Epsilon Labs Security Source Code Review Scoping Questionnaire – v 2.0
December 2012

	Question	Yes	No	Additional notes
1 Basic application description				
1.1	Describe briefly the application (what the application is supposed to do) and list the main business functions/modules.			
2 Documentation and Security Requirements				
2.1	Is the application architecture documented and to what extent?			
2.2	Are all the application interfaces documented and to what extent?			
2.3	Are the application security requirements documented and to what extent?			
2.4	Is the application threat model documented?			
2.5	Are there any codding conventions and are they documented?			
2.6	What is the primary documentation language?			
3 Data and data classification				
3.1	Is any of the data processed, transferred or stored by the application subject to data security/protection regulations/standards (PCI-DSS, HIPPA, FERPA etc.)? If so please specify which standards/regulations/			
4 Basic application architecture and implementation details				

4.1	What is the primary development language?			
4.2	Are there parts of the code developed using other than the primary programming languages? If so please specify the languages.			
4.3	Is the application tiered and if so how many tiers it consists of?			
4.4	Is the application built on top of commercial or open source platform and if so which one?			
4.5	Is there are third-party code called by the application classes/method/functions?			
4.6	Is there DB backend and if so what type?			
4.7	Is the application web service oriented and if so what type of services it is implementing and/or consuming?			
4.8	What protocols the application relies on (communication protocols)?			
4.9	Are they any custom protocols that the application implements?			
5 Access, User and role management				
5.1	Does the application implement SSO or/and federated authentication?			
5.2	What type of access control the application implements – mandatory access control, discretionary access control, role based access control or other?			
5.3	Does the application segregate the logic accessible to users in different roles? If so how many roles are supported?			

5.4	Is the user/role management handled by the application logic itself or it relies on third party authorization mechanisms?			
6 Metrics				
6.1	What is the number of files to be reviewed?			
6.2	What is the number of custom developed classes?			
6.3	What is the number of the communication interfaces (interfaces connecting the application with external entities)?			
6.4	What is the number of the application input paths (for example user, configuration files, backend etc.)?			
6.5	What is the number of custom developed stored procedures and triggers?			