Keysight E8247C, E8257C, E8267C, E8257D, E8267D, E8257N, E8663B, E8663D PSG Signal Generators

Security Features and Document of Volatility

KEYSIGHT TECHNOLOGIES

Notices

Copyright Notice

Manual Part Number

E8251-90379

Edition

Edition: 1, March 2022

Supersedes: February 2020

Published by:

Keysight Technologies Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S Government Rights

The Software is “commercial computer software,” as defined by Federal Acquisition Regulation (“FAR”) 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement (“DFARS”) 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at http://www.keysight.com/find/sweula

The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data.

Warranty

THE MATERIAL CONTAINED IN THIS DOCUMENT IS PROVIDED “AS IS,” AND IS SUBJECT TO BEING CHANGED, WITHOUT NOTICE, IN FUTURE EDITIONS. FURTHER, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, KEYSIGHT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, WITH REGARD TO THIS MANUAL AND ANY INFORMATION CONTAINED HEREIN, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. KEYSIGHT SHALL NOT BE LIABLE FOR ERRORS OR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, USE, OR PERFORMANCE OF THIS DOCUMENT OR OF ANY INFORMATION CONTAINED HEREIN. SHOULD KEYSIGHT AND THE USER HAVE A SEPARATE WRITTEN AGREEMENT WITH WARRANTY TERMS COVERING THE MATERIAL IN THIS DOCUMENT THAT CONFLICT WITH THESE TERMS, THE WARRANTY TERMS IN THE SEPARATE AGREEMENT SHALL CONTROL.

Safety Information

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

WARNING

A **WARNING** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Where to Find the Latest Information

Documentation is updated periodically. For the latest information about these products, including instrument software upgrades, application information, and product information, see the following URLs:

http://www.keysight.com/find/psg

To receive the latest updates by email, subscribe to Keysight Email Updates:

http://www.keysight.com/find/emailupdates

Information on preventing instrument damage can be found at:

http://www.keysight.com/find/PreventingInstrumentRepair

Is your product software up-to-date?

Periodically, Keysight releases software updates to fix known defects and incorporate product enhancements. To search for software updates for your product, go to the Keysight Technical Support website at:

http://www.keysight.com/find/techsupport

Table of Contents

1 Contacting Keysight Sales and Service Offices

Assistance with test and measurement needs, and information to help you find a local Keysight office, is available via the internet at, http://www.keysight.com/find/assist. If you do not have internet access, please contact your designated Keysight representative.

NOTE

In any correspondence or telephone conversation, refer to the instrument by its model number and full serial number. With this information, the Keysight representative can determine whether your unit is still within its warranty period.

2 Products Covered by this Document

Product Family Name	Product Name	Model Number	Firmware Revision
Keysight Signal Generators	PSG Signal Generator	E8663D	All
		E8663B	All
		E8267D	All
		E8267C	C.03.40 or higher
		E8257N	All
		E8257D	All
		E8257C	C.03.40 or higher
		E8247C	C.03.40 or higher

CAUTION

While the table above lists *All* for some models and firmware revisions, older firmware versions with the use of certain security features may cause the deletion of some of the instrument's system files. Before using the security features, please update your firmware to the appropriate revision listed in Chapter 8, "Security Issues for Certain Firmware Revisions".

Document Purpose

This document describes instrument memory types and security features. It provides a statement regarding the volatility of all memory types, and specifies the steps required to declassify an instrument through memory clearing, sanitization, or removal.

For additional information, go to:

http://www.keysight.com/find/security

IMPORTANT

Be sure that all information stored by the user in the instrument that needs to be saved is properly backed up before attempting to clear any of the instrument memory. Keysight Technologies cannot be held responsible for any lost files or data resulting from the clearing of memory.

Be sure to read this document entirely before proceeding with any file deletion or memory clearing.

3 Security Terms and Definitions

Term	Definition
Clearing	As defined in Section 8-301a of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)", clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. Hence, clearing is typically used when the instrument is to remain in an environment with an acceptable level of protection.
Instrument Declassification	A term that refers to procedures that must be undertaken before an instrument can be removed from a secure environment, such as is the case when the instrument is returned for calibration. Declassification procedures include memory sanitization or memory removal, or both. Keysight declassification procedures are designed to meet the requirements specified in DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)", Chapter 8.
Sanitization	As defined in Section 8-301b of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)", sanitization is the process of removing the data from media before reusing the media in an environment that does **not** provide an acceptable level of protection for the data that was in the media before sanitizing. Hence, instrument sanitization is typically required when an instrument is moved from a secure to a non-secure environment, such as when it is returned to the factory for calibration. Keysight memory sanitization procedures are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS). These requirements are specified in the "Clearing and Sanitization Matrix" in Section 5.2.5.5.5 of the ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM.
Secure Erase	Secure Erase is a term that is used to refer to either the clearing or sanitization features of Keysight instruments.

4 Instrument Memory & Volatility

This chapter contains information on the memory components in your instrument.

NOTE **The sanitization procedures described in this chapter are not available in the E8257N instrument, unless Option 340 is installed.**

The tables provide details of the size of each memory component, its type, how it is used, its location, volatility, and the sanitization procedure.

Table 4-1 Base Instrument (All models and options)

Memory Component, Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
1. Main Memory (SDRAM) 64 MByte	Yes	No	Firmware operating memory	Operating system (not user)	CPU board. Not battery backed.	Turn off instrument power.
2. Main Memory (Flash) 20 MByte	Yes	Yes	Factory calibration/ configuration data User file system, which includes instrument status backup, flatness calibration, IQ calibration, instrument states, waveforms (including header and marker data), modulation definitions, and sweep lists	Firmware upgrades and user-saved data	CPU board (same chip as firmware memory, but managed separately) User data is not stored in this memory if hard disk (Option 005) or flash drive (Option 008/009) is installed.	User data areas are sanitized by the procedure "Erase and Sanitize All" on page 17.

Table 4-1 Base Instrument (All models and options)

Memory Component, Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
3. Firmware Memory (Flash) 12 MByte	No	Yes	Main firmware image	Factory installed or firmware upgrade	CPU board (same chip as main flash memory, but managed separately)	None required (no user data)
	Yes	Yes	LAN configuration	Front panel entry or remotely		
4. Battery Backed Memory (SRAM) 512 KByte	Yes	Yes	User-editable data (table editors) Last instrument state, last instrument state backup, and persistent instrument state and instrument status	Firmware operations	CPU board The battery is located on the CPU board.	Sanitized by the procedure described in "Erase and Sanitize All" on page 17.
5. Bootrom Memory (Flash) 128 KByte	No	Yes	CPU bootup program and firmware loader/updater	Factory programmed	CPU board During normal operation, this memory cannot be overwritten or erased.	None required (no user data)
6. Calibration Backup Memory (Flash) 512 KByte	No	Yes	Factory calibration/ configuration data backup	Factory or service only	Motherboard	None required (no user data)
7. Boards Memory (Flash) 512 Bytes	No	Yes	Factory calibration and information files, code images, and self-test limits	Factory or service only	All RF boards, baseband generator, and motherboard	None required (no user data)
8. Micro-processor Cache (SRAM) 3 KByte	Yes	No	CPU data and instruction cache	Memory is managed by CPU, not user	CPU board, not battery backed.	Turn off instrument power.

Table 4-2 Vector Models with Baseband Generator (E8267D with Options 601 or 602)

Memory Component, Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
1. Waveform Memory (SDRAM) 40 MByte–320 MByte	Yes	No	Waveforms (including header and marker data) and PRAM	Normal user operation	Not battery backed.	Turn off instrument power.
2. BBG Firmware Memory (Flash) 32 MByte	No	Yes	Firmware image for baseband generator	Firmware upgrade		None required (no user data)
3. Co-processor Memory (SRAM) 32 MByte	Yes	No	Operating memory of baseband co-processor CPU	During normal operation, some user information, such as payload data, can remain in the memory.	This memory is used during normal baseband generator operation. It is not directly accessible by the user. Not battery backed.	Turn off instrument power.
4. Buffer Memory (SRAM) 5 x 512 KByte	No	No	Support buffer memory for ARB and real-time applications	Normal user operation	This memory is used during normal baseband generator operation. It is not directly accessible by the user. Not battery backed.	Turn off instrument power.

Table 4-3 Hard Disk (E8267C/E8267D with Option 005)

Memory Component, Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks[a]	Sanitization Procedure
1. Media Storage (Built-in Hard Disk) 6 GByte or 10 GByte (4 GByte usable in both cases)	Yes	Yes	User files, including flatness calibrations, IQ calibration, instrument states, waveforms (including header and marker data), modulation definitions, and sweep lists	User-saved data	If it is installed, these files are stored on the hard disk instead of in flash memory.	The magnetic residue requires several rewrite cycles or drive removal and destruction. User data is completely sanitized by the procedure "Erase and Sanitize All" on page 17.
2. Buffer Memory (DRAM) 512 KByte	No	No	Buffer (cache) memory	Normal operation, via hard disk		Turn off instrument power.

Table 4-4 Flash Drive (E8257N with Options 008, E8257D/E8663D with Option 008, and E8267D with Option 009)

Memory Component, Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks[a]	Sanitization Procedure
1. Memory Storage (Removable Flash drive) Size varies	Yes	Yes	User files, including flatness calibrations, IQ calibration*, instrument states, waveforms (including header and marker data), modulation definitions, and sweep lists (* This is not the instrument calibration data, which is stored in the instrument's main memory. See item 2 in Table 4-1 above.)	User-saved data	If it is installed, these files are stored on the flash drive instead of in flash memory.	User data is completely sanitized by the procedure "Erase and Sanitize All" on page 17.[b]

a. With serial number prefixes ≥ US/MY4829 the E8267D Option 005 built-in hard disk (drive) is replaced with the E8267D Option 009 removable flash drive.

b. If Option 008/009 was factory installed, then removing the flash drive card from an instrument with one of these options sanitizes the instrument. Otherwise perform the "Erase and Sanitize All" feature.

5 Memory Clearing, Sanitization and Removal Procedures

This chapter describes several security functions you can use to remove sensitive data stored in the instrument before moving it from a secure development environment. The functions described are:

- "Erase All" on page 15
- "Erase and Overwrite All" on page 16
- "Erase and Sanitize All" on page 17
- "Clear Persistent State Information" on page 18

NOTE The functions described in this chapter are **not** available in the E8257N instrument, unless Option 340 is installed.

CAUTION These functions do **not** erase or sanitize external media connected to the instrument's USB port.

CAUTION The use of older firmware during a security feature operation may result in the loss of instrument system files. Before using the security features, please update your firmware to the appropriate revision listed in Chapter 8, "Security Issues for Certain Firmware Revisions"

CAUTION An interruption of instrument power during a security feature operation may cause the loss of instrument system files such as calibration and licenses.

Erase All

This function removes all user files, user flatness calibrations, user I/Q calibrations, and resets all table editors with original factory values, ensuring that user data and configurations are not accessible or viewable. The instrument appears as if it is in its original factory state, however, the memory is not sanitized. This action is relatively quick, typically taking less than one minute (the exact time depends on the number of files).

Key Sequence: **Utility** > **Memory Catalog** > **More** > **Security** > **Erase All** > **Confirm Erase**

Note that there is a similar but distinct function, as described below, that deletes all user files but does **not** reset the table editors:

Key Sequence: **Utility** > **Memory Catalog** > **More** > **Delete All Files**

Erase and Overwrite All

This function performs the same actions as **Erase All**, plus it clears and overwrites various memory types, as described below.

Memory Type	Models	Description
CPU Flash	All	User data is erased with flash chip block-erase commands. No overwrite is performed. During erasure, the system files are temporarily moved to main memory and are then restored to CPU Flash when erasure is complete.
Hard Disk	E8267C, E8267D with Option 005	All addressable locations are overwritten once with a random character.
Flash Drive	E8257N with Options 008 E8257D, E8663D with Option 008 E8267D with Option 009	All addressable locations are overwritten once with a random character.

Model	Key Sequence
All	**Utility** > **Memory Catalog** > **More** > **Security** > **Erase and Overwrite All** > **Confirm Overwrite**

Erase and Sanitize All

This function performs the same actions as **Erase All**, plus it clears and overwrites the various memory types, as described below.

Memory Type	Models	Description
SRAM (Battery- backed)	All	All addressable locations are overwritten once with random characters.
CPU Flash	All	User data is erased with flash chip block-erase commands. No overwrite is performed. During erasure, the system files are temporarily moved to main memory and are then restored to CPU Flash when erasure is complete.
Hard Disk	E8267C, E8267D with Option 005	All addressable locations are overwritten with a random character three times.
Flash Drive	E8257N with Options 008 E8257D, E8663D with Option 008 E8267D with Option 009	All addressable locations are overwritten with a random character three times.

Key Sequence: **Utility** > **Memory Catalog** > **More** > **Security** > **Erase and Sanitize All** > **Confirm Sanitize**

Clear Persistent State Information

The persistent state settings contain instrument setup information that can be toggled within predefined limits such as display intensity, contrast and the GPIB address. In vector models, the user IQ Cal is also saved in this area.

The following functions can be used to clear the IQ Cal file and to set the operating states that are not affected by an instrument power-on, preset, or ***RST** command to their factory default:

Instrument Setup

Key Sequence **Utility** > **Power On/Preset** > **Restore System Defaults** > **Confirm Restore Sys Defaults**

SCPI Command: `:SYSTem:PRESet:PERSistent`

LAN Setup

The LAN setup (hostname, IP address, subnet mask, and default gateway) information is not modified by an instrument power-on or ***RST** command.

This information can be changed or cleared by entering new data.

User IQ Cal File (Vector Models Only)

When a user-defined IQ Calibration has been performed, the cal file data is removed by using the Erase All feature, or by setting the cal file to default, as follows:

Key Sequence: **I/Q** > **I/Q Calibration** > **Revert to Default Cal Settings**

SCPI Command: `:CAL:IQ:DEF`

6 Using Secure Mode

NOTE The "Secure Mode" procedure described here is **not** available on 8257N instruments (unless Option 340 is installed), or on E82x7C instruments with firmware revisions earlier than C.03.76.

CAUTION The use of the security features **Erase All**, **Erase and Overwrite All**, **Erase and Sanitize All**, **Erase**, **Overwrite**, or **Sanitize** with older firmware, may cause the deletion of some of the instrument's system files. Before using the security features, please update your firmware to the appropriate revision listed in Chapter 8, "Security Issues for Certain Firmware Revisions".

Secure Mode automatically applies the selected **Security Level** action the next time the instrument's power is cycled.

To activate Secure Mode, do the following:

Step	Action	Notes
1	Open the Security Level menu	Press: **Utility** > **Memory Catalog** > **More** > **Security** > **Security Level**
2	Select the Security Level	Available options: – **None** – equivalent to a factory preset, no user information is lost – **Erase** – equivalent to Erase All – **Overwrite** – equivalent to Erase and Overwrite All – **Sanitize** – equivalent to Erase and Sanitize All

Step	Action	Notes
3	Activate Secure Mode	**CAUTION** Once you activate secure mode (by pressing **Confirm)**, you cannot deactivate or decrease the Security Level; the erasure actions for the selected Security Level execute at the next power cycle. Once you activate Secure Mode, you can only increase the Security Level until you cycle power. For example, you can change **Erase** to **Overwrite**, but not the reverse. After the power cycle, the Security Level selection remains the same, but the secure mode is not activated. Press: **Utility** > **Memory Catalog** > **More** > **Security** > **Enter Secure Mode** > **Confirm** The **Enter Secure Mode** softkey changes to **Secure Mode Activated**.

7 Using Secure Display

NOTE

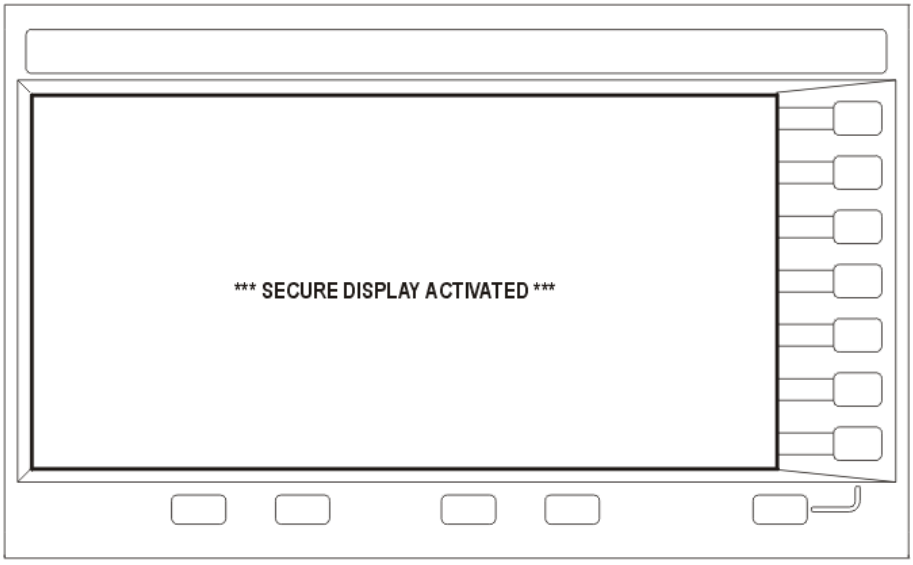
Front panel control of this feature is **not** available on theE8257N instruments (unless Option 340 is installed), or on E82x7C instruments with firmware revisions earlier than C.03.76. The feature can be activated remotely, however, using SCPI commands. Refer to the “System Commands” chapter of the instrument’s **SCPI Command Reference** for more information.

This function prevents unauthorized personnel from reading the instrument display or tampering with the current configuration via the front panel. When Secure Display is active, the display is blank, except for an advisory message, as shown in Figure 7-1 below. All front panel keys are disabled.

To set Secure Display, press: **Utility** > **Display** > **More** > **Activate Secure Display** > **Confirm Secure Display**

Once Secure Display has been activated, the power must be cycled to re-enable the display and front panel keys.

Figure 7-1 Signal Generator Screen with Secure Display Activated



8 Security Issues for Certain Firmware Revisions

CAUTION If your instrument currently has one of the firmware revisions listed in Table 8-1, using certain security features may cause the deletion of some of the instrument's system files. Before using the security features, update your firmware to the appropriate revision listed in the "Update to" column of Table 8-1.

Table 8-1 Firmware Revisions by Instrument Model

Model	Affected firmware revisions	Update to
E8257D	C.04.81, C.04.85, or C.04.92	C.04.94 or later
E8267D	C.04.81, C.04.85, or C.04.92	C.04.94 or later
E8663B	C.04.90	C.04.93 or later

Firmware Update Procedure

To obtain the latest firmware online, perform the following steps:

1. Access the instrument's web page: `www.keysight.com/find/<model_number>` (Example: www.keysight.com/find/e8267d).
2. Under the **Support**, select **Drivers, Firmware and Software**, and follow the remaining links to the firmware upgrade page.

If web access is not available, Keysight can provide the new firmware on CD-ROM. To obtain the CD-ROM, contact Keysight or your Keysight representative, as described in "Contacting Keysight Sales and Service Offices" on page 5.

Error Messages and Secure Environments

If you cannot upgrade the firmware prior to using the security features, Keysight will help you to recover from error messages that may appear after executing the security functions. The error messages indicate that instrument system files have been erased. The following list shows some possible error messages:

- `256, File name not found; /SYS/LICENSE.TXT`
- `617, Configuration Error; License file not found. Creating empty one.`
- `A missing or damaged system file was encountered while trying to diagnose the system.`

Even if these error messages appear, the security function has completely sanitized the instrument. If the instrument is located in a secure environment, it is safe to remove it. After removing it from the secure area, follow the process below to recover the lost system files.

Recovering Erased System Files

To recover the lost files, perform the following steps:

1. Obtain your instrument's model and serial number.
2. Contact Keysight and request a replacement license file.

   The Keysight representative will ask for the model and serial number.
3. Update the firmware to the revision specified in the "Update to" column of Table 8-1 on page 22.

   a. If problems occur when upgrading the firmware, manually enter as many license keys as possible using **Utility** > **Instrument Adjustments** > **Instrument Options** > **Software Options**

   b. Upgrade the firmware again.
4. Open Internet Explorer and enter `http://<instrument IP address>/update`.
5. Locate **Recover Self-test System Files** and click **Execute**.
6. Locate **Overwrite LICENSE.TXT**, cut and paste the replacement license file (obtained in Step 2) into the text box, and click **Execute**.
7. Cycle the power on the instrument.
8. If configuration errors persist after completing the previous steps, contact Keysight again.

9 Procedure for Declassifying a Faulty Instrument

If the instrument is not functional, and you are unable to use the security functions, you may physically remove the Processor board and Hard Disk or Solid State Drive (if installed).

For removal and replacement procedures, refer to the Service Guide for your instrument.

Once the Processor and Hard Disk assemblies have been removed, proceed as in Table 9-1 below:

Table 9-1 Assembly Disposal Procedures

Assembly	Procedure
Processor (CPU) Board	**Either** Discard the processor board and send the instrument to a repair facility. A new Processor Board will be installed, then the instrument will be repaired and calibrated. If the instrument is still under warranty, you will not be charged for the new Processor Board. **or** If you have another working instrument, install the Processor Board into that instrument and erase the memory. Then reinstall the Processor Board back into the non-working instrument and send it to a repair facility for repair and calibration. If you discover that the Processor Board does not function in the working instrument, discard the Processor Board and note that it caused the instrument failure on the repair order. If the instrument is still under warranty, you will not be charged for the new Processor Board.
Hard Disk E8267D Option 005, and E8267C Option 005	**Either** Discard the Hard Disk and send the instrument to a repair facility. Indicate on the repair order that the Hard Disk was removed and must be replaced. A new Hard Disk will be installed, then the instrument will be repaired and calibrated. If the instrument is still under warranty, you will not be charged for the new hard disk. **or** Keep the Hard Disk and send the instrument to a repair facility. When the instrument is returned, reinstall the Hard Disk.

Table 9-1 Assembly Disposal Procedures

Assembly	Procedure
Solid State (Flash) Drive E8257N Option 008, E8257D/E8663D Option 008, and E8267D Option 009	Remove the Solid State Drive from the instrument, then send the instrument to a repair facility. Indicate on the repair order that the Solid State Drive was removed. When the instrument is returned, reinstall the Solid State Drive. **NOTE** The Solid State (Flash) Drive is not required for repair or calibration, so a Solid State Drive may not be returned with the repaired instrument.

A: References

1. **DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)"**

   United States Department of Defense. Revised February 28, 2006.

   https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodm/522022m.pdf

   The document may also be found by using the search feature on the Defense Security Service (DSS) website:

   https://www.dcsa.mil/

2. **ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM**

   Defense Security Service.

   DSS-cleared industries may request a copy of this document via email, by following the instructions at:

   https://www.dcsa.mil/Portals/69/documents/odaa/ODAA%20Process%20Manual%20Version%203.2.pdf?ver=2018-11-29-102431-710

   The document may also be found by using the search feature on the Defense Security Service (DSS) website:

   https://www.dcsa.mil/

3. **Greenliant NANDrive Security Erase Feature, Purge Command Specification**

   This Application Note may be obtained in PDF format from Greenliant Systems Ltd., by contacting the company via their web site:

   http://www.greenliant.com/contact_us

4. **AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS)**

   INCITS Technical Committee T13/1699-D Revision 6a, September 6th, 2008

   This standard may be downloaded in Acrobat (PDF) format from the INCITS T13 web site:

   https://www.t13.org/

5. **Installation Guide**

   Keysight Technologies Inc.

   http://literature.cdn.keysight.com/litweb/pdf/E8251-90352.pdf

6. **Programming Guide**
Keysight Technologies Inc.
http://literature.cdn.keysight.com/litweb/pdf/E8251-90355.pdf

7. **SCPI Command Reference**
Keysight Technologies Inc.
http://literature.cdn.keysight.com/litweb/pdf/E8251-90356.pdf

8. **Service Guide**
Keysight Technologies Inc.
E8663B Analog Signal Generator
http://literature.cdn.keysight.com/litweb/pdf/E8663-90009.pdf
E8257N, E8257D/67D, E8663D PSG Signal Generators
http://literature.cdn.keysight.com/litweb/pdf/E8251-90359.pdf

Edition 1, March 2022

E8251-90379

www.keysight.com