Keysight N5192A/94A UXG X-Series Agile Vector Adapter

Security Features and Document of Volatility

KEYSIGHT TECHNOLOGIES

Notices

Copyright Notice

Manual Part Number

N5191-90018

Edition

Edition: 1, February 2019

Supersedes: December 2018

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, contact your local Keysight office, as detailed in "Contacting Keysight Sales and Service Offices" on page 5.

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
UXG X-Series Vector Adapter	UXG Agile Vector Adapter	N5192A N5194A	All

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.

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

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 (DRAM) 1 GByte	Yes	No	Firmware operating memory.	Operating system	CPU board, not battery backed. Volatile memory	Turn off instrument power.
2. Main Memory (Flash) 512 MByte, partitioned as follows: 200 MByte: Boot (Main firmware image, Operating system) 50 MByte: System (Calibration/ Configuration) 1 MByte: Secure Storage 180 MByte: Reserved	Yes	Yes	Factory calibration and configuration data plus LAN IP Address Configuration	None	CPU board	None required (no user data)

Table 4-1 Base Instrument

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. Front Panel Memory (Flash) 24 KByte	No	Yes	Front panel keyboard controller firmware	Operating system	Front Panel board	None required (no user data)
4. Front Panel Memory (SRAM) 2 KByte	Yes	No	Front panel operating memory	Front panel firmware	Front Panel board Volatile memory	Turn off instrument power.
5. Front Panel Memory (EEPROM) 256 Byte	No	Yes	Unused	None	Front Panel board	None required (no user data)
6. DAC Board Memory (SRAM) 18 MByte	Yes	No	Stores Loaded list points, etc.	Operating system	DAC Board Volatile memory	Turn off instrument power.
7. DAC Board Memory (EEPROM) 16 MByte	No	Yes	Factory calibration data	None	DAC Board	None required (no user data)
8. Microdeck Board Memory (EEPROM) 6 MByte	No	Yes	Factory calibration data	None	Microdeck Board	None required (no user data)
9. Infrastructure Board Memory (EEPROM) 16 MByte	No	Yes	Factory calibration data	None	Infrastructure Board	None required (no user data)

Table 4-1 Base Instrument

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
10. SSD (Flash) 480 GByte, partitioned as follows: 1 MByte: Reserved 1 1 MByte: Reserved 2 479.998 GByte: User	Yes	Yes	User file system, which includes user flatness calibration*, instrument states, and sweep lists (* This is **not** the instrument calibration data, which is stored in the instrument's main memory. See item 2 above.)	User-saved data	Instrument Rear Panel	Remove SSD Assembly from instrument and store securely. For details of procedure, see "Removal or Replacement of Solid-State Disk Drive (SSD)" on page 14.
11. 10 GByte Ethernet Interface Board Memory (EEPROM) 16 MByte	No	Yes	Factory Calibration Data	None	Rear Panel Board	None required (no user data)

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:

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

Erase SSD

This function erases all user files, such as List files and flatness correction files, from the instrument's SSD, using the ATA command SECURITY ERASE UNIT, with the "Erase Mode" parameter set to "Normal". (For more details of this command, see AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS))

All instrument settings revert to default values, except for LAN and GPIB settings.

No internal settings are stored in the instrument's main memory.

Key Sequence: **System** > **File** > **More** > **Security** > **Erase SSD** > **Confirm Erase**

SCPI Command: `:SYSTem:SECurity:ERASe`

Clear Persistent State Information

The persistent state settings contain instrument setup information that can be specified within predefined limits, such as display intensity, contrast and the GPIB address.

The following key sequence or SCPI command can be used to set most operating states that are not affected by an instrument power-on, preset, or *RST command to their factory default.

NOTE

This command does **not** reset the state of the current mode; see Clear Most Mode States and Persistent State Information below. It also does **not** affect the Multi-box Sync Setup and the LO Control Setup settings.

Key Sequence: **System** > **More** > **Power On/Preset** > **Restore System Settings to Default Values** > **Persistent System Settings** > **Confirm Restoring Persistent System Settings**

SCPI Command: `:SYSTem:PRESet:PERSistent`

Clear Most Mode States and Persistent State Information

This command sets most states of the instrument back to their factory default settings, including all mode states, and states that are not normally affected by instrument power–on, preset, or *RST. This also includes the current mode, which will be set to Normal.

The following key sequence or SCPI command can be used to set operating states that are not affected by an instrument power-on, preset, or *RST command to their factory default:

NOTE

Multi-box Sync Setup and the LO Control Setupsettings are not adjusted by the key sequence nor the command stated in this section.

Key Sequence: **System** > **More** > **Power On/Preset** > **Restore System Settings to Default Values** > **All Settings** > **Confirm Restoring All System Settings**

SCPI Command: `:SYSTem:PRESet:ALL`

Multi-box Sync Setup

NOTE No other feature defaults these values including the actions of **Persistent System Settings** (`:SYSTem:PRESet:PERSistent`) and **All Settings** (`:SYSTem:PRESet:ALL`).

This key sequence or command sets the Multi-box Sync settings to their factory default settings.

The following table shows the key sequence or SCPI command that can be used to set their values to their factory default:

Key Sequence:	**System** > **More** > **Power On/Preset** > **Restore System Settings to Default Values** > **Multi-box Sync Settings** > **Confirm Preset All Multi-box Sync Settings**
SCPI Command:	`:SYSTem:PRESet:MBSync`

LO Control Setup

NOTE No other feature defaults these values including the actions of **Persistent System Settings** (`:SYSTem:PRESet:PERSistent`) and **All Settings** (`:SYSTem:PRESet:ALL`).

This key sequence or command sets the LO Control settings to their factory default settings.

The following table shows the key sequence or SCPI command that can be used to set their values to their factory default:

Key Sequence:	**System** > **More** > **Power On/Preset** > **Restore System Settings to Default Values** > **LO Settings** > **Confirm Restoring LO Settings**
SCPI Command:	`:SYSTem:PRESet:ELO`

LAN Setup

You can reset the LAN setup either via the front panel or by sending a SCPI command.

Key Sequence: **System** > **I/O Config** > **LAN Setup** > **Advanced Settings** > **Restore LAN Settings to Default Values** >**Confirm Restore LAN Settings to Default Values**

SCPI Command: `:SYSTem:COMMunicate:LAN:DEFaults`

Removal or Replacement of Solid-State Disk Drive (SSD)

The Erase SSD procedure described above may be considered sufficient to sanitize the instrument. However, the instrument may also be sanitized by physical removal of the Solid-State Disk Drive Assembly (SSD). The instrument still operates without the SSD, but it is unable to store user data. Calibration data is still available.

Optionally an unclassified replacement SSD may be installed without compromising the instrument sanitized state.

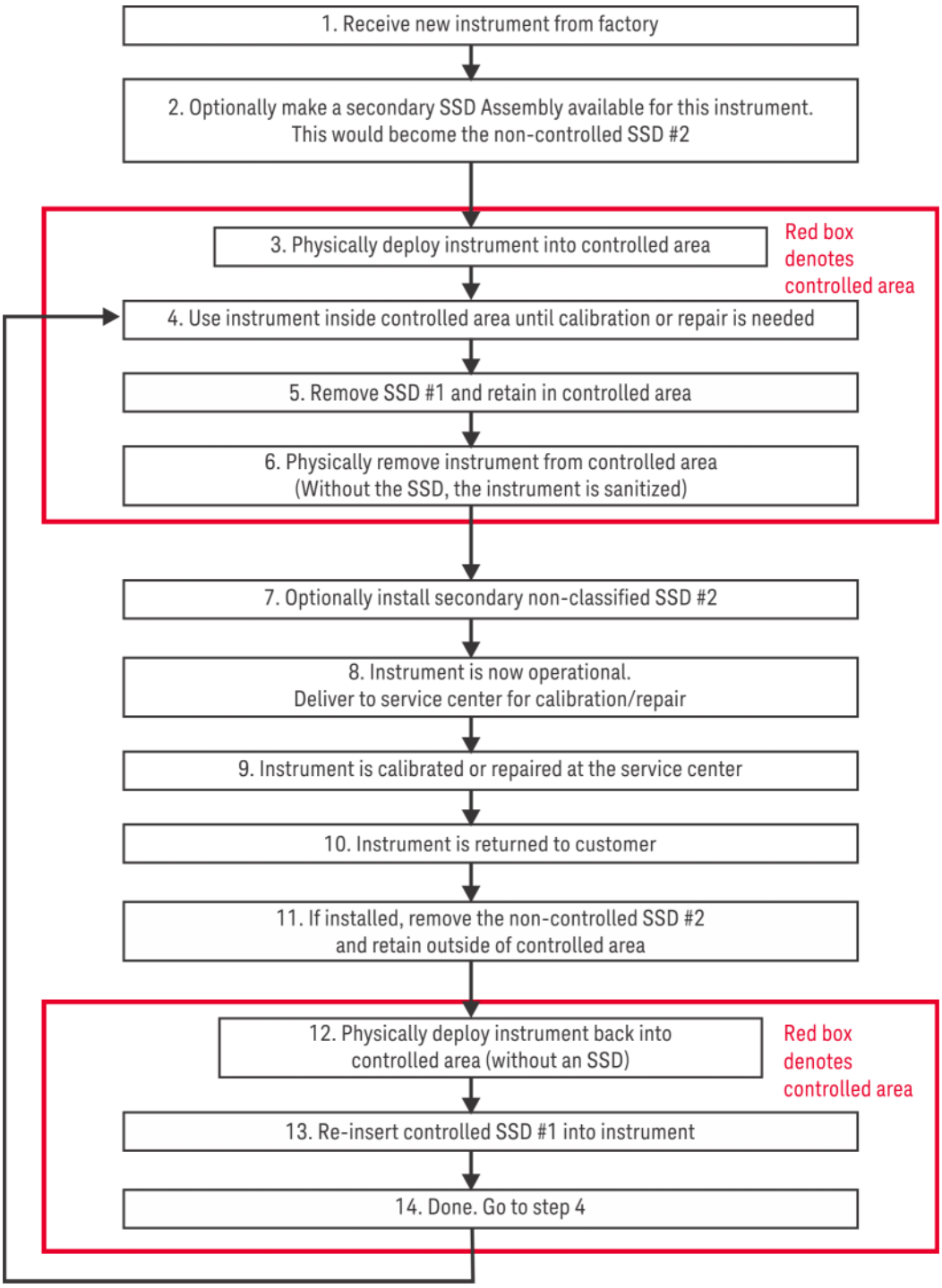
This section describes how to sanitize an instrument by physical removal and optional replacement of the SSD.

Refer to the flowchart in Figure 5-1 below for details of how to perform this procedure.

For the procedure on how to remove the SSD Assembly (flow chart Step 5), see “SSD Removal Procedure” on page 16.

CAUTION **Before removing the SSD Assembly, ensure that the instrument’s power is turned off.**

Figure 5-1 Flowchart for Instrument Sanitization Process by SSD Removal



6 SSD Removal Procedure

This chapter describes the procedures for physical removal and replacement of the instrument's Solid-State Disk Drive assembly (SSD). This is an alternate method for instrument sanitization, in addition to the function "Erase SSD" on page 11 (which does **not** require removal of the SSD and may be considered sufficient to sanitize the instrument).

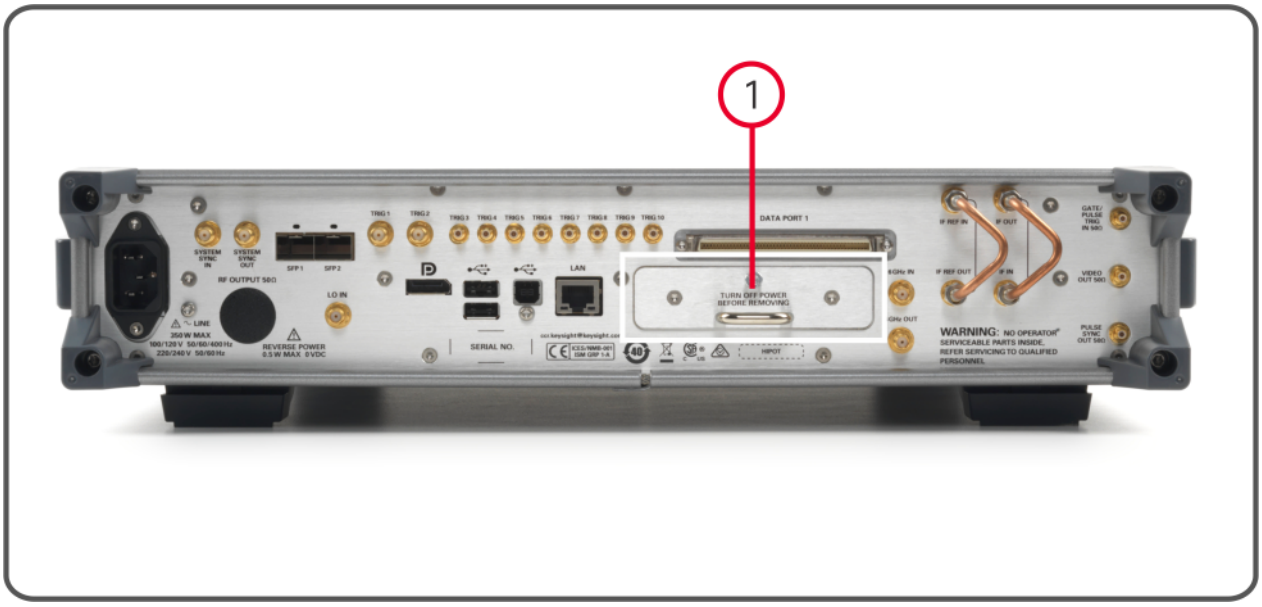
To remove the SSD, use the following procedure. The numbered items in the figures correspond to the step numbers in the procedure.

CAUTION

Before removing the SSD Assembly, ensure that the instrument's power is turned off.

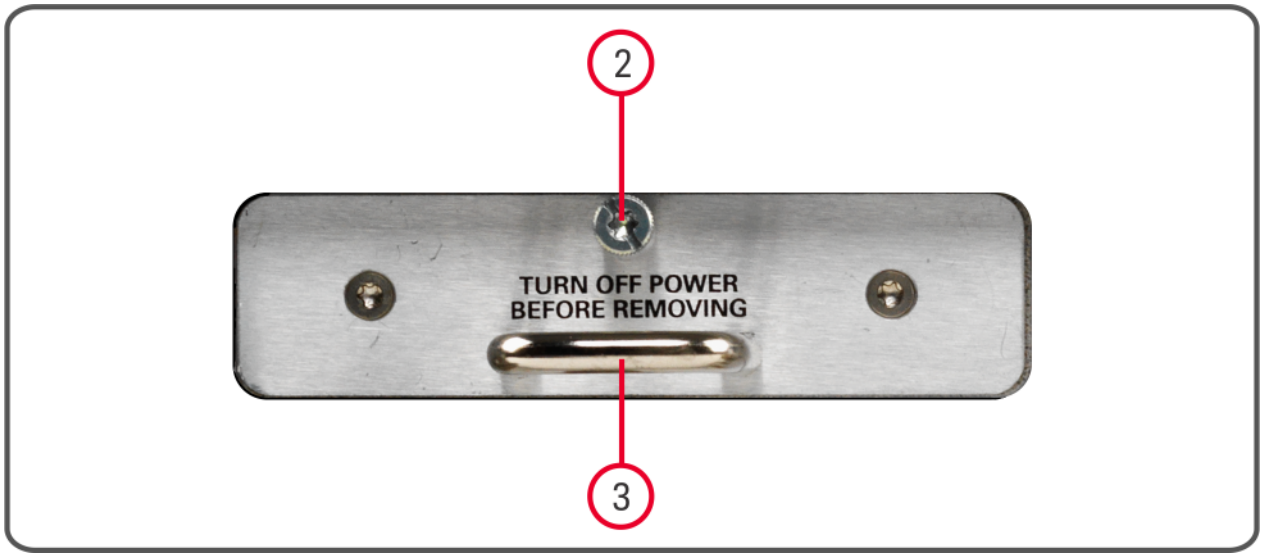
1. Locate the SSD Assembly on the instrument's rear panel, as shown in Figure 6-1.

Figure 6-1 Instrument Rear Panel & SSD Assembly Location



2. Turn the thumbscrew on the SSD panel, as shown in Figure 6-2 below, to release the SSD Assembly from the rear panel. If the thumbscrew is too tight to turn by hand, use a TORX T10 screwdriver to loosen it.

Figure 6-2 Removable SSD Assembly details



3. Pull the U-shaped handle attached to the SSD Assembly, to remove the drive from the instrument, as shown in Figure 6-2 above.

7 Secure Display & Restricted Display

Secure Display

This function prevents unauthorized personnel from reading the instrument display or tampering with the current configuration via the front panel.

– **On** This selection turns the instrument display on, showing the current settings. Cycling the instrument power also restores the display. Note that the current instrument state may be the last state before rebooting.

– **Off** This selection blanks the instrument's display, hiding the settings and disabling the front panel keys.

When Secure Display is active, all front panel keys are disabled, and the display is blank, except for the advisory message:

```
*** SECURE DISPLAY ACTIVATED ***
```

Key Sequence:	**System** > **More** > **Display** > **More** > **Activate Secure Display** > **Confirm Secure Display**
SCPI Command:	`:SYSTem:SECurity:DISPlay ON|OFF|1|0`
Default	ON

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

Restricted Display

This command enables or disables the secure restricted display mode.

– **On** This selection turns on the secure restricted display, blanking the frequency. The keys that access Frequency, and User Amplitude, Phase and Time Corrections, are disabled.

– **Off** This selection turns off the secure restricted display mode, allowing the instrument's display to show the current frequency.

Key Sequence:	**System** > **More** > **Display** > **More** > **Activate Restricted Display** > **Confirm Restricted Display**

SCPI Command: `:SYSTem:SECurity:DISPlay:RESTricted ON|OFF|1|0`

Default OFF

8 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 8-1 below:

Table 8-1 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.

A: References

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

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

   http://www.dss.mil/isp/fac_clear/download_nispom.html

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:

   http://www.dss.mil/documents/odaa/ODAA%20Process%20Manual%20Version%203.2.pdf

3. **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:

   http://www.t13.org/documents/UploadedDocuments/docs2008/D1699r6a-ATA8-ACS.pdf

4. **Getting Started Guide**

   Keysight Technologies Inc.

   Part Number: N5191-90016

   To obtain a copy of this document, contact your local Keysight office, as detailed in "Contacting Keysight Sales and Service Offices" on page 5.

5. **Service Guide**

   Keysight Technologies Inc.

   Part Number: N5191-90019

   To obtain a copy of this document, contact your local Keysight office, as detailed in "Contacting Keysight Sales and Service Offices" on page 5.

Edition 1, February 2019

N5191-90018

www.keysight.com