security Kit interface board in CP2000-h, i, S/SB, X/XB models is similar to the procedure for the CP2000-ZX, with the only difference being the cardcage is accessed from the top of the projector instead of the operator side.

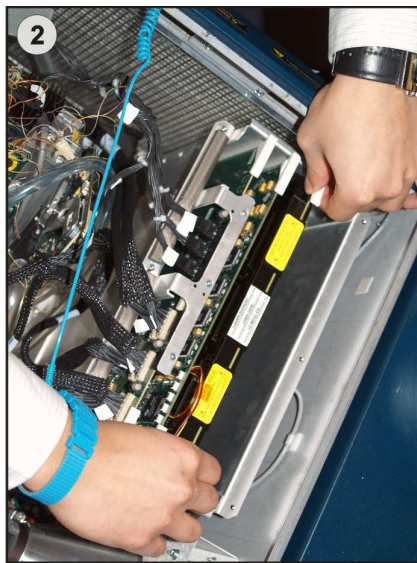
Refer to *Installation for CP2000-ZX* for complete installation/handling instructions.

In general,

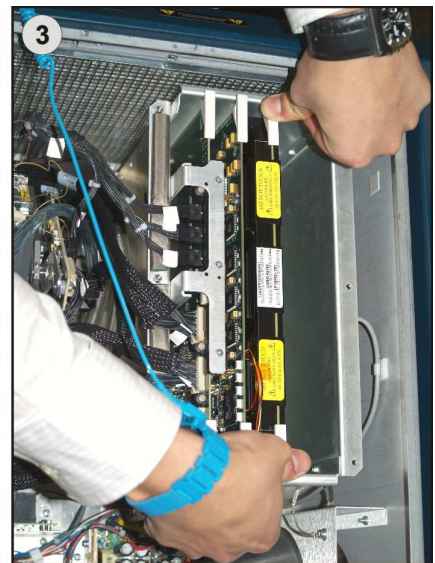
1. **BEFORE** removing the non-secure interface board, upgrade the DLP® projector software to v14.2.50 (or higher). Install TPC 2.9 (or higher). This is mandatory to ensure the proper status reports are logged. For software upgrade instructions, refer to [Software Upgrade, on page 6](#)
2. Remove the light engine lid and cardcage lid. Refer to the *CP2000 Service Manual*.
3. Wearing a grounded wrist strap, remove the existing non-secure interface board. Handling the board along its taped edges only, place it into a protective ESD sleeve.
4. Hold the Security Kit interface board from both the ejector tabs and insert into the cardcage guide rails (**Figure 5, #1**).
5. Carefully, slide the board into the cardcage (**Figure 5, #2**).
6. Press on both ejector tabs until the board is properly seated in the cardcage (**Figure 5, #3**). Ensure the tabs are inline with the hinges.
7. Replace the light engine lid and cardcage lid.



**Line-up with guide rails**



**Slide into cardcage**



**Seat board in cardcage**

**Figure 5 Install Security Kit Interface Board**

## SOFTWARE UPGRADE

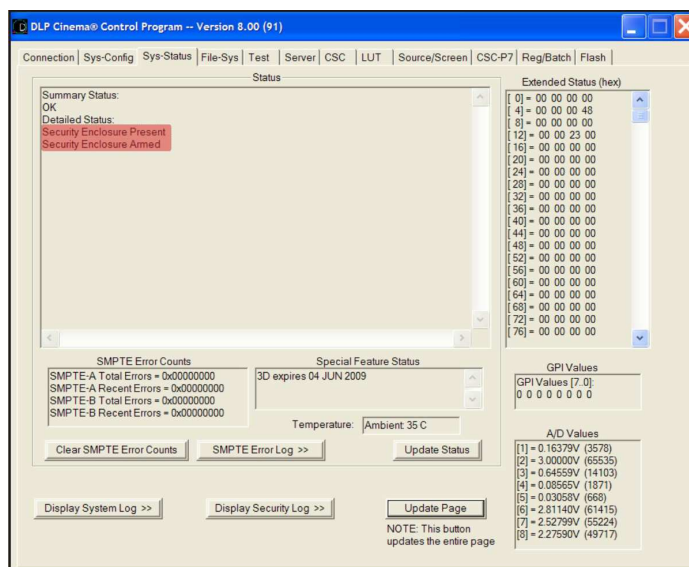
**DLP® Software v14.2.50 (or higher) is required to run the projector with the Security Kit Interface Board. TPC 2.9 (or higher) and PCM 3.0 (or higher) are mandatory to ensure the proper status reports are logged.** For details, contact Christie Technical Support (1-800-221-8025). For the most current listings, refer to the website at [www.christiedigital.com](http://www.christiedigital.com), click on the **Contact Us** tab and select **Technical Support**.

### **To upgrade projector software to v14.2.50 or higher:**

1. Power-up the projector.
2. Open DLP Cinema® Firmware Installation Program V3.01(28) or higher.
3. Enter the projector's IP Address and connect via the Ethernet Port. **NOTE:** Default IP Addressing for the Security Kit as follows:
  - IP Address: 192.168.100.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.100.1
  - DNS Server: 192.168.100.1
4. Log on to the projector.
5. Click **Select Release Installation File**, locate the **Release 14** (or higher) folder and select the *Release.dlpcinema* file.
6. Confirm the correct release version is displayed in the window installation program; click the **Start Auto-Install** button to begin the installation. This process could take several minutes.
7. Exit the DLP Cinema® Firmware Installation Program.
8. Reset the IP address. For details, refer to the *User Manual*.

## CONFIRMING A SUCCESSFUL INSTALL

1. Open the latest DLP Cinema® Control Program. Enter the projector's IP Address and connect via the Ethernet Port.
2. Log on to the projector.
3. Click the **Sys-Status** tab and check the **Status** window (**Figure 6**) for the following entries:
  - **Security Enclosure Present**
  - **Security Enclosure Armed**



**Figure 6 Status Window - Successful Install Messages**

## CONTROL DISPLAY PANEL (CDP) AFTER A SUCCESSFUL INSTALL

When the system successfully installs the **Security** menu on the CDP will display:

- Security Installed: Yes
- Security Armed: Yes
- Security Tamper: No

To access the **System** menu on the CDP go to **Menu>Status>Security**.



Figure 7 CDP Successful Install

## TOUCH PANEL CONTROLLER (TPC) AFTER A SUCCESSFUL INSTALL

When the system successfully installs the TPC **Status** menu will display green LEDs for each of the Security Enclosure variables. To access the **Status** menu on the TPC, go to **System>Status** and scroll down to **Security Enclosure**.



Figure 8 TPC Successful Install

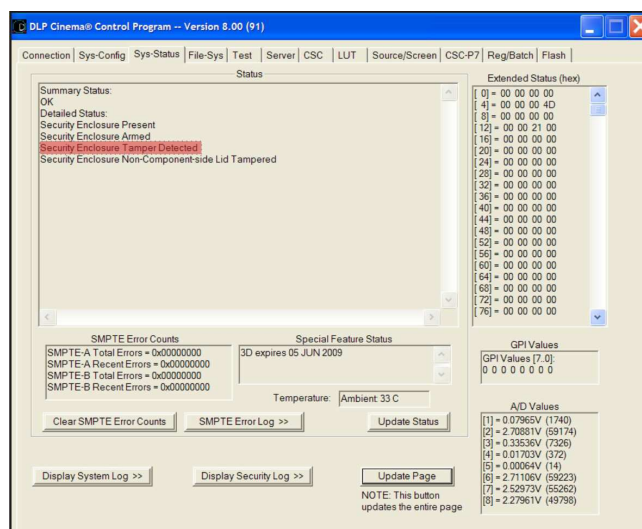
## UNSUCCESSFUL INSTALL - TAMPERED SECURITY KIT

If installation was unsuccessful and a tamper is detected, it is recommended you record the Electronic Serial Number from the security kit and contact Christie Technical Support for further action. You may also install a new Security Kit interface board if available. If a board is not available at the time, reinstall the existing non-secure interface board and replace it once a new Security Kit interface board is available.

You will see the following messages if there has been a tamper.

- **Security Enclosure Tampered Messages**

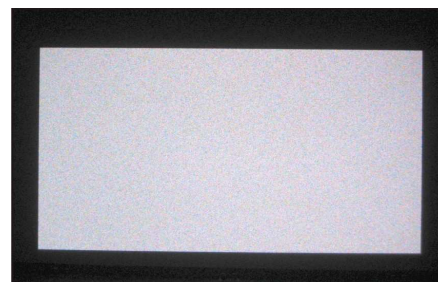
In the **Sys-Status** window the following message appears if the security enclosure has been tampered (**Figure 9**).



**Figure 9 System Status - Tamper Messages**

- **Security Enclosure Tamper Detected**

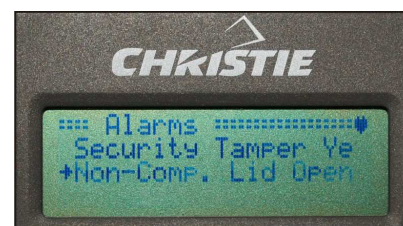
When the system detects a tampered Security Kit, the image shown in **Figure 10** is projected on screen when playing secured content.



**Figure 10 CineLink Snow**

## CONTROL DISPLAY PANEL (CDP) WHEN TAMPER DETECTED

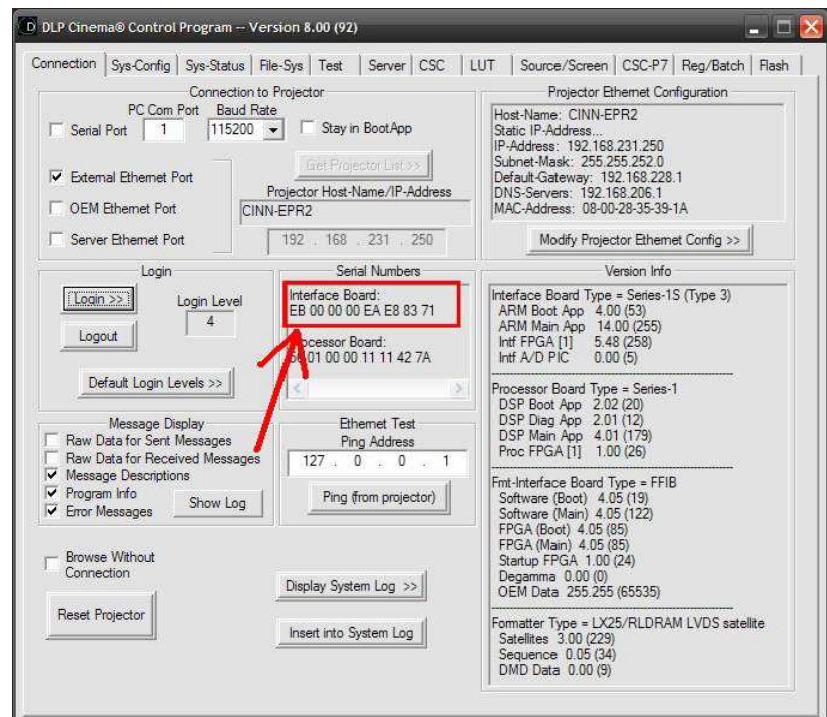
When a tampered Security Kit is detected the CDP displays **Security Tamper Yes** (**Figure 11**).



**Figure 11 CDP Security Menu**

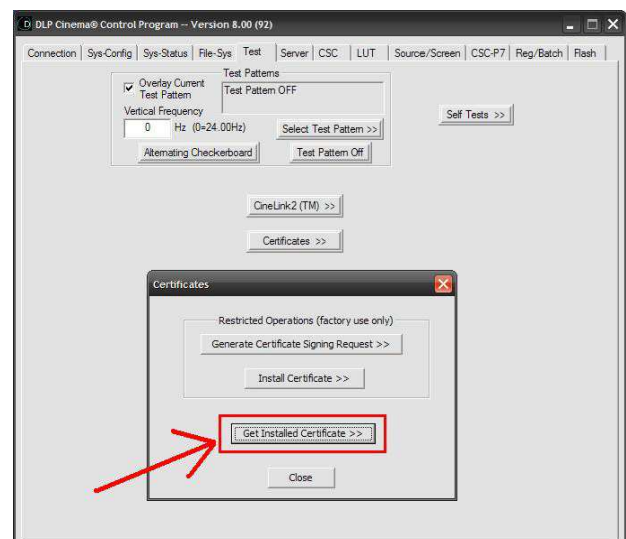
## CERTIFICATE VALIDATION AND LOGGING

1. After confirming a successful Security Kit installation, use the DLP Control Program® to connect to the DLP electronics. Log in and record the Electronic Serial Number (ESN) of the Security Kit interface board - refer to **Figure 12**.



**Figure 12 Electronic Serial Number**

2. Navigate to the **Test** page and click on the **Certificates >>** button. A dialogue box will pop up - click on **Get Installed Certificate** - see **Figure 13**. Save the certificate to your PC. The filename of the certificate will contain the Security Kit ESN. Verify that the ESN in **Figure 12** and the filename match.
3. The default filename of the certificate should have the Security Kit interface board ESN. Verify that the ESN is correct by comparing it to the ESN displayed on the **Connection** page of the DLP Control Program. These MUST match.
4. Using the Managed Services Sharepoint system, track your installation by recording the ESN of the Security Kit interface board in this database. Also verify that all corresponding information for that particular screen is correct (i.e. Projector serial number, screen number, site name etc). This will ensure the database is maintained and up-to-date for KDM's generated as part of the Trusted Device List.



**Figure 13 Downloading Certificate**

## CHECKLIST FOR TAMPERED SECURITY KIT

Use the following checklist whenever you encounter a “tampered” Security Kit interface board.

1. Record the following information for **each** tamper:

- Exhibitor
- Security Kit
- Projector Model (CP-S/SB, CP-X/XB etc.)
- Projector Serial Number
- Security Kit Manufacturer’s Serial Number (MSN)
- Security Kit Electronic Serial Number (ESN)
- NOC Call Log Ticket Number (if applicable)

2. Distinguish between 5 possible types of tampers. Tamper types are defined as:

- **Type 1 - Shipping Tamper**

Unit was already tampered upon install and no physical damage can be seen on the GORE material. A review of the Security Logs should show the time of tamper to be in the past.

- **Type 2 - Installation Tamper**

Symptoms will be similar to Type 1, but the tamper date\time shown in the Security Log should reflect the exact time the board was handled and physically installed into the projector on the initial power-up.

- **Type 3 - Button-Up Tamper**

Security Kit was shown to be un-tampered during initial installation but registered a tamper upon start-up after installing all covers, screws, etc...). Again, a review of the System Log and Security Log will need to be done to determine this.

- **Type 4 - Battery Harness Connector causing ‘GORE’ Damage**

- **Type 5 - Post-Installation Tamper**

Security Kit registered a tamper after running for some time.

- **Type 6 - Other**

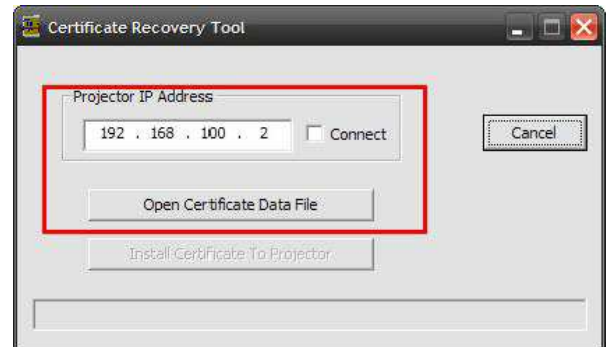
3. Data Collection

- Dump all relevant log files (i.e. System Log, Status Summary, Security Log, TPC Error Logs) using the DLP Control Program.
- Take pictures of any damage to the GORE material, enclosure overhang, loose enclosure clamps etc.
- *Send data to Christie Technical Support. To contact them call 1-800-221-8025 or go to our website at [www.christiedigital.com](http://www.christiedigital.com), click on the **Contact Us** tab and select **Technical Support***

## RE-ARM ATTEMPT PROCEDURE

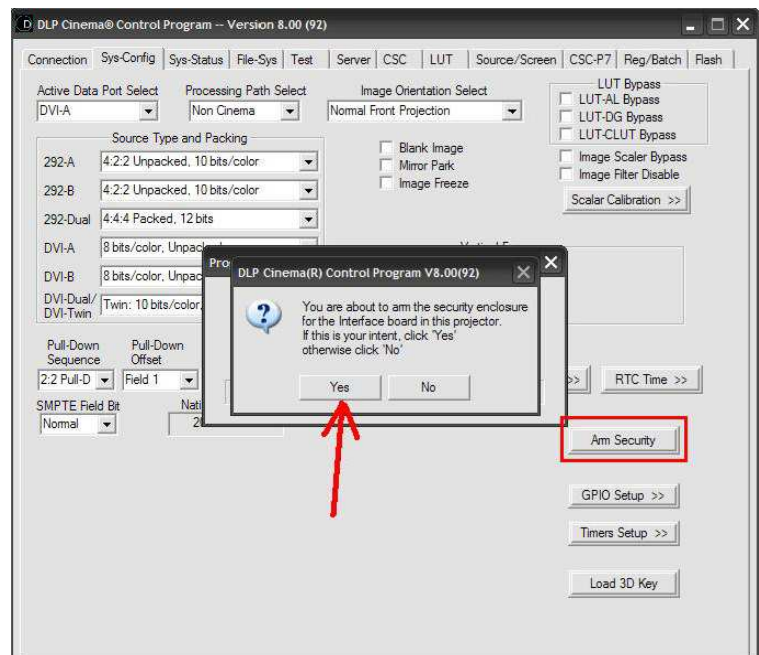
Use this procedure only after you have determined you have a tamper Type 1, 2 or 3. For all other tampers, send the board back under standard RMA procedure.

1. Contact Christie Technical Support with the ESN of the Security Kit. Christie will put in a request to the contract manufacturer for a new certificate to be generated for that particular Security Kit. This may take up to 24hrs.
2. You will receive a \*.crf file and a Certificate Recovery Tool that will need to be installed on your PC.
3. Once the software tool is installed, load the Certificate Recovery Tool, enter the IP address of the DLP electronics on that projector and click Connect. Click on **Certificate Data File** and browse for the \*.crf file that was given to you from Tech Support - see **Figure 14**.



**Figure 14**

4. Now you are ready to load the new certificate to the Security Kit interface board. Press **Install Certificate To Projector**. You may be asked for a login and password - use the same login credentials as you would use for the DLP Cinema Control Program. This should only take 20-30 seconds at most. You will be prompted with a message that the certificate was either loaded successfully or unsuccessfully. If the certificate would not load, double check that the ESN given to Christie Technical Support was correct. You will have to acquire a new \*.crf file in this case.



**Figure 15 Re-Arm**

5. If the certificate loaded successfully, you must now attempt to re-arm the Security Kit interface board. Close the **Certificate Recovery Tool** and load the **DLP Cinema Control Program®**.

Login and navigate to the **Sys-Config** page and press the **Arm Security** button - see **Figure 15**. You will be prompted with a message asking you to proceed - press **Yes**.

6. If the Security Kit 'arms' successfully, refer to section [\*Certificate Validation and Logging, on page 9\*](#) and complete the installation procedure.
7. If the Security Kit does not arm successfully, the board must be sent back to Christie under standard RMA procedure.