The R2 Standard Consensus Body has approved this Formal Interpretation in line with Article 10 – Interpretations Policy in the SERI Manual of Policies and Procedures for R2 Standard Development and the ANSI Standards Development process. This Formal Interpretation is hereby published by SERI and effective on November 29, 2022.

QUESTION

Logical Sanitization in Appendix B references the use of "software" in requirements (10) and (11). Is "software" limited to applications that automate the logical sanitization process and create a record of the sanitization?

FORMAL INTERPRETATION

"Software" is intended to mean applications that automate, control, and record results of data sanitization for each unique identifier. Because performing manufacturer-provided factory resets directly on a device do not always make data irrecoverable by commercial software, sanitization by software methods must be the primary method of logical sanitization. However, on some devices, manufacturer-provided factory resets may be the only available option (when a device is functional and not damaged). For a specific device containing data, when no software exists that fully automates, controls, and records the data sanitization results, "software" can extend to include the application that is directing, controlling, and recording the manual workflow to sanitize the data according to the manufacturer provided instructions ("manufacturer reset"). The software facilitating the manufacturer-prescribed data sanitization process and recording its results shall be demonstrated to fulfill the data sanitization software requirements in Appendix B(11) and the records requirements in Appendix B(10).

"Commercial software" in Appendix B(13) refers to the level of data recovery techniques applied to the sampling method. Commercial software is a level between basic visual inspection for data and forensic laboratory analysis. It means a level where data could not be recovered by software designed for data recovery that a normal user could download or purchase and use to recover data from a device.

LIMITATIONS

This formal interpretation does not apply to situations where there is software, but the device is damaged and cannot be connected to a remote computer to be sanitized by software. One example is an Android phone with a damaged IO port. It is widely known that there is software that can automate and control the sanitization process of these devices from a remote computer. In these cases, to be categorized as "non-data" devices according to the R2 Equipment Categorization because it was sanitized with software, the IO port would need to be repaired first to be connected and sanitized with the available software. Otherwise, a manual reset would not meet the requirement even if it was directed, controlled, and recorded by a software application. The choice to not repair cannot be a reason to not use software to automate the sanitization process where it is available.

BACKGROUND

This request for formal interpretation of "software" in Appendix B was made by SERI after learning of challenges throughout the industry in implementing the requirement.

DISCUSSION

See Guidance – A Discussion on Logical Data Sanitization in R2v3

APPLICATION

Some common data containing devices that may not have sanitization and commercial recovery software include, but is not limited to:

- Smart Speakers
- Smart TVs
- Smart Watches
- Fitness Trackers
- Gaming Consoles w/ built in memory chips as opposed to hard drives
- TV Sticks/Boxes
- Desk phones
- Printers w/ built in memory chips as opposed to hard drives
- Smart Thermostats
- IP-connected home security devices
- Mobile Routers/MiFi/Hotspots
- Mobile Feature Phones
- Switches
- Chromebooks

The R2 Certified facility is responsible for the "data" on any devices in their possession. Step 1 is to determine if data could be stored on the device. Does the device have non-volatile storage capabilities?

The second point of distinction is whether a device contains "Data" that requires sanitization or only "General Information" that does not require sanitization.

The R2 Standard defines data as:

> "Data" is the private, personally identifiable, confidential, licensed or proprietary information contained on an electronic device or memory component that requires secured management and sanitization under this standard. Data does not include General Information as defined in the R2 Standard

The Standard also defines General Information as follows:

> "General information" is publicly available information or information that is provided with the original electronic equipment from the manufacturer. General information does not require sanitization.

The third consideration is whether the device actually stores the data locally, or stores the data remotely on a PC, server, Cloud etc. Linked data is not stored on the device, so the device would not require data sanitization. However, it is critical in these cases, that the connection to the remote storage would need to be removed under Appendix B (12).

The final consideration is whether software exists to automate the data sanitization process. This is not a choice of whether to use the software or not. If a software exists, then a software solution must be implemented.

If no software is available to automate the sanitization process, then the manufacturer instructions may be incorporated into a software platform to control the workflow to implement the manufacturer

instructions and create detailed records of completion for each device. Implementation of manufacturer reset instructions is sometimes found in commercial software (off-the shelf software) that can be purchased. This software has been found to incorporate these instructions for devices in which the software cannot automate the process. The software becomes a hybrid approach to logical sanitization by organizing and controlling all logical sanitization functions on the same platform. Purchased software for data sanitization is not necessarily required for purposes of this Interpretation. The integration of workflow steps could be accomplished through the facility's ERP system or another platform, creating a custom software solution.

AUDITING

Automated software solutions that do not rely on manual resets is the intention of this requirement and should be required when software is available. When automated software solutions are not available, a robust software system to control the workflow of the process is expected with detailed records of sanitization to provide transparency and accountability about the data sanitization event on each device.

This interpretation does not allow for broken devices to use manual manufacturer reset instructions when automated software sanitization is possible.

Evaluating Records required in Appendix B(10)

Simple operator created records on a spreadsheet, for example, are not considered acceptable records of software sanitization as these are more vulnerable to errors and suspect results. The following are recommended data points for data sanitization records modeled after NIST SP 800-88 Rev.1 Section 4.8:

- Device/Media Manufacturer
- Device/Media Model
- Device/Media Serial Number (preferably read by the software and not manually entered)
- Unique Identifier assigned (preferably scanned from a label)
- Media Type (i.e., magnetic, flash memory, hybrid, etc.)
- Media Source (i.e., user or computer the media came from)
- Device/Media Capacity (i.e., number and size of LBA's)
- Sanitization Type (Clear, Purge, Destroy)
- Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.)
- Tool Used (including version)
- Sanitization Person
    - Name of Person
    - Position/Title of Person
    - Date/Time (automatically recorded from the system)
    - Location
    - Phone or Other Contact Information
    - Signature
- Verification Method (i.e., verified successful sanitization record, sampling, etc.)
- Verification Person
    - Name of Person
    - Position/Title of Person
    - Date/Time (automatically recorded from the system)
    - Location

- Phone or Other Contact Information
- Signature

Evaluating the software that integrates manual manufacturer reset instructions required in Appendix B(11)

First, the manufacturer's reset instructions should be evaluated to verify that the instructions deem the data inaccessible, not that it just resets the configuration of the device. This is an important distinction in meeting Appendix B (11)(a).

Second, the workflow should be configured to fail the process if there is any disruption during the sanitization process or any failures related to an ineffective clear, to meet Appendix B (11)(b).

Third, "maintained with software patches" would be fulfilled by updating the instructions in the software with any manufacturer changes. Written documentation of an automated process or a manual schedule to check for updates and a record of updates to the instructions could be a method to present evidence that meets Appendix B (11)(c).

Verifying the current supported version in utilizing the manufacturer's reset instruction means ensuring that the most current instructions are implemented. This requires a process to routinely check the manufacturer's website or other sources for updates. The version or date of the instructions used should be recorded in the sanitization record of each device. Should there ever be a glitch found in the manufacturer's instructions, having this in the record allows the facility to identify those devices that would be vulnerable and need correction.