Once you approve and submit the following information, changes may only be made through the NesCom Administrator.

Draft PAR Confirmation Number 269667461.20719	
Submittal Email: matt.ball@ieee.org	
Type of Project: PAR for a revision to existing Standard 1619-2007	
1.1 Project Number: P1619	
1.2 Type of Document: Standard for	
1.3 Life Cycle: Full	
2.1 Title of Standard: Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices	**Old Title:** IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

3.1 Name of Working Group: Security in Storage Working Group(C/IA/SIS-WG)
Contact information for Working Group Chair
Matthew Ball
1020 Birch St
Broomfield, CO 80020
US
matt.ball@ieee.org
Working Group Vice Chair: Eric Hibbard
950 Larkspur Ave
Sunnyvale, CA 94086
US, **Email:** eric.hibbard@hds.com

3.2 Sponsoring Society and Committee:IEEE Computer Society/Storage Systems(C/SS)
Contact information for Sponsor Chair:
Curtis Anderson
2421 Mission College Blvd.
Santa Clara, CA 95054
US
curtisanderson1@comcast.net
Contact information for Standards Representative:

3.3 Joint Sponsorship:
IEEE Computer Society/Information Assurance(C/IA)

4.1 Type of Ballot: Individual

4.2 Expected Date of Submission for Initial Sponsor Ballot: 2010-05

4.3 Projected Completion Date for Submittal to RevCom: 2010-12

5.1 Approximate number of people expected to work on this project: 10

5.2 Scope of Proposed Standard: This standard specifies the XTS cryptographic mode of operation for the AES block cipher and an XML-based key archive format for block-oriented storage devices.	**Old Scope:** This standard specifies elements of an architecture for cryptographic protection of data on block-oriented storage devices, describing the methods, algorithms, and modes of data protection to be used.

5.3 Is the completion of this standard is dependent upon the completion of another standard: No
If yes, please explain:

5.4 Purpose of Proposed Standard: The purpose of this standard is to expand the XTS cryptographic mode while maintaining backwards compatibility with existing implementations that are compliant with IEEE Std 1619-2007.	**Old Purpose:** This standard defines specific elements of an architecture for cryptographically protecting data stored in constant length blocks. Specification of such a mechanism provides an additional and improved tool for implementation of secure and interoperable protection of data residing in storage.

5.5 Need for the Project: The XTS-AES cryptographic mode of operation was submitted to NIST for consideration as an approved mode of operation under FIPS 140. A number of technical issues were raised as a result of the NIST review. This project will examine the NIST review and produce a revised standard based on the feedback from the NIST public comment period.

5.6 Stakeholders for the Standard: The stakeholders include vendors of data storage devices such disk drives, disk storage systems, and encryption appliances.

Intellectual Property
6.1.a. Has the IEEE-SA policy on intellectual property been presented to those responsible for preparing/submitting this PAR prior to the PAR submittal to the IEEE-SA Standards Board? Yes
If yes, state date: 2009-05-14
If no, please explain:
6.1.b. Is the Sponsor aware of any copyright permissions needed for this project? No
If yes, please explain:
6.1.c. Is the Sponsor aware of possible registration activity related to this project? Yes
If yes, please explain: The SISWG maintains an OID registry for cryptographic algorithms. See http://grouper.ieee.org/groups/1619/SISWG_OID_registry.txt

7.1 Are there other standards or projects with a similar scope? No
Explanation:
Sponsor Organization:

Project/Standard Number:
Project/Standard Date: 0000-00-00
Project/Standard Title:

7.2 International Standards Activities

a. Adoptions

Is there potential for this standard to be adopted by another organization? Do not know at this time
Organization:
Technical Committee Name:
Technical Committee Number:
Contact person Name:
Contact Phone:
Contact Email:

b. Joint Development

Is it the intent to develop this document jointly with another organization? Do not know at this time
Organization:
Technical Committee Name:
Technical Committee Number:
Contact person Name:
Contact Phone:
Contact Email:

c. Harmonization

Are you aware of another organization that may be interested in portions of this document in their standardization development efforts? Yes
Organization: ISO/IEC JTC1
Technical Committee Name:
Technical Committee Number: SC27
Contact person Name: Eric Hibbard
Contact Phone:
Contact Email: Eric.Hibbard@hds.com

8.1 Additional Explanatory Notes: (Item Number and Explanation)

The revisions to the scope and purpose of 1619-2007 are intended to limit any changes to just the XTS mode of operation and the associated XML based key backup format.

Submit to NesCom | Save and Come Back Later

Contact the NesCom Administrator