LEGAL NOTICE:

LEGAL DISCLAIMER:

THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "**AS IS**" BASIS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NVM EXPRESS, INC. (ALONG WITH THE CONTRIBUTORS TO THIS DOCUMENT) HEREBY DISCLAIM ALL REPRESENTATIONS, WARRANTIES AND/OR COVENANTS, EITHER EXPRESS OR IMPLIED, STATUTORY OR AT COMMON LAW, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, VALIDITY, AND/OR NONINFRINGEMENT.

All product names, trademarks, registered trademarks, and/or servicemarks may be claimed as the property of their respective owners.

VTM Group (Beaverton, OR):
NVM Express Workgroup
c/o VTM Group
3855 SW 153rd Drive
Beaverton, OR 97003 USA
info@nvmexpress.org

NVM Express Technical Proposal for New Feature

Technical Proposal ID	**4022 – Sanitize with DST**
Change Date	**3/04/2018**
Builds on Specification	**NVM Express 1.3a**

Technical Proposal Author(s)

Name	Company
Yoni Shternhell	WDC

This technical proposal suggests adding clear text to the spec to abort the DST operation in progress, when new sanitize operation starts.

Revision History

Revision Date	Change Description
1/10/2018	Initial proposal
02/01/2018	- Make the TP to request changes regarding DST operations only (and not operations in progress) - Refer to sanitize operation that started and not to sanitize command
02/22/2018	- Phase 3 discussion
02/26/2018	- Some editorial modifications
08/20/2018	Ratified

Description of Specification Changes

Modify a portion of section 5.24 (Sanitize command – NVM Command Set Specific) as shown below:

5.24 Sanitize command – NVM Command Set Specific

The Sanitize command is used to start a sanitize operation or to recover from a previously failed sanitize operation. The sanitize operation types that may be supported are Block Erase, Crypto Erase, and Overwrite. All sanitize operations are processed in the background (i.e., completion of the Sanitize command does not indicate completion of the sanitize operation). Refer to section 8.15 for details on the sanitize operation.

When a sanitize operation starts on any controller, all controllers in the NVM subsystem:

- Shall clear any outstanding Sanitize Operation Completed asynchronous event;
- Shall update the Sanitize Status log (refer to section 5.14.1.9.2);
- Shall abort any command (submitted or in progress) not allowed during a sanitize operation with a status of Sanitize In Progress (refer to section 8.15.1);
- Shall abort device self-test operations in progress;
- Should suspend power management activities; and
- Shall release stream identifiers for any open streams.

Modify a portion of section 8.11.1 (Short Device Self-Test Operation) as shown below:

8.11.1 Short Device Self-Test Operation

A short device self-test operation should complete in two minutes or less. The percentage complete of the short device self-test operation is indicated in the Current Percentage Complete field in the Device Self-test Log (refer to section 5.14.1.6).

A short device self-test operation:

a) shall be aborted by any Controller Level Reset;

b) shall be aborted by a Format NVM, if the Namespace Identifier field specified in the Format NVM command is the same as the Device Self-test command that invoked the device self-test operation;

c) shall be aborted when a sanitize operation is started (refer to section 5.24);

d) shall be aborted if a Device Self-test command with the Self-Test Code field set to Fh is processed; and

e) may be aborted if the specified namespace is removed from the namespace inventory.

Modify a portion of section 8.11.2 (Extended Device Self-Test Operation) as shown below:

8.11.2 Extended Device Self-Test Operation

An extended device self-test operation should complete in the time indicated in the Extended Device Self-test Time field in the Identify Controller data structure or less. The percentage complete of the extended device self-test operation is indicated in the Current Percentage Complete field in the Device Self-test Log (refer to section 5.14.1.6).

An extended device self-test operation shall persist across any Controller Level Reset, and shall resume after completion of the reset or any restoration of power, if any. The segment where the extended device self-test operation resumes is vendor specific, but implementations should only have to perform tests again within the last segment that was being tested prior to the reset.

An extended device self-test operation:

a) shall be aborted by a Format NVM, if the Namespace Identifier field specified in the Format NVM command is the same as Device Self-test command the invoked the device self-test operation;
b) shall be aborted when a sanitize operation is started (refer to section 5.24);
c) shall be aborted if a Device Self-test command with the Self-Test Code field set to Fh is processed; and
d) may be aborted if the specified namespace is removed from the namespace inventory.

Modify a portion of Figure 99 (Get Log Page - Self-test Result Data Structure) as shown below:

<table>
<tr><th>Bytes</th><th>Description</th></tr>
<tr><td>0</td><td>Device Self-test Status: This field indicates the device self-test code and the status of the operation.

Bits 7:4 indicates the Self-test Code value that was specified in the Device Self-test command that started the device self-test operation that this Self-test Result Data Structure describes.

<table>
<tr><th>Value</th><th>Definition</th></tr>
<tr><td>0h</td><td>Reserved</td></tr>
<tr><td>1h</td><td>Short device self-test operation</td></tr>
<tr><td>2h</td><td>Extended device self-test operation</td></tr>
<tr><td>3h – Dh</td><td>Reserved</td></tr>
<tr><td>Eh</td><td>Vendor specific</td></tr>
<tr><td>Fh</td><td>Reserved</td></tr>
</table>

Bits 3:0 indicates the result of the device self-test operation that this Self-test Result Data Structure describes.

<table>
<tr><th>Value</th><th>Definition</th></tr>
<tr><td>0h</td><td>Operation completed without error</td></tr>
<tr><td>1h</td><td>Operation was aborted by a Device Self-test command</td></tr>
<tr><td>2h</td><td>Operation was aborted by a Controller Level Reset</td></tr>
<tr><td>3h</td><td>Operation was aborted due to a removal of a namespace from the namespace inventory</td></tr>
<tr><td>4h</td><td>Operation was aborted due to the processing of a Format NVM command</td></tr>
<tr><td>5h</td><td>A fatal error or unknown test error occurred while the controller was executing the device self-test operation and the operation did not complete</td></tr>
<tr><td>6h</td><td>Operation completed with a segment that failed and the segment that failed is not known</td></tr>
<tr><td>7h</td><td>Operation completed with one or more failed segments and the first segment that failed is indicated in the Segment Number field</td></tr>
<tr><td>8h</td><td>Operation was aborted for unknown reason</td></tr>
<tr><td>9h</td><td>Operation was aborted due to a sanitize operation</td></tr>
<tr><td>Ah – Eh</td><td>Reserved</td></tr>
<tr><td>Fh</td><td>Entry not used (does not contain a test result)</td></tr>
</table>
</td></tr>
<tr><td>1</td><td>Segment Number: This field indicates which segment the first self-test failure occurred. The field is ignored if the Device Self-test Status field is not set to 7h.</td></tr>
<tr><td>2</td><td>Valid Diagnostic Information: This field indicates the diagnostic failure information that is reported.</td></tr>
</table>

	Bits 7:4 are reserved. Bit 3 defines the SC_Valid bit. If set to '1', then the contents of Status Code field is valid. If cleared to '0', then the contents of Status Code field is invalid. Bit 2 defines the SCT_Valid bit. If set to '1', then the contents of Status Code Type field is valid. If cleared to '0', then the contents of Status Code Type field is invalid. Bit 1 defines the FLBA_Valid bit. If set to '1', then the contents of Failing LBA field is valid. If cleared to '0', then the contents of Failing LBA field is invalid. Bit 0 defines the NSID_Valid bit. If set to '1', then the contents of Namespace Identifier field is valid. If cleared to '0', then the contents of Namespace Identifier field is invalid.
3	Reserved
11:4	**Power On Hours (POH):** This field indicates the number of power-on hours at the time the device self-test operation was completed or aborted. This does not include time that the controller was powered and in a low power state condition.
15:12	**Namespace Identifier (NSID):** This field indicates the namespace that the Failing LBA occurred on. The contents of this field are valid only when the NSID_Valid bit is set to '1'.
23:16	**Failing LBA:** This field indicates the LBA of the logical block that caused the test to fail. If the device encountered more than one failed logical block during the test, then this field only indicates one of those failed logical blocks. The contents of this field are valid only when the FLBA_Valid bit is set to '1'.
24	**Status Code Type:** This field may contain additional information related to errors or conditions. Bits 7:3 are reserved. Bits 2:0 may contain additional information relating to errors or conditions that occurred during the device self-test operation represented in the same format used in the Status Code Type field of the Completion Queue Entry (refer to section 4.6.1.1) The contents of this field are valid only when the SCT_Valid bit is set to '1'.
25	**Status Code:** This field may contain additional information relating to errors or conditions that occurred during the device self-test operation represented in the same format used in the Status Code field of the Completion Queue Entry (refer to section 4.6.1.2) The contents of this field are valid only when the SC_Valid bit is set to '1'.
27:26	Vendor Specific