From:	"[redacted]" via 800-171comments
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] Comment: Information in Shared System Resources (03.13.04)
Date:	Friday, December 8, 2023 1:12:59 PM
Attachments:	SP 800-171 Comment - Information in Shared System Resources (03.13.04).pdf

---

Thank you for the opportunity to send comments on NIST SP 800-171 Rev. 3! I apologize for sending a PDF, but I was unable to fit and format the sole topic in the Excel format.

The attached document provides commentary on the control *Information in Shared System Resources (03.13.04)*, referred to as SC-4 in NIST SP 800-53. Based on a review of prior NIST SP 800-53 revisions and earlier security criteria that SP 800-53 (and hence SP 800-171) were initially derived from, there appears to be a scope conflict within the control's discussion (i.e., supplemental guidance) statement.

Thank you again and for all you all do!

NIST SP 800-171 Comment: Analysis of 03.13.04 (Information in Shared System Resources)

This document provides a historical review and analysis of the NIST SP 800-53 security control **SC-4**, *Information in Shared System Resources*, also referred to as **03.13.04** in NIST SP 800-171. While this document has been sent in response to the NIST SP 800-171 Rev. 3 Final Public Draft, it equally applies to NIST SP 800-53. For consistency, "SC-4" will be used to reference the underlying security control.

This document argues that, as currently written, SC-4 is self-contradictory and cannot be implemented. Specifically, it is argued that due to terminology changes and supplemental guidance modifications, SC-4 has inadvertently excluded itself from being implemented by the inclusion of a caveat in its guidance.

1 WHAT WAS SC-4 ORIGINALLY ABOUT?

The original version of SC-4 (currently titled *Information in Shared System Resources*) was created nearly two decades ago in the original NIST SP 800-53 (2005). At that time, SC-4 was instead titled *Information Remnants*, and the control's text — substantively unchanged to this day — read as follows:

> *The information system prevents unauthorized and unintended information transfer via shared system resources.*

Readers wanting context for SC-4 would then read its original supplemental guidance, which stated:

> *Control of information system remnants, sometimes referred to as object reuse, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.*

After reading both the control and its supplemental guidance, it would be clear to the reader that SC-4 was about **object reuse** — a now somewhat-dated term addressing the concern of residual data being available reused or reallocated storage media (e.g., hard drives and memory). At the time, the security concerns underlying object reuse was often referred to as **data remanence**, with the terms often being used interchangeably.[1] In fact, SC-4's original name, *Information Remnants*, is itself a synonym for "data remanence."[2]

The primary protection against object reuse concerns was to "zero-out" data on storage devices — to comprehensively overwrite data on a storage medium. For example, if John, a new NIST employee, used a computer after Marcy, another NIST employee, then John could be able to access the Marcy's data in

[1] For example, see: National Computer Security Center – A Guide to Understanding Data Remanence in Automated Information Systems (September 1991) (used throughout) and NIST SP 800-33, Underlying Technical Models for Information Technology Security ("Some examples of system protections are: residual information protection (also known as object reuse)").

[2] The author could find no instances in which the term "information remnants," or its other spellings, were used prior to the original NIST SP 800-53. (See, e.g., Google Ngram Viewer.) Presumably, SC-4 was called "information remnance" rather than "data remnance" to standardize terminology.

the working memory unless it is cleared. To a lesser extent, object reuse concerns also addressed what is now termed "media sanitization"; however, the primary focus was on actively used/shared devices.

2 WHERE DID NIST GET THE IDEA FOR SC-4?

One might wonder: what prompted NIST to create a control for object reuse at all? The proximate answer lies in a Department of Defense (DoD) security standard initially created in 1983, titled the DoD Trusted Computer System Evaluation Criteria ("DoD Criteria"). The DoD Criteria, often called the "Orange Book," contained the following requirement for object reuse security in its 1985 edition:

> 3.3.1.2 Object Reuse
>
> All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subjects actions is to be available to any subject that obtains access to an object that has been released back to the system.

How does the above text from 1985 relate to SC-4 in 2005? The answer is that the former prompted the creation of the latter: namely, the original supplemental guidance for SC-4 was based directly off the DoD Criteria's requirement on object reuse. This can be seen by performing a simple comparison, as below, of SC-4's original supplemental guidance with the DoD Criteria text pictured above:

> ~~All authorizations to the~~ Control of information ~~contained within a storage~~system remnants, sometimes referred to as object ~~shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No~~reuse, prevents information, including encrypted representations of information, produced by ~~a prior subjects~~the actions ~~is to be~~of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any ~~subject~~current user/role (or current process) that obtains access to ~~an object~~a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

It is clear from this comparison that the roots of SC-4 are found in the DoD Criteria.[3]

The connection between the original SC-4 and the DoD Criteria, as well as the earlier discussion on the history of object reuse, allows to tentatively make three conclusions: (1) SC-4 was intended to be about object reuse; (2) SC-4's original name, *Information Remnants*, was used as a synonym for object reuse; and (3) data remanence, object reuse, and information remnants are all terms used to identify the same security concern of remnant data making its way from one user to another.

[3] Specifically, both: (1) follow the same structure, (2) contain the statement "information, including encrypted representations of information," and conclude with the similar "has been released back to the [information] system."

3 When did the issue with SC-4 begin?

From the original NIST SP 800-53 to its first and second revisions, SC-4 was essentially unchanged and was clearly about object reuse.[4] However, this changed in 2009 with NIST SP 800-53 Rev. 3, which is when the issue this document focuses on first arose.

NIST SP 800-53 Rev. 3 changed SC-4 in an important way, but not by changing the text of the control itself. Rather, the change to SC-4 came from a modification to its supplemental guidance. Below, we provide a red-line comparison of SC-4's "Rev. 3" guidance to its "Rev. 2" counterpart:

> ~~Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents~~The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.

Reviewing the changes to SC-4's guidance, we first see that its initial sentence was slightly reworded but otherwise not significantly changed. Next, we see that a second sentence has been added to the guidance, stating: "Control of information in shared resources is also referred to as object reuse." Neither change here significantly affects SC-4, but it's notable that the term "object reuse" is used.

It is the final change to SC-4's guidance where the issue arises. This new sentence, which caveats the scope of SC-4, states the following:

> *[SC-4] does not address:*
>
> *i. Information remanence, which refers to residual representation of data that has been in some way nominally erased or removed;*
> *ii. Covert channels, where shared resources are manipulated to achieve a violation of information flow restrictions; or*
> *iii. Components in the information system for which there is only a single user or role.*

Here, we see the issue: SC-4 simultaneously claims to be about object reuse and *not* be about information remanence. However, as discussed above, both terms refer to the same underlying concept and address the same security requirement. Information remanence *is* object reuse. Therefore, SC-4's supplemental guidance nullifies the control it was written for.[5]

---

[4] In the first revision of NIST SP 800-53, the supplemental guidance for SC-4 was even updated to state: "Control of information system remnance, sometimes referred to as object reuse, or data remnance . . ."

[5] It's notable the revised guidance also excludes covert channels, a topic addressed nearby in the DoD Criteria. Presumably, the exclusion of covert channels is to avoid conflict with the NIST SP 800-53 control AC-4, *Information Flow Enforcement*, though a type of covert channel (storage channels) does fit within the context of SC-4.

With only slight editorial changes,[6,7] this issue with SC-4 remains in NIST SP 800-53 Rev. 5 and NIST SP 800-171 Rev. 3.

4 CONCLUSION

While the author does not know the best way to address this issue, the following is recommended for consideration:

1. Despite the issue above, the original and primary intent of SC-4 remains the issue of object reuse, information/data remanence, or, as most recently called in the Common Criteria, the spiritual successor to the DoD Criteria, residual information protection. If NIST determines that this should remain the primary concern for SC-4, then the control should be updated to state as such.
2. However, it's also worth observing that object reuse has become a much more niche topic since the 1980s. The only modern, publicly available source of security requirements addressing object reuse appears to be the above-reference Common Criteria itself.
3. Security regarding object reuse is itself a highly niche and hard-to-assess topic. In terms of the standard NIST control assessment regime, the only way one could meaningfully verify a system component implements object reuse security would be to verify that the component has been analyzed under the Common Criteria requirements. It would also be unclear as to what the scope of object reuse security would be (i.e., "to which media/devices/storage is it required for?").
4. The majority of the concerns regarding SC-4 (in its broadest reading) are already addressed in other security controls, such as AC-4, CM-6 and MP-6.
5. Finally, the appendix at the end of this document provides a comparison of controls from alternative security standards related to SC-4 as was listed in the original NIST SP 800-53.

[6] In what is generally considered to be the replacement of the DoD Criteria, the international Common Criteria standard, the term "object reuse" was renamed "residual information protection."

[7] The latest guidance/discussion for SC-4 additionally caveats itself by saying "in other contexts, control of information in shared system resources is referred to as object reuse and residual information protection," but the contextual distinction, if any, is unclear.

Appendix A: Related Controls in Alternative Security Standards

The original NIST SP 800-53 contains a mapping of the then-new NIST security controls with other standards that existed at the time. The table below lists each alternative-standard control relationship with SC-4 and provides insight as to the initial construction of SC-4.

Standard	Identifier	Control Text
ISO 17799:2005[8]	10.8.1	**Information Exchange Policies and Procedures.** Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communications facilities.
GAO FISCAM (2003)	AC-3.4	**Sanitation of equipment and media prior to disposal or reuse.** Procedures are implemented to clear sensitive data and software from discarded and transferred equipment and media.
DoD 8500.2	ECRC-1	**Resource Control.** All authorizations to the information contained within an object are revoked prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system. There is absolutely no residual data from the former object.
DCID 6/3 Manual (2002)	4.B.2.a(13)	

[8] The author was unable to obtain a primary copy of this document. Instead, the control text listed comes from a secondary source, which may not be identical.