Email This Letter

02 November 2006

Jack Cole
US Army Research Laboratory
504 Idlewild Road
Bel Air, MD 21014-4419
jack.cole@ieee.org

Re: P1619.2 - Standard for Wide-Block Encryption for Shared Storage Media

Dear Jack:

I am pleased to inform you that on 02 November 2006 the IEEE-SA Standards Board approved the above referenced project until 31 December 2010. A copy of the file can be found on our website at http://standards.ieee.org/board/nes/projects/1619-2.pdf.

Now that your project has been approved, please forward a roster of participants involved in the development of this project. This request is in accordance with the IEEE-SA Operations Manual, Clause 5.1.2i under Duties of the Sponsor which states:

"Submit annually to the IEEE Standards Department an electronic roster of individuals participating on standards projects"

For your convenience, an Excel spreadsheet for your use has been posted on our website at http://standards.ieee.org/guides/par/roster.xls. Please forward this list to me via e-mail at s.hampton@ieee.org no later than 31 January 2007.

Please visit our website, IEEE Standards Development Online (http://standards.ieee.org/resources/development/index.html), for tools, forms and training to assist you in the standards development process. Also, we strongly recommend that a copy of your draft be sent to this office for review prior to the final vote by the working group to allow for a quick review by editorial staff before sponsor balloting begins.

If you should have any further questions, please contact me at +1 732 562 6003 or by email at s.hampton@ieee.org.

Sincerely,

Sherry Hampton
Administrator, Governance
Standards Activities
Phone +1 732 562 6003
FAX +1 732 875 0695
Email: s.hampton@ieee.org

CC: curtisanderson1@comcast.net, james.hughes@sun.com

PAR Request Date: 27 September 2006	
PAR Approval Date: 02 November 2006	
PAR Signature Page on File: Yes	
Type of PAR: New IEEE Standard	
Status: PAR for a New IEEE Standard	
Root Project:	
1.1 Project No.: **P1619.2**	
1.2 Type of Document: Standard	
1.3 Life Cycle: Full-Use	
1.4 Is this document in ballot now? No	
2.1 Title Standard for Wide-Block Encryption for Shared Storage Media	
2.1 Amendment/Corrigenda Title	
3.1 Working Group Name	Storage System Standards Working Group
Working Group Chair	Hughes, James Phone: 202 375 0311 Email: james.hughes@sun.com
Working Group Vice Chair	
3.2 Sponsor	IEEE Computer Society Information Assurance (C/IA)
Sponsor Chair	Cole, Jack Phone: 410 278 9276 Email: jack.cole@ieee.org
Name of Standards Liaison Representative (if applicable)	
3.3 Joint Sponsor	IEEE Computer Society Storage Systems (C/SS) Anderson, Curtis Email: curtisanderson1@comcast.net
4.1 Type of Ballot: Individual	
4.2 Expected Date of Submission for Initial Sponsor Ballot: September 2007	
4.3 Projected Completion Date for Submittal to RevCom: March 2008	
5.1 Approximate number of people expected to work on this project: 15	
5.2 Scope: This standard specifies an architecture for encryption of data in random access storage devices, oriented towards applications which benefit from wide encryption-block sizes of 512 bytes and above.	
5.3 Is the completion of this document contingent upon the completion of another document? No	
5.4 Purpose: This standard specifies an architecture for media security and enabling components. Wide encryption blocks are well suited to environments where the attacker has repeated access to cryptographic communication or ciphertext, or is able to perform traffic analysis of data access patterns. The standard is oriented towards fixed-size encryption blocks without data expansion, but anticipates an optional data expansion mode to resist attacks involving data tampering.	

5.5 Need for the Project: The IEEE Information Assurance Standards Committee is developing standards for secure storage of data on random and sequential access devices. This standard is part of that effort and is designed to focus on the requirements of random access devices where attackers have a high degree of access to the stored data and/or to data traffic to and from the device. This standard will specify cryptographic solutions which are optimized to protect against this threat model and which will enhance the security of stored data in such environments.

5.6 Stakeholders for the Standard: Stakeholders include potential implementors and customers. Implementors include hardware disk drive manufacturers, providers of cryptographic security modules for data storage, and software implementations of disk data encryption systems. Customers include a wide range of industries and services which will benefit from enhanced security of stored data.

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 **Presented Date:** 2006-08-30
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? No
If yes, please explain:

7.1 Are there other standards or projects with a similar scope? Yes
If yes, please explain:
The IEEE Security in Storage Working Group is creating standards for secure storage of data in a variety of environments and threat models. This standard is part of that work and is distinguished from other standards of the Working Group by its focus on a particular threat model and set of attacker characteristics.
Sponsor Organization: IEEE Computer Society
Project/Standard Number: P1619
Project/Standard Date: 2002-08-15
Project/Standard Title: Standard Architecture for Encrypted Shared Storage Media

7.2 Is there potential for this standard (in part or in whole) to be adopted by another national, regional, or international organization? ? Do not know at this time
Technical Committee Name and Number:
Contact person:
Contact person Phone Number:
Contact person Email Address:

7.3 Will this project result in any health, safety, security, or environmental guidance that affects or applies to human health or safety? No

7.4 Additional Explanatory Notes:
Item 3.1 - The correct name of the working group is "Security in Storage Working Group" (SIS-WG). This name was not offered as an option by the web form.

8.1 Sponsor Information:
Is the Scope of this project within the approved scope/definition of the Sponsor's Charter? Yes
If no, please explain: