

NP Letter Ballot

VOTE ON A PROPOSED NEW WORK ITEM

ISO/IEC JTC 1 N5729

Date of Ballot Close: **2007-09-19**

Please return all votes and comments directly to the JTC 1/ (SC YY) Secretariat by the due date indicated.

Proposal for a new work item on Guidelines for application security (27034)

A. Vote		YES	NO	Comments
Q.1	Do you accept the proposal in document JTC 1 (SC 27) N 5729 as a sufficient definition of the new work item? (If you have responded "NO" to the above question, you are required to comment.)		X	The proposal does not provide sufficient information about the future content of the new standard and its multiple parts. As such it is unclear what the scope of the standard and its parts will be and leaves it open to a variety of interpretations. It is also unclear whether the parts as planned will have overlapping content. Since a definition of application security is not provided, the reader is left wondering what it means and how it is different from software security. When it comes to the security principles, considerations, and practices that should be added to the software lifecycle it is irrelevant whether the security practices apply only at the application layer or at multiple layers. There is nothing unique about how application layer software is specified, designed, implemented, tested, or maintained. While it appears that more attacks are targeting the application level software, in many cases the application level software is just a conduit through which

		<p>software vulnerabilities in lower-level software are being targeted, including vulnerabilities in network protocols, frameworks/middleware, and operating system device drivers and DLLs, etc. Software in general needs to have its security improved – not just application-level software. A security-enhanced SDLC would benefit ALL software with the same the security-enhanced practices, such as ensuring that security requirements are adequate and reflect the true threat environment in which the software will operate, adhering to secure design and coding principles and practices, reviewing and verifying the adequate security of architectures designs and of third-party components, performing adequate security analysis and testing on source and binary code and on the integrated software system as a whole, and adhering to security principles and secure practices for distribution, deployment, and sustainment of implemented software (including secure SCM, patch management, software rejuvenation, refactoring/reengineering, etc.).</p> <p>The current scope and the diagram provided in Annex A do not address the fact that there are existing ISO standards that provide software and system development lifecycles. The application security standard should not be attempting to rewrite existing Sw and system development lifecycles, on the contrary, it should address integration of</p>
--	--	---

				security into Sw and system development lifecycles to ensure that any application (or software) is developed using best Sw development and security practices.
Q.2	Do you support the addition of the new work item to the programme of work of the joint technical committee?		X	Proposal needs to be revised to provide more detailed scope statements for the overall standard and each part before it can be added to the programme of work.
B. Participation				
Q.3	Do you commit yourself to participate in the development of this new work item?		X	
Q.4	Are you able to offer a project editor who will dedicate his/her efforts to the advancement and maintenance of this project? (If "YES," please identify)		X	
C. Documentation				
Q.5	Do you have a major contribution or a reference document ready for submittal?		X	
Q.6	Will you have such a contribution in ninety days?		X	
Q.7	Which standard development track is proposed		X	

P-member Voting: National Body	Date:	Submitted by: Name