SWGDE Recommended Guidelines for Validation Testing

Disclaimer:

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:

Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

SWGDE Recommended Guidelines for Validation Testing

Table of Contents

1. Introduction

Validation testing is critical to the outcome of the entire examination process. Validation, based on sound scientific principles, is required to demonstrate that examination tools (hardware and software), techniques and procedures are suitable for their intended purpose. Tools, techniques and procedures should be validated prior to initial use in digital forensic processes. Failure to implement a validation program can have detrimental effects.

2. Target Audience

All organizations performing digital forensic examinations.

3. Definition of Validation Testing

An evaluation to determine if a tool, technique or procedure functions correctly and as intended.

4. Scope of Testing

Validation testing should be applied to all tools, techniques and procedures utilized in the performance of digital forensics.

Mobile devices present special challenges for the validation of tools, techniques, and procedures. These challenges include: rapid development cycles, undocumented operating and file systems, the overwhelming diversity of devices, firmware revisions, and the need for narrowly specialized tools and methods. These challenges will persist as emerging technologies evolve and consideration should be given when determining which subsets of a tool's functionality should be validated. It is not practical to test every combination of tool version and device type. It is best practice, at a minimum, to test those subsets of a tool's functionality that are relevant to its expected use. However, a confirmation of the result received may be sufficient.

Tools, techniques, and procedures, which by virtue of their widespread use, duration of use, and acceptability by the larger information technology community, are generally acknowledged as reliable and trustworthy. Consideration may be given to the general acceptance of a tool, technique, or procedure in the determination of whether validation is required.

5. When

Validation testing should be performed whenever new, revised, or reconfigured tools, techniques or procedures are introduced into the forensic process. While media and operating systems are not generally considered tools for the purposes of this document, these may exhibit characteristics that might not remain consistent when used with different tools, techniques, and procedures. These situations may require additional testing. Editorial changes or changes made for clarification purposes only will not require revalidation.

6. Why

To ensure the integrity of the components utilized in the forensic process.

7. Process

1. Develop and document test plan before testing begins. The test plan should contain the following:

   a. Purpose and scope

   b. Requirements to be tested – what does the tool have to do?

   c. Methodology – how to test? (Identify support tools required to assist in evaluation of results when applicable)

   d. Test scenarios

   - Condition or environment required for test scenario

   - Actions to perform during utilization of the tool, technique or procedure

   - Expected results -determine pass/fail criteria

   - One test may be sufficient depending on the tool, technique or procedure being tested. The number of test scenarios should be sufficient to cover the various environments encountered – for example, different file systems, media sizes, platforms, device types, etc.

   - Different options may need to be tested such as user configurable option settings, switch settings, etc., in accordance with purpose and scope

   e. Test data to fulfill conditions of test scenarios – can the existing reference data set be used? (Identify support tools required to assist in the development of test data when applicable)

   f. Document test data used

   > **Note:** Be sure each requirement is assigned to at least one test scenario.

2. Perform test scenario(s) and document results in test report

   a. Use media and/or other sample materials that are in a known state or condition

   b. Use test equipment with known configuration which corresponds to your examination environment

   c. If anomaly occurs then:

- Attempt to identify conditions causing anomaly

- Attempt to independently verify conditions causing anomaly

- If feasible, implement alternative procedure and re-test

d. If re-tests are performed, results of <u>all</u> tests must be documented

e. Be sure pass/fail status for each requirement is annotated in test report

f. Ensure to annotate all testers and dates assigned to test scenario

g. Individual test scenario(s) must be documented separately, but a summary report should be written which states the overall pass/fail status of the tool, technique or procedure, along with any recommendations, concerns, etc.

h. Validation of results: comparison between actual and expected results must be performed and discrepancies between the two must be documented

8. Test Plan Template

The validation testing process shall be documented in detail to enable independent replication and shall be written before testing begins. There is no standard format or title for this document, but a typical format might include:

1. Purpose and scope

2. Requirements: what does the tool have to do?

3. Description of methodology: how to test?

4. Expected results: global view of pass/fail

5. Test Scenarios for each:

   a. Conditions: test environment (hardware/software configurations, etc.)

   b. Actions: specific actions

   c. Assigned requirements

   d. Expected results: specific pass/fail

6. Description of test data

9. Test Scenario Report Template

Individual test scenario(s) must be documented and a summary report should be written which states the overall pass/fail status of the tool, technique or procedure along with any recommendations, concerns, etc.

There is no standard format or title for a Test Scenario Report, but a typical format might include:

1. Test number/identification: Each test should have a unique identifier for referral, indexing, etc.

2. Test title

3. Test date

4. Test person

5. Test designer/reviewer when applicable: Test reviewer should be independent of the designer and the tester

6. Test description

7. Test result (overall pass/fail result)

8. Configuration of test platform: Document both hardware and software configurations as well as any preference or option settings when test is performed

9. Tool being tested

    a. Title

    b. Manufacturer

    c. Version or date

10. Notes regarding test data set

11. Test notes

    a. Notes of tool or test being performed

12. Procedures

    a. Procedures should be written granular enough to allow exact replication by independent party

b. Document options or switches used if applicable

13. Observations

14. Results

    a. Expected results

    b. Actual results

15. Validation results – comparison between actual and expected results must be performed and discrepancies between the two must be documented

The Summary Report should state the overall pass/fail status of the tool, technique or procedure along with any recommendations, concerns, etc. There is no standard format or title for this report, but a typical format might include:

1. Test report title and number/identification

2. Test date

3. Test description

4. Title, manufacturer and version/date of tool, technique or procedure tested

5. Test result (overall pass/fail result)

    a. List each requirement and its result

6. Observations, concerns, limitations

7. Recommendations (optional)

> **Note regarding included samples:** The attached samples are in an abbreviated form and are included for demonstration purposes only. Actual documentation of these types may include steps not delineated here.

10. References

Below are several links to organizations that test and validate digital forensics tools. This list is not considered all inclusive.

- National Institute of Standards and Technology Computer forensics tool testing project: www.cftt.nist.gov

- Defense Cyber Crime Institute RDT & E component: http://www.dc3.mil/technical-solutions/dcci-requests

Appendix A: Sample Test Plan

Sample Test Plan

Test Number: SWWB -04-01
Test Title: Software Write-Block (Software WB)

Purpose and Scope:

This test plan will test the ability of the Software WB to write-protect supported hard disks attached to a system during operational usage. The plan will consist of four test scenarios.

Requirements:

1. The Software WB forensic tool should allow normal operation to unprotected disks (i.e., the system drive)

2. The Software WB forensic tool should block all modifications to protected disks

3. The before-test and after-test md5sums should match for the protected disks

4. The Software WB forensic tool should provide feedback to the user as to the status of the tool and the disks that the tool can affect

Description of Methodology:

Various supported hard drives will be attached to standard forensic computer configuration and system will be booted. The Software WB utility must protect all non-system devices and not allow modifications from taking place. Modifications shall be attempted by executing functions that should write to protected and unprotected drives.

Expected Results:

1. The Software WB forensic tool allows normal operation to unprotected disks (i.e., the system drive)

2. The Software WB forensic tool should block all modifications to protected disks

3. The before-test and after-test md5sums match on protected disks

4. The Software WB forensic tool provides feedback to the user as to the status of the tool and the disks that the tool can affect

Appendix A: Sample Test Plan

Test Scenarios:

Test Number	Environment:	Actions:	Assigned Reqt's:	Expected Results:
04-01-01	ATA drive, primary slave SCSI drive, ID0	Copy/create/edit/ erase file	All	No modification to protected disks
04-01-02	ATA drive, secondary	Copy/create/edit/ erase file	All	No modification to protected disks
04-01-03	SCSI drive, ID0	Copy/create/edit/ erase file	All	No modification to protected disks
04-01-04	SCSI drive, ID1	Copy/create/edit/ erase file	All	No modification to protected disk

Test Data Description:

Test Data Set:

Maxtor 541DX Model 2B010H1 (ATA)
Md5sum: d0aeab1c1ace0234ee50b6b2f65791a7
Seagate Barracuda Model ST318437LW 18.4 GB (SCSI)
Md5sum: ecdb8df03e39e11ab67e8cd1dc235387

Appendix B: Sample Test Scenario Report

Sample Test Scenario Report

Test Number: SWWB -04-01-01 (a similar report will be created for all test scenarios)
Test Title: Software Write-Block during Operational Testing **Test Date:** 8/07/2003
Tester: John Doe

Test Description:

This test procedure will test the ability of the Software WB to write-protect an ATA hard drive and a SCSI hard drive attached to a system during operational usage. The procedure will consist of one case. The case consists of attaching a wiped ATA hard drive as a primary drive and attaching the SCSI hard drive on a SCSI chain. The system will then be booted, the system status confirmed and then shutdown.

Test Result:

Passed. The Software WB write-protected the SCSI and the ATA hard drives.

Hardware:
Test System:
OS Name & Version: Microsoft Windows 2000 Professional
                          5.0.2195 Service Pack 2 Build 2195
System Manufacturer: Dell
System Model: Precision Workstation 530MT
Processors: x86 Family 15 Model 2 GenuineIntel ~37202 Mhz (as indicated by
                          System Information)
                          x86 Family 15 Model 2 GenuineIntel ~37202 Mhz (as indicated by
                          System Information)
BIOS Version: 2/25/2002 SCSI Adapter: Adaptec 2940

Forensic Tool:
Title: Software WB
Manufacturer: Umpty-phrat Technologies Inc.
Version: Version 4.10.00

Appendix B: Sample Test Scenario Report

Test Data Notes:

Test Data Set: Maxtor 541DX Model 2B010H1
Md5sum: d0aeab1c1ace0234ee50b6b2f65791a7
               Seagate Barracuda Model ST318437LW 18.4 GB
Md5sum: ecdb8df03e39e11ab67e8cd1dc235387

Test Notes:

1. Since the Software WB is a Windows 2000 application, the hard drive is unprotected until the application starts during initial boot up

2. The Software WB application is loaded on the test system before the procedure is run. Automatically lock local and Network drives was selected during the Software WB install

3. The test system boot sequence is 1) Hard-disk drive c:, 2) IDE CD-ROM device, and 3) Diskette drive

4. The ATA test hard drive is attached to the test system as the primary slave. The SCSI is attached to the test system via a SCSI chain with ID0

5. A Linux bootable CD-ROM, version 3.99, is utilized to perform the validation tests

Procedures:

1. The test system is shutdown

2. Press the **"On/Off"** switch on the test system

    - Step Result: The system boots up

3. Double-click the **"SoftwareWB"** icon

    - Step Result: The Software WB application opens with the Media tab having focus. The following table is on the tab:

Media:	Partitions:	Write Blocked:
System Partition	C	No
FloppyDrive0	A	Yes
CDRomDrive0	E	Yes
HardDrive0	C	No
HardDrive1	D, I, J	Yes
HardDrive2	F, G, H	Yes

4. Close the Software WB window

    - Step Result: The Software WB window closes

Appendix B: Sample Test Scenario Report

5. Press the **"Start"** button and select **"Settings", "Control Panel"**

   - Step Result: The **"Control Panel"** window opens

6. Double-click **"Administrative Tools"**

   - Step Result: The **"Administrative Tools"** window opens

7. Double-click **"Computer Management"** button

   - Step Result: An independent **"Computer Management"** window opens

8. Select **"Disk Management"**

   - Step Result: The right side panel changes to display the attached drives information

Device	Function
Disk 0	C:
Disk 1	D: I: J: Healthy Unallocated
Disk 2	F: G: H: Healthy
CDROM0	E

9. Close the **"Computer Management"** window

   - Step Result: The window closes

10. Close the **"Administrative Tools"** window

    - Step Result: The window closes

11. Launch **"Windows Explorer"**

    - Step Result: The **"Windows Explorer"** window opens

12. Select text file **"Test.txt"** from system drive C:

13. Right-Click on file and choose **"Copy"** option

14. Select D: drive (Disk 1, first partition)

15. Right-Click and choose **"Paste"** option

   - Step Result: Dialog box appears with message **"Unable to copy the file 'test.txt'. The media is write-protected"**

16. Press **"OK"** to close the dialogue box

   - Step result: The dialogue box closes

17. In **"Windows Explorer"** window, highlight text file **"Dataset.doc"** from Disk 1, first partition path D:\

18. Press delete key

   - Step Result: Dialog box appears with message **"Are you sure you want to delete 'Dataset.doc'?"**

19. Press **"Yes"** at dialog box

   - Step Result: Dialog box appears with message **"Unable to delete the file 'Dataset.doc'. The media is write-protected"**

20. Press **"OK"** to close the dialogue box

   - Step result: The dialogue box closes

21. Close the **"Windows Explorer"** window

   - Step result: The window closes

System Shutdown:

1. Click the **"Start"** button and select **"Shutdown"**

   - Step Result: The Windows shutdown dialog box opens

2. Select "Shutdown" and press the **"OK"** button

   - Step Result: The test system shuts down

3. Remove the test hard drives from the test system

Appendix B: Sample Test Scenario Report

Expected/Actual Results:

Expected:

1. The Software WB forensic tools should allow normal operation to unprotected disks (i.e., the system drive)

2. The Software WB forensic tools should block all modifications to protected disks

3. The before-test and after-test md5sums should match

4. The Software WB forensic tool should provide feedback to the user as to the status of the tool and the disks that the tool can affect

Actual:

The actual results were the expected results

Validation Results:

1. Connect a validated hardware write-block device to the ATA test drive and boot test machine with a Linux bootable CD-ROM. Run the md5sum utility to produce an md5sum for the test drive. The following command should be used:

   ➢ tty1:/# md5sum /dev/hda

   • Step Result: The md5sum before and after test md5sums match

Test Drive	md5sum
Maxtor 541DX Model 2B010H1 (ATA)	d0aeab1c1ace0234ee50b6b2f65791a7

2. Connect an validated hardware write-block device to the SCSI test drive and boot test machine with a Linux bootable CD-ROM. Run the md5sum utility to produce an md5sum for the test drive. The following command should be used:

   ➢ tty1:/# md5sum /dev/sda

   • Step Result: The md5sum matches the before test md5sum

Test Drive	md5sum
Seagate Barracuda Model ST318437LW 18.4 GB (SCSI)	ecdb8df03e39e11ab67e8cd1dc235387

Appendix B: Sample Test Scenario Report

This test procedure validated the test criteria for the Software WB. The criteria and a validation statement are given below:

1. The Software WB forensic tool shall not block any requests to unprotected disks

    - The system was able to boot from the unprotected system drive and the system drive was used throughout the procedure

2. Following the installation of the Software WB forensic tool, all attempts to write to the write-protected ATA hard drive shall be unsuccessful

    - The unchanged before-test and after-test md5sums show that the ATA and the SCSI hard drive was not changed by the execution of the procedure

3. The Software WB forensic tool shall provide feedback to the user as to the status of the tool and the disks that the tool can affect

    - Throughout the procedure, the Software WB application provided the status of the tool relative to the disk the tool could affect

4. The unchanged before-test and after-test md5sums show that the ATA and the SCSI hard drive was not changed by the execution of these procedures

Appendix C: Sample Summary Report

Sample Summary Report

Test Number: SWWB -04-01
Test Title: Software Write-Block (Software WB)
Test Date: 8/07/2003 – 08/16/2003

Test Description:

This documents the results of testing the ability of the Software WB to write-protect supported hard disks attached to a system during operational usage. The test plan consists of four test scenarios including ATA and SCSI hard disks.

Forensic Tool:

Title: Software WB
Manufacturer: Umpty-phrat Technologies Inc.
Version: Version 4.10.00

Test Results:

Test Number	Environment	Req't 1	Req't 2	Req't 3	Req't 4
04-01-01	ATA drive, primary SCSI drive, ID0	Pass	Pass	Pass	Pass
04-01-02	ATA drive, secondary	Pass	Fail	Fail	Pass
04-01-03	SCSI drive, ID0	Pass	Pass	Pass	Pass
04-01-04	SCSI drive, ID1	Pass	Pass	Pass	Pass

Requirements:

1. The Software WB forensic tool should allow normal operation to unprotected disks (i.e., the system drive)

2. The Software WB forensic tool should block all modifications to protected disks

3. The before-test and after-test md5sums should match for the protected disks

4. The Software WB forensic tool should provide feedback to the user as to the status of the tool and the disks that the tool can affect.

Observations/Concerns:

N/A

Limitations:

Not to be used with ATA drive attached to secondary IDE channel.

Recommendations:

To be used with SCSI drives, and ATA drives connected to primary IDE channel only.

SAMPLE

SWGDE Recommended Guidelines for Validation Testing

History

Revision	Issue Date	Section	History
	08/20/2004	All	**Draft document created**
1	Approved 02/04/2004	p. 4	Changed "Test Report Template" (original document, p. 4) to **"Test Scenario Report Template"**
2	Approved 02/04/2004	p. 5	Added **"Note Regarding Included Samples"** after No. 7 ("Recommendations (optional)")
3	Approved 02/04/2004	p. 6	Changed (under "Test Scenarios, Test Number 04-01-01, Environment:) **"ATA drive, primary"** to **"ATA drive, primary slave, SCSI Drive, 100"**
4	Approved 02/04/2004	p. 8	Changed (under "Sample Test Scenario Report, Test Number): **"SWWB –04-01"** to **"SWWB –04-01-01 (a similar report will be created for all test scenarios"**)
5	Approved 02/04/2004	p. 9	Added (under "Test Notes") No. 5 (**"A Linux bootable CD-ROM, version 3.99, is utilized to perform the validation tests"**)
6	Approved 02/04/2004	p. 9	Revised the table under "Procedures," No. 3: **"HardDrive 1/D,I,J/Yes"** changed to **"HardDrive0 /C/No"; "HardDrive2/K/Yes"** changed to **"HardDrive1/D,I,J/Yes"; "HardDrive3/F,G,H/Yes"** changed to **"HardDrive2/FGH/Yes"**
7	Approved 02/04/2004	p. 9	Revised the table under "Procedures", No. 8: **"Disk 2/K"** changed to **"Disk 2/F:, G:, H:, Healthy";** replaced **"Disk 3/F:"** with **"CDROM0/E"**
8	Approved 02/04/2004	p. 9	Added, under "Procedures," No. 10: Procedures **Nos. 11-13 14-19**, **20-21**
9	Approved 02/04/2004	p. 10	Under "Validation Results," No. 1: changed **"Connect the ATA test drive to a Linux system (using an Acard) and use the md5sum utility to produce an md5sum for the test drive"** to **"Connect an Acard to the ATA test drive and boot test machine with a Linux bootable CD-ROM. Run the md5sum utility to produce an md5sum for the test drive"**
10	Approved 02/04/2004	p. 10	Under "Validation Results," No. 1: changed content of table under "Test Drive" – added **"(ATA)"** after Maxtor *reference (p.*
11	Approved 02/04/2004	p.10	Under "Validation Results," No. 2: changed **"Connect the SCSI test drive to a Linux system and use the md5sum utility to produce an md5sum for the test drive"** to **"Connect an Acard to the SCSI test drive and boot test machine with a Linux bootable CD-ROM. Run the md5sum utility to produce an md5sum for the test drive"**

Revision	Issue Date	Section	History
12	Approved 02/04/2004	p. 10	Under "Validation Results," No. 2: changed content of table under "Test Drive" – added **(SCSI)** after Seagate Barracuda Model reference
13	Approved 02/04/2004	p. 11	Under **"This test procedure validated the test criteria"**: No. 1: deleted; replaced by No. 2 No. 2: deleted; replaced by new No. 2 No. 3: retained No. 4: new
14	Approved 02/04/2004	All	Reformatted entire document (jb)
15	03/01/2004	pp. 7, 9, 10-15	Removed **highlights** from sections modified at the Feb. 2004 meeting
16	04/14/2004	p. 2	Added the following final three (3) sentences to paragraph under "**When**"
17	04/15/2004	p. 4	Under **"Process,"** deleted **"Develop and document test plan"**; replaced with **"Develop and document test plan before testing begins. The test plan should contain the following"**:
18	04/15/2004	p. 4	Under **"Process,"** deleted old 1.a (**"Shall be written before testing begins"**); replaced with new 1.a (**"Purpose and scope"**).
19	04/15/2004	p. 4	Under **"Process"**, replaced old 1.b (**"Document's purpose and scope"**) with new bullet**: "Requirements to be tested – what does the tool have to do?"**
20	04/15/2004	p. 4	Under **"Process"**, replaced old 1.c (**"Develop and document requirements to be tested – what does the tool have to do?"**) with new bullet**: "Methodology – how to test? (Identify support tools required to** assist with evaluation results when applicable)"
21	04/15/2004	p. 4	Under **"Process"**, replaced old 1.d (**"Describe and document methodology . . ."**) with new bullet: **"Test scenarios"**
22	04/15/2004	p. 4	Under **"Process"**, replaced old 1.e (**"Identify and document test scenarios"**) with new bullet: **"Test data to fulfill conditions of test scenarios – can existing reference set data be used? (Identify support tools required to assist with developing test data when applicable)"**
23	04/15/2004	p. 4	Under **"Process"**, replaced old 1.f (**"Develop or identify test data . . ."**) with new bullet: **"Document test data utilized"**
24	04/15/2004	p. 4	Added **boxed note**
25	04/15/2004	p. 4	Under **"Process"**, replaced 2.a (**"use media that is in a known state"**) with new bullet: **"Use media and/or other sample materials that are in a known state or condition"**
26	04/15/2004	p. 5	Under **"Process"**, deleted "workaround" under Bullet 2.c and added **"alternative procedure"**
27	05/12/2004	pp. 10 - 17	Added **"SAMPLE"** to all **"Sample Test Plan"** pages

Revision	Issue Date	Section	History
28	05/12/2004	All	Revised footer to read **"Final Version – Approved 04/15/2004"**
29	05/12/2004	p. 1	Revised cover page of document
30	01/15/2009	All	Revised all pages to read Version 1.1
31	01/15/2009	All	Revised footer on all pages to update version date **"(July 2004)"** to **"January 2009"**
32	01/15/2009	p. 1	Under **"Disclaimer"**, added **"(s)"** to "**Request**"
33	01/15/2009	p. 1	Under **"Disclaimer",** replaced email address (**swgde@mail.ucf.edu**), with (**research@swgde.us**)
34	01/15/2009	pp. 3, 9, 18-19	Removed "." for format consistency
35	01/15/2009	p. 16	Under **"Validation Results:",** replaced **"an Acard"** with **"a validated hardware write-blocking device"**
36	01/15/2009	p. 8	Added **"References"** section to include **"NIST"** and **"DCCC"**
37	06/06/2014	Scope	Added new language to the "Scope" and removed the note box. Voted for re-release as a Draft for Public Comment. Changed from Version 1.1 to Version 2.0.
38	06/11/2014	All	Updated formatting throughout the document to match the current SWGDE formatting scheme (including numbered headers and a table of contents) and added new disclaimer. No changes to content. Formatted for release as Draft for Public Comment. (Version 2.0)
39	08/28/2014	None	No changes made; voted to publish as an Approved document. (Version 2.0)
40	09/05/2014	All	Formatting and technical edit performed for release as an Approved document. (Version 2.0)