Rillor

EXPLAINER

What to do before selling surplus GPU servers

Before you sell used GPU servers: save the health logs, find every data store, sanitize and certify each drive under NIST SP 800-88 Rev. 2 and screen the buyer.



Rillor

Contents

01 Summary

02 Background

03 Method

04 Findings

05 Implications

06 Limits of this analysis

07 Sources

Summary

Selling a GPU server hands its drives and logs to a new owner, and NIST SP 800-88 Rev. 2 counts a resale as a change of control over storage media [1].

- A GPU server keeps data beyond its drives. One maker's statement of volatility, its list of the memory in an 8-GPU server [36], includes BIOS settings, a management controller holding user data and logs, and a Trusted Platform Module that stores encryption keys [2].
- NIST SP 800-88 Rev. 2, final in September 2025, defines three sanitization methods: clear, purge and destroy [1]. It prefers purge to clear where possible [1].
- NIST's decision flow destroys media not meant for reuse [1]. Reused media that leaves the organization is purged if its data's security categorization is low or moderate, and destroyed if high [1]. Selling is among NIST's reasons purge can suit better than destroy [1].
- Save health records before any erase. One maker's server-wide erase leaves only the erase request and the controller's restart entries in its Lifecycle Log [3], and NIST advises checking records retention duties before sanitizing [1].
- NIST asks for a certificate of sanitization for each sanitized device, recording the method, technique, tool version, verification and the people who verified and validated the result [1].
- Warranties do not follow every unit. Supermicro's applies only to the original purchaser [4], Dell's can move when the transfer is recorded with Dell, at Dell's sole discretion [5], and NVIDIA support entitlements are non-transferable [6].
- Drives and parts that are not reused can go to a recycler certified to R2 or e-Stewards, the two accredited U.S. standards EPA names, both of which require destruction of all data [7].
- Export rules apply to the sale itself. The Export Administration Regulations (EAR) bar selling an item with knowledge that a violation is about to occur [8], and the Commerce Department's Bureau of Industry and Security (BIS) names domestic and foreign customers alike in its red flags for advanced computing chips [9].

Background

NIST SP 800-88 Rev. 2 covers "media before disposal, reuse, or leaving the effective control of an organization" [1]. It names the moments when control changes: "Media control can change when an ISM is returned from a leasing agreement, donated, resold to be reused outside of the organization, or sent to a recycling facility" [1]. ISM is NIST's abbreviation for information storage media [1]. Nongovernmental organizations may use the guide on a voluntary basis [1].

A GPU server sold to a new owner leaves with every drive, controller and log inside it, and the terms of its first sale decide what warranty and software cover goes with it. Items in the United States and U.S.-origin items wherever located are subject to the EAR [10], so the export rules can follow it too.

This report is for operators and enterprises that refresh GPU fleets and sell the servers they no longer need. It sets out, in order, where the data sits, which records to save, how to sanitize and certify each drive, which warranty and software terms survive a sale, where unusable parts go and how to screen a buyer. Price is a separate question.

Method

Sources. NIST SP 800-88 Rev. 2, its FAQ and the IEEE standards it cites [1, 11, 12, 13]. Makers' documents: one server's statement of volatility, specification sheet and management controller guide, NVIDIA's DGX, nvidia-smi, memory error, triage and Data Center GPU Manager (DCGM) pages, two makers' warranty pages and NVIDIA's support and licensing terms. Tool and interface documentation, the Cybersecurity and Infrastructure Security Agency (CISA) alert on management controllers, EPA, e-Stewards and Sustainable Electronics Recycling International (SERI) on recycling, the EAR in 15 CFR, BIS guidance and the Consolidated Screening List.

How. Each source was read in full or in the part cited, and quotes are copied from it. The EAR was read at its 5 November 2026 issue in the eCFR, and web pages were viewed on 8 November 2026. Tools appear as examples from their makers' documentation, never as a ranking or an endorsement.

Out of scope. Prices, valuations, payment terms, tax and accounting treatment of disposals, and any license decision for a particular server, buyer or destination.

Findings

1. Where data sits in a GPU server

Count every store. NIST notes that many items contain several types of storage media that can need different methods, as a desktop computer holds "a hard drive, motherboard, RAM, and ROM" [1]. Non-volatile storage keeps its contents after power is removed, and NIST says it "is where most organizations should focus their sanitization efforts" [1]. Hidden capacity counts. In NIST's example of a drive with 1,024 GB of physical storage and 900 GB of user capacity, user data may sit on the full 1,024 GB [1].

The statement of volatility. NIST says such a statement generally lists every volatile and non-volatile memory, the nature of its data, whether the user can access it and how it can be erased or sanitized, and that "vendors can state volatility details differently" [1]. Dell's March 2023 statement for its PowerEdge XE9680, an 8-GPU server [36], is one example [2]. It leaves out "Components chosen as user-definable configuration options (those not soldered to the motherboard)" [2].

Store	What it holds	How the statement says it is cleared	Source
Chipset CMOS memory, 256 bytes	Real-time clock and BIOS settings	Jumper, removing the coin cell for 30 seconds, or defaults in F2 setup	[2]
BIOS SPI flash, 32 MB	Boot code, system configuration, UEFI environment, ME	"Not possible with any utilities or applications"	[2]
iDRAC SPI flash, 4 MB, and BMC eMMC, 16 GB	Controller firmware, logs including the System Event Log, MAC address	Not completely. User data, logs and firmware repository through Delete Configuration and Retire System	[2]
Trusted Platform Module (TPM), 128 bytes	Encryption keys	An F2 setup option	[2]

Table 1. Non-volatile stores besides the drives in the statement of volatility of one 8-GPU server [36], which also lists a BOSS-N1 boot controller [2].

Drives and keys. NVIDIA's DGX H100/H200 carries two 1.92 TB NVMe M.2 drives in RAID 1 for the operating system and eight 3.84 TB NVMe U.2 self-encrypting drives (SEDs) in RAID 0 as a data cache [14]. NVIDIA's `nv-disk-encrypt` tool "stores the vault and SED authentication keys on the TPM instead of on the file system", which "allows the vault data to persist even if the system is reimaged" [15]. A reimage leaves those keys in the TPM. The guide gives the BIOS path to clear it, ending in "TPM Clear" [15].

The management controller. CISA and the National Security Agency (NSA) describe baseboard management controllers (BMCs) as components that "operate separately from the operating system (OS) and firmware to allow for remote management and control, even when the system is shut down" [16]. Their settings include network configuration and local usernames and passwords [17], and they leave with the server.

The GPU. NVIDIA describes the InfoROM as "a small, persistent store of configuration and state data for the GPU" [18]. Remapped memory rows are recorded there [19], which makes it part of the health history in Finding 4.

2. Clear, purge and destroy under NIST SP 800-88 Rev. 2

The publication. Revision 2, by Ramaswamy Chandramouli of NIST and Eric Hibbard of Samsung Semiconductor, was published in final form in September 2025 and supersedes Revision 1 of December 2014 [1]. Sanitization "renders access to target data on the media infeasible for a given level of effort" [1]. Rev. 2 keeps its guidance on cryptographic erase (CE) and drops the old technique tables [1]. In NIST's words, "Apart from CE, which is commonly used across all encrypted media, all sanitization technique and tool details have been replaced with recommendations to comply with IEEE 2883, NSA specifications, or an organizationally approved standard" [1]. Its process figure opens with a decision about reuse [1]. NIST's FAQ of 16 July 2026 confirms that Rev. 2 recommends no specific technique per media type [11].

Method	Protects against	How, and the media afterwards	Source
Clear	Simple, non-invasive recovery	Logical techniques through the interface available to the user	[1]
Purge	Recovery with state-of-the-art laboratory techniques	Overwrite, block erase or cryptographic erase under IEEE 2883, media potentially reusable	[1]
Destroy	Recovery with state-of-the-art laboratory techniques	Disintegrate, incinerate, melt, pulverize or shred, media no longer usable for storage	[1]

Table 2. The three methods as NIST SP 800-88 Rev. 2 defines them.

Clear. Clear uses logical techniques on all user-addressable locations, through "the same interface that is available to the user" [1]. On flash with spare cells and wear leveling, overwriting cannot reach all previous data [1]. Overwrite practice once ran "from a single pass to as high as 39", and the FAQ says "Revision 2 clarifies that multi-pass overwriting is unnecessary" [1, 11]. A factory reset without rewriting still counts as clear for devices that offer nothing else, "as long as the device interface available to the user does not facilitate retrieval of the original data" [1].

Purge. Purge defeats laboratory recovery "but preserves the ISM in a potentially reusable state. When possible, the purge sanitization method should be used instead of the clear sanitization method" [1]. Under IEEE 2883, purge techniques "can include overwrite, block erase, and cryptographic erase using dedicated, standardized device sanitize commands", which "require trust and assurance from the ISM vendor that the commands have been implemented as expected" [1]. Degaussing should not be used on flash, and on an SSD it "can complete successfully, but no sensitive data is sanitized" [1].

Destroy. NIST lists disintegrate, incinerate, melt, pulverize and shred, and says drilling or bending "may only partly damage the ISM" [1]. Pulverizing and shredding suit only the lowest security categories, which the FAQ explains by data density [1, 11].

Cryptographic erase. "At a basic level, CE is based on the sanitization of keys used to encrypt data or to prevent access to the keys that encrypt data" [1]. It needs no prior plaintext on the media and a strength of at least 128 bits under ISO/IEC 27040 [1]. Copies matter, since CE "should not be trusted on ISM that have been backed up or escrowed unless the organization has a high level of confidence regarding how and where the keys were stored and managed outside of the ISM" [1]. NIST's ten items to document for CE include whether "the key has ever been escrowed from or injected into the ISM" [1].

Reuse, categorization and control decide the method. In NIST's Fig. 1, media not reused is destroyed, low and moderate media leaving the organization is purged, and high media leaving the organization is destroyed [1]. Purge, and clear where it applies, "may be more appropriate than destroy sanitization techniques when factoring in contractual obligations (e.g., lease returns), environmental concerns, the desire to reuse the ISM (either within the organization or by selling or donating the ISM)" and cost [1]. For media not intended for reuse, "the simplest and most cost-effective sanitization method can be to destroy the media" [1]. NIST prefers sanitizing the whole device, and warns that a sanitized device often does not resemble a factory-fresh one and that "Additional configuration changes may be necessary" before reuse [1]. Before any of it, owners are "strongly advised to consult" privacy officials or records retention offices [1].

The IEEE standards. IEEE 2883-2022, published on 17 August 2022, specifies methods for sanitizing logical and physical storage, with technology-specific requirements [12]. IEEE 2883.1-2025, published on 19 June 2025, recommends how to use those methods "to appropriately sanitize storage media before reuse, resale, or disposal" [13].

Tools, from their makers' documents.

- **NVMe drives.** The nvme-cli `sanitize` command starts a block erase, an overwrite or a crypto erase. Its Purge Required option asks that "the user data be purged as defined by IEEE Std 2883", and a supporting controller fails an operation that does not purge [20].
- **A server-wide erase.** Dell's iDRAC9 `racadm systemErase` can, component by component, reset BIOS and iDRAC to defaults, clear Lifecycle Controller data and logs, cryptographically erase SED, NVMe and PCIe devices and overwrite SAS and SATA disks [3]. It "does not clear the data from the Easy Restore flash memory", and two iDRAC features named in the guide block it until they are disabled [3].

- **DGX data drives.** `nv-disk-encrypt erase` "Sets the drives in an unlocked state. Disables locking on the drives. Removes the RAID 0 array configuration", with a caution that all data is lost [15]. A drive whose keys are lost can be reset, losing its data, with a value printed on its label [15].
- **Management controllers.** The DMTF Redfish `ResetToDefaults` action "resets the manager settings to factory defaults" [17]. "ResetAll" resets everything, while "PreserveNetworkAndUsers" keeps "network and local usernames/passwords" [17], so that type leaves a seller's accounts in place for the buyer.

3. Validation and the certificate of sanitization

Verify, then validate. Verification determines the outcome of the technique, which for logical techniques means "checking the completion status of the tools and identifying errors, anomalies, and the health of the ISM" [1]. Unless policy requires it, "elaborate sampling of an ISM's contents (e.g., full or representative) after clear or purge sanitization techniques is not necessary" [1]. Validation then decides whether "the target data was effectively sanitized" [1]. A rejection means repeating with a different technique or "escalating to a more secure sanitization method" [1]. NIST's reasons to doubt a result include parts of a device that are no longer reachable through its interface, a method that does not suit the media, uncalibrated tools and a scope "too narrowly focused", as when an overprovisioned drive is cleared with simple writes [1].

Completion evidence. The NVMe sanitize log reports 0x0001 when "The most recent sanitize operation completed successfully" and 0x0003 when it failed [21]. Its Purged bit means the operation "purged user data, as defined by IEEE Std 2883, because the Purge Required (PREQ) bit was set" [21].

One certificate per device. "Following sanitization, a certificate of sanitization (see Appendix C) should be completed for each ISM that has been sanitized, per the organization's policies", on paper or electronically [1]. Its minimum fields are the manufacturer, model, serial number, property number, media type and source, the method, technique, "Tool used, including version" and verification method, and the name, position, date, location, contact information and signature of each person who verified and validated [1]. The sample form in Appendix C records whether the media was operational or damaged and its destination: "Internal Reuse, External Reuse, Recycling Facility, Manufacturer, Other" [1]. A drive sold with its server is external reuse.

What to ask the drive maker. NIST suggests asking how a device implements its sanitize commands, whether it complies with IEEE 2883, and for "A list of any areas that are not addressed by the sanitization command" [1].

4. Health records that support resale

The records a buyer uses to judge a GPU sit on the GPU and in the server's logs.

- **Memory error counts.** nvidia-smi says "Aggregate error counts persist indefinitely and thus act as a lifetime counter", and "Clearing aggregate counts is not supported on Ampere+" [18].

- **Remapped rows.** The row remapper reports correctable and uncorrectable remapping counts, Pending and Remapping Failure Occurred fields and a bank availability histogram [18]. A row marked Pending needs a GPU reset to take effect [18]. The remap count is "the number of entries recorded in the InfoROM, not the ones remapped in hardware" [19].
- **Serial numbers.** The GPU serial "matches the serial number physically printed on each board" [18]. A board serial "might be shared between multiple GPUs on the same board", so NVIDIA recommends the UUID or PCI bus ID, and nvidia-smi also reports a chassis serial [18].
- **Logs.** For a GPU issue reported to the system vendor, NVIDIA's triage guide lists "Output of nvidia-bug-report.sh", "Fabric manager log files for HGX systems" and "DCGM Diagnostics logs" [22].

Order of work. After Dell's System Erase, "All previous information is removed" from the Lifecycle Log except the erase request and entries made as iDRAC restarts [3], and NIST advises consulting records retention offices before sanitizing [1]. Logs, counters and serial numbers therefore come off before any erase or reimage, with the management controller's event log.

5. Warranty and software terms on resale

Each maker sets its own terms [4, 5, 6].

Supermicro. "This Limited Warranty applies only to the original purchaser of the Product" [4]. GPU systems carry three years of labor, one year of parts and one year of advance cross-ship from the invoice date, absent special invoice terms [4]. Repairs by others and removed identification markings void it, third-party components are excluded, and "Supermicro shall not be liable for the loss of any Customer data" [4].

Dell. System warranties "may be transferred if the current owner transfers ownership of the system and records the transfer with us", Dell-certified memory's may not, and "All requests to transfer ownership are at Dell's sole discretion" [5]. Support applies only in the country where Dell originally sold the system [5]. SATA and SAS drives bought with Dell servers carry their own one-year warranty [5].

NVIDIA support. "Support entitlements are tied to the company and not an individual, are non-transferable, are non-assignable and may be terminated when the product is transferred to another party" [6].

Software tied to the card. NVIDIA's licensing guide, last updated 2 September 2026, says "Each NVIDIA H100 PCIe or NVL Tensor Core GPU includes a five-year NVIDIA AI Enterprise subscription" [23]. The subscription is usable only on the system in which the GPU is installed, and its start date "cannot be modified, as it is tied to the specific card" [23]. Hopper DGX systems include it in the DGX software bundle, and Blackwell DGX systems need a separate purchase [23].

What a seller records. Whose warranty applies, whether and how it moves to a buyer, when it ends, which drives carry their own term and which entitlements end at transfer [4, 5, 6, 23].

6. Testing and grading before sale

None of the standards reviewed defines condition grades for GPU servers. SERI describes R2v3's Appendix C as defining "the requirements for all electronics test and repair activities as well as the verification of the device condition and level of functionality", not required for "simple power-on or non-functional evaluations ... such as visual inspections" [24].

NVIDIA measured its DCGM diagnostic levels on Hopper systems [25].

Level	4-GPU systems	8-GPU systems	Source
r2	< 2.5 minutes	< 10.5 minutes	[25]
r3	< 10 minutes	< 35 minutes	[25]
r4	< 45 minutes	< 2.25 hours	[25]

Table 3. DCGM run levels and measured run times. Level r1 runs in under 2.5 seconds [25].

NVIDIA says DCGM diagnostics are not designed to provide comprehensive hardware diagnostics or facilitate any RMA process [25]. A test record names the level run and keeps its logs.

7. Parts that cannot be reused: certified recyclers

EPA's page, last updated 31 July 2026, says "Currently two accredited certification standards exist", R2 and e-Stewards, and both "require destruction of all data on used electronics" [7]. The ANSI-ASQ National Accreditation Board accredits the certifying bodies in the United States, and "EPA recommends using certified electronics recyclers to manage unwanted used electronics" without endorsing the entities it lists [7]. "All e-Stewards processors must destroy all residual data on equipment they receive" [26].

SERI adopted R2v3 in June 2020, and it is now approved as an American National Standard [27]. SERI describes Appendix B as covering "any logical data sanitization and an enhanced level of physical sanitization where additional tracking, verification and quality controls are required", for facilities "that perform logical data sanitization such as ITAD and mobile repair operations" [24]. It is not required for physical destruction by methods in NIST's guidelines when carried out under the standard's Core Requirement 7(c)(2)(B) [24]. Appendix C test and repair requires Appendix B, and Appendix B facilities "can provide tracking down to the serial number level" [27].

Under NIST, a drive not intended for reuse can be destroyed [1]. A drive sent to a recycler gets a certificate like any other, with the destination marked Recycling Facility [1].

8. Export obligations after the sale

This section is general information on published rules, not legal advice, and draws no license conclusion for any server, buyer or destination.

Scope and definitions. The EAR applies to "All items in the United States" and "All U.S. origin items wherever located" [10]. A transfer (in-country) is "a change in end use or end user of an item within the same foreign country" [10]. Five facts decide what applies: classification, destination, end user, end use and conduct [8].

The seller's prohibition. General Prohibition Ten says "You may not sell, transfer, export, reexport, finance" or otherwise service an item subject to the EAR with knowledge that a violation "has occurred, is about to occur, or is intended to occur" in connection with it [8]. "There are no license exceptions to this General Prohibition Ten" [8]. Knowledge includes "an awareness of a high probability of its existence or future occurrence", inferred from "conscious disregard of facts" or "willful avoidance of facts" [28].

Which entries name GPU servers. Export Control Classification Number (ECCN) 3A090.a covers chips, GPUs included, with a total processing performance (TPP) of 4,800 or more, or 1,600 or more at a performance density of 5.92 or more [29]. The 4,800 threshold "can be met with 600 tera integer operations ... at 8 bits or 300 tera FLOPS ... at 16 bits" [29]. ECCN 4A090 covers computers containing such chips, and 5A992.z covers mass market encryption commodities that meet the same parameters [29]. BIS names "servers classified as ECCN 5A992.z" among covered items [9].

License requirements, as dated texts state them. As of 5 November 2026, § 742.6(a)(6)(iii)(A) requires a license for items in 3A090.a, 4A090.a and 5A992.z.1, among others, "to or within any destination worldwide" [30]. BIS's guidance of 31 May 2026 says BIS announced in May 2025 that it would not enforce the new compliance requirements of the January 2025 rule BIS calls "the AI Diffusion Rule" [31]. It says a license requirement "continues to apply" under that paragraph to all destinations outside the United States when the items are for entities headquartered in, or whose ultimate parent is headquartered in, Country Group D:5 or Macau [31]. It adds that "Bona fide operators of data centers who are otherwise engaged in activities consistent with the EAR" need not "cease the ongoing use, storage, disposal, or servicing of advanced computing items because of this guidance, until further notice from BIS" [31].

Red flags and the duty to ask. BIS's Know Your Customer guidance "does not change or interpret the EAR" [32]. When red flags appear, "you have a duty to check out the suspicious circumstances and inquire about the end-use, end-user, or ultimate country of destination" [32]. "Do not self-blind", it says, and if doubts remain, refrain or apply for a license [32]. Its flags include declined installation or maintenance, "A freight forwarding firm is listed as the product's final destination" and a buyer evasive "about whether the purchased product is for domestic use, export or reexport" [32].

BIS's guidance of 13 May 2025 lists 11 red flags for advanced computing chips [9]. Two name "domestic or foreign" customers, and two more apply to parties "wherever located" [9]. The flags include a residential address with quantities "inconsistent with its individual/personal use", an unknown delivery or installation address, and a data center that cannot affirm the power, cooling or space to run such servers [9]. Its due

diligence steps include an end-user certification under § 748.5 and a written attestation from the data center [9]. Among the information to ask a customer, BIS lists whether the items are to be "Resold with a specification as to who the next customer is (name and address)" [9]. The Consolidated Screening List combines export screening lists of the Departments of Commerce, State and the Treasury, its tools update every day, and before acting the user must check the official publication of restricted parties in the Federal Register [33].

Paperwork when the seller exports. The exporter puts a destination control statement and the ECCNs of items such as 3A090, 4A090 and 5A992.z on the commercial invoice [34]. Records "must be retained for five years from the latest of" the export, any known reexport, transfer (in-country) or diversion, or other termination of the transaction [35].

9. A seller's checklist

Stage	Step	Sources
Before any erase	Save serials and UUIDs, ECC counts, row remapper fields, the bug report, Fabric Manager and DCGM logs and the controller's event log	[3, 18, 19, 22]
Before any erase	Check records retention duties	[1]
Inventory	List every non-volatile store from the statement of volatility, plus add-in cards	[1, 2, 14]
Decide	Purge drives that are reused. If their data has a high security categorization and they leave the organization, NIST's flow sends them to destroy. Destroy drives that are not reused	[1]
Sanitize	Use the drive's sanitize commands per IEEE 2883, purge requested where supported	[12, 20]
Reset	Reset the management controller, clear the TPM and restore BIOS defaults	[2, 15, 17]
Verify and validate	Read the completion status, then approve or reject	[1, 21]
Record	One certificate per drive, destination external reuse	[1]
Warranty and software	Record whose warranty applies and what ends at transfer	[4, 5, 6, 23]
Recycle	Send unused drives and parts to an R2 or e-Stewards recycler	[7, 26]

Stage	Step	Sources
Screen the buyer	End user, end use, installation address, resale plans, screening list	[9, 32, 33]
If exporting	Classification, destination control statement, five-year records	[29, 34, 35]

Table 4. Each step traces to the findings above.

Implications

Records first, erase second. One maker's server-wide erase removes all previous Lifecycle Log information [3]. Saving the error counters nvidia-smi reports [18] and the logs NVIDIA's triage guide lists [22] before any erase keeps the unit's history with it.

A program with records. Rev. 2 points to IEEE 2883 for techniques and asks for a certificate per device [1, 11]. A seller's records show the method, technique, tool version and who validated the result [1].

Reuse favors purge. NIST treats resale as a change of control and names reuse among the reasons to prefer purge over destroy [1]. A drive that stays in a sold server needs a method that leaves it usable, and NIST's flow gives one for low and moderate data. For high data leaving the organization, it calls for destroy [1].

Warranty is part of what is sold. Two makers and NVIDIA differ on transfer [4, 5, 6], so recording the terms tells a buyer what cover comes with the unit.

Screening attaches to the sale. BIS's red flags name domestic and foreign customers [9], and General Prohibition Ten bars selling with knowledge of a violation [8].

Resale through Rillor. Rillor resells GPU servers their owners no longer need, and tests, grades and documents each unit to the same standard before offering it. Each unit's report lists serial numbers for the system and each GPU, the configuration as received, firmware versions, the burn-in and diagnostic results, physical condition and the condition grade. Every order goes through export screening of the buyer, consignee and end user, and includes an end-use statement.

Limits of this analysis

- This is general information, not legal advice. The EAR text and BIS's enforcement guidance are dated [30, 31].
- One server's statement of volatility and NVIDIA's DGX pages were reviewed [2, 14]. Other makers state their stores differently [1].
- Warranty terms come from two makers and NVIDIA [4, 5, 6], and Supermicro's yield to special terms set in an invoice [4].
- The documents reviewed describe the InfoROM as a store of configuration and state data [18]. None of them states that GPU memory keeps user data after power-off, and this report makes no claim about it.
- R2v3 is described only through SERI's public pages [24, 27].
- Tool descriptions come from each tool's documentation, and this report rates none of them against NIST's methods.

Sources

1. Guidelines for Media Sanitization, NIST SP 800-88 Rev. 2. Ramaswamy Chandramouli and Eric Hibbard, National Institute of Standards and Technology, September 2025, viewed 8 November 2026. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf

2. Statement of Volatility, Dell PowerEdge XE9680. Dell Technologies, March 2023 (PDF modified 9 August 2023), viewed 8 November 2026. https://dl.dell.com/content/manual37172022-dell-poweredge-xe9680-statement-of-volatility.pdf?language=en-us

3. Erasing system and user data, Integrated Dell Remote Access Controller 9 (iDRAC9) User's Guide, 7.xx. Dell Technologies, viewed 8 November 2026. https://www.dell.com/support/manuals/en-us/xc7525-core/idrac9_7.xx_ug/erasing-system-and-user-data?guid=guid-169cb24b-f48d-44a4-b814-91eec4bea9fe&lang=en-us

4. Supermicro Limited Warranty. Super Micro Computer, Inc., viewed 8 November 2026. https://www.supermicro.com/en/support/warranty

5. Dell Limited Hardware Warranty. Dell Technologies, viewed 8 November 2026. https://www.dell.com/en-us/legal/lp/art-limited-hardware-warranties

6. Support Details, NVIDIA Enterprise Support and Services User Guide. NVIDIA, viewed 8 November 2026. https://docs.nvidia.com/enterprise-support-and-services-user-guide/support-details

7. Certified Electronics Recyclers. U.S. Environmental Protection Agency, last updated 31 July 2026, viewed 8 November 2026. https://www.epa.gov/smm-electronics/certified-electronics-recyclers

8. 15 CFR § 736.2, General prohibitions and determination of applicability. eCFR, Office of the Federal Register, current to 5 November 2026, viewed 8 November 2026. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-736/section-736.2

9. Industry Guidance to Prevent Diversion of Advanced Computing Integrated Circuits. Bureau of Industry and Security, U.S. Department of Commerce, 13 May 2025 (file regenerated 15 October 2026), viewed 8 November 2026. https://www.bis.gov/media/documents/ai-counter-diversion-industry-guidance-may-13-2025.pdf

10. 15 CFR part 734, Scope of the Export Administration Regulations (§§ 734.3, 734.13, 734.14, 734.16). eCFR, Office of the Federal Register, current to 5 November 2026, viewed 8 November 2026. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734

11. Frequently Asked Questions for NIST SP 800-88r2, Guidelines for Media Sanitization. National Institute of Standards and Technology, 16 July 2026, viewed 8 November 2026. https://csrc.nist.gov/files/pubs/sp/800/88/r2/final/docs/sp800-88r2-faq.pdf

12. IEEE 2883-2022, IEEE Standard for Sanitizing Storage. IEEE Standards Association, published 17 August 2022, viewed 8 November 2026. https://standards.ieee.org/ieee/2883/10277/

13. IEEE 2883.1-2025, IEEE Recommended Practice for Use of Storage Sanitization Methods. IEEE Standards Association,

published 19 June 2025, viewed 8 November 2026. https://standards.ieee.org/ieee/2883.1/11015/

14. Introduction to NVIDIA DGX H100/H200 Systems, NVIDIA DGX H100/H200 User Guide. NVIDIA, last updated 17 October 2026, viewed 8 November 2026. https://docs.nvidia.com/dgx/dgxh100-user-guide/introduction-to-dgxh100.html

15. Managing Self-Encrypting Drives, NVIDIA DGX OS 7 User Guide. NVIDIA, last updated 27 October 2026, viewed 8 November 2026. https://docs.nvidia.com/dgx/dgx-os-7-user-guide/managing-seds.html

16. CISA and NSA Release Joint Guidance on Hardening Baseboard Management Controllers (BMCs). Cybersecurity and Infrastructure Security Agency, 14 June 2023, viewed 8 November 2026. https://www.cisa.gov/news-events/alerts/2023/06/14/cisa-and-nsa-release-joint-guidance-hardening-baseboard-management-controllers-bmcs

17. Manager schema, version 1.25.0 (Redfish release 2026.1). DMTF, viewed 8 November 2026. https://redfish.dmtf.org/schemas/v1/Manager.v1_25_0.json

18. NVIDIA System Management Interface (nvidia-smi) documentation. NVIDIA, viewed 8 November 2026. https://docs.nvidia.com/deploy/nvidia-smi/index.html

19. User Visible Statistics, NVIDIA GPU Memory Error Management. NVIDIA, last updated 4 November 2026, viewed 8 November 2026. https://docs.nvidia.com/deploy/a100-gpu-mem-error-mgmt/user-visible-statistics.html

20. nvme-sanitize(1), nvme-cli documentation. linux-nvme project, viewed 8 November 2026. https://raw.githubusercontent.com/linux-nvme/nvme-cli/master/Documentation/nvme-sanitize.txt

21. nvme-log-sanitize(1), nvme-cli documentation. linux-nvme project, viewed 8 November 2026. https://raw.githubusercontent.com/linux-nvme/nvme-cli/master/Documentation/nvme-log-sanitize.txt

22. GPU Node Triage, NVIDIA GPU Debug Guidelines. NVIDIA, last updated 4 November 2026, viewed 8 November 2026. https://docs.nvidia.com/deploy/gpu-debug-guidelines/gpu-node-triage.html

23. NVIDIA AI Enterprise Licensing, NVIDIA Enterprise Licensing Guide. NVIDIA, last updated 2 September 2026, viewed 8 November 2026. https://docs.nvidia.com/ai-enterprise/planning-resource/licensing-guide/latest/licensing.html

24. R2v3 Appendix Applicability Guidance. Sustainable Electronics Recycling International (SERI), last updated 11 September 2024, viewed 8 November 2026. https://sustainableelectronics.org/knowledge-base/r2v3-appendix-applicability-guidance/

25. DCGM Diagnostics, NVIDIA DCGM User Guide. NVIDIA, last updated 17 June 2026, viewed 8 November 2026. https://docs.nvidia.com/datacenter/dcgm/latest/user-guide/dcgm-diagnostics.html

26. e-Stewards. Basel Action Network, viewed 8 November 2026. https://e-stewards.org/

27. R2 Standard. Sustainable Electronics Recycling International (SERI), viewed 8 November 2026. https://sustainableelectronics.org/r2-standard/

28. 15 CFR § 772.1, Definitions of terms as used in the Export Administration Regulations ("Knowledge"). eCFR, Office of the Federal Register, current to 5 November 2026, viewed 8 November 2026. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-772/section-772.1

29. Supplement No. 1 to Part 774, The Commerce Control List (ECCNs 3A090, 4A090, 5A992). eCFR, Office of the Federal Register, current to 5 November 2026, viewed 8 November 2026. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-774/appendix-Supplement%20No.%201%20to%20Part%20774

30. 15 CFR § 742.6, Regional stability. eCFR, Office of the Federal Register, current to 5 November 2026, viewed 8 November 2026. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-742/section-742.6

31. Guidance Regarding Enforcement of License Requirements for Advanced Computing Items for Entities Headquartered in Country Group D:5 and Macau. Bureau of Industry and Security, U.S. Department of Commerce, 31 May 2026, viewed 8 November 2026. https://www.bis.gov/media/documents/bis-guidance-may-31-2026.pdf

32. Supplement No. 3 to Part 732, BIS's "Know Your Customer" Guidance and Red Flags. eCFR, Office of the Federal Register, current to 5 November 2026, viewed 8 November 2026. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-732/appendix-Supplement%20No.%203%20to%20Part%20732

33. Consolidated Screening List. International Trade Administration, U.S. Department of Commerce, viewed 8 November 2026. https://www.trade.gov/consolidated-screening-list

34. 15 CFR § 758.6, Destination control statement and other information furnished to consignees. eCFR, Office of the Federal Register, current to 5 November 2026, viewed 8 November 2026. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-758/section-758.6

35. 15 CFR part 762, Recordkeeping (§§ 762.1, 762.6). eCFR, Office of the Federal Register, current to 5 November 2026, viewed 8 November 2026. https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-762

36. PowerEdge XE9680 Specification Sheet. Dell Technologies, April 2025, viewed 8 November 2026. https://www.delltechnologies.com/asset/en-us/products/servers/technical-support/poweredge-xe9680-spec-sheet.pdf

About this report

Published by Rillor on 12 November 2026. Superintelligence (SI) tools assist research and drafting, and every figure cites its source. Rillor builds and secures SI systems, supplies the data they learn from and delivers the infrastructure they run on. We apply SI to financial and compute markets.

Cite as: Rillor. What to do before selling surplus GPU servers. 12 November 2026. https://rillor.com/insights/selling-surplus-gpu-servers

Notices

Rillor is not a registered investment adviser or commodity trading advisor and does not provide investment or trading advice. Research, forecasts, data and software described on this site are for research and engineering use. Nothing here is an offer or recommendation to buy or sell any security, commodity interest or digital asset. Past or simulated results do not indicate future results.

NVIDIA, AMD, Ceph, Kubernetes and related product names are trademarks of their owners and are used only to identify products. No affiliation or endorsement is implied.

Work with Rillor

Send the workload, system, quantity, delivery window and destination. Contact us at rillor.com/contact?type=gpu-systems or contact@rillor.com. More on GPU systems: rillor.com/compute/gpu-systems