SUPPLEMENTARY SUBMISSION No. 4.1

Supplementary Submission 2 To Australian Federal Parliament
Joint Select Committee on Cyber Safety

Prepared By
Louis Leahy
Director
Armorlog International Ltd
Suite 3, 6-16 Riverview Street
PO Box 80 North Richmond
New South Wales
Australia 2754
Armorlog@Armorlog.com.au
1 June 2010

1. **Further to our previous submission to the honourable Committee Members we provide a further update in regard to development of the technology referred to in that submission and supporting independent industry research for such a solution.**

2. **We confirm that the Commercialisation Australia application was refused without explanation.**

3. **We confirm the Government Director of Authentication refused to consider our innovation without explanation.**

4. **We confirm we have written to all major Government sponsored research and development organisations associated with technology development without any substantive response from any of those organisations and without any response whatsoever for the majority perhaps some 75% or more.**

5. **We have written to the former Prime Minister and the Current Prime Minister and had no response from either.**

6. **While we are being ignored in our endeavour to garner that support people continue to be, tricked, cheated, defamed and defrauded and confidence in internet based commerce and communications is being severely eroded to such an extent that some people are arguing that the answer is to switch off the internet. Certainly this issue has become that critical that the Parliament in its wisdom has seen fit to commission this inquiry.**

7. **We believe there has been discrimination on the basis of the size of our organisation which is contrary to the spirit of Federal Government procurement guidelines which we understand have a legislative basis.**

8. **We have entered into a lead distribution agreement with a large North American software distribution company known as Digital River.**

9. **We are still coding the initial commercial grade release of the technology and have a revised target release date of March or April 2011.**

10. **Our Company has been accepted as a Member of the Online Trust Alliance (OTA) subject to a board committee level review. We had the opportunity to meet with significant industry representatives at the OTA forum in Washington and have briefed among others a Distinguished Engineer of one of the leading online payments companies about our technology.**

11. **The technology has been well received by everyone who has taken the time to review in detail.**

12. **We had a successful showing at CommunicAsia with the assistance of NSW Industry & Investment and Austrade.**

13. **It appears we will attend a trade mission with Austrade to ASEAN countries shortly.**

14. **It is now becoming apparent from various industry research that is being conducted, that the Armorlog ™ VPCSML ™ authentication technology is the correct solution that will provide significantly improved protection against current forms of attacks against network authentication.**

15. **This is because it is now clear from research conducted by companies such as Verizon (Verizon 2010 Data Breach Report) that the most damaging cases of loss involve circumstances where the credentials of a user have been successfully acquired or altered to access the network. Thus a key requirement is to prevent a user from being tricked into revealing their codes and to prevent codes from being surreptitiously accessed or copies which is what our technology does.**

16. **We have come up against arguments that this is too simplistic an approach however those arguments are misconstrued and based on attacks on client side devices and their applications code and operating systems which completely misses the point. The key to protecting user information online is to ensure the protection on the network server has been designed to protect the user credentials and consequently protect the privacy of the user information on that network database. Other forms of attack while they are often malicious and cause harm do not, as the research shows, result in the most significant losses because they do not result in ownership of the credentials and consequently access to the network by stealth which is the true aim of criminal enterprises.**

17. **It is also clear from research conducted by the Independent Oracle User Group (IOUG) that more than 68% of organizations cannot tell if they have had a data breach. We argue that given the ease with which the current authentication topology can be circumvented that these events are occurring at much higher rates than anyone is prepared to admit.**

18. **We view this with great concern given that there is an ongoing push to outsource information systems management and hosting to networks on which the organisation has far less control over who has access i.e. cloud computing.**

19. **A survey conducted on over 250,000 user social networking accounts by BitDefender found that over 75% used the same password for multiple accounts. This means an attacker may secure a victims password to gain control of an account by simply enticing them to establish an account at site already controlled by the attacker. Our technology is designed to ensure that an Administrator can have unique passwords for users to protect their network. We have designed the system in such a way that the user can devise a memorable password without the need for undue complexity without a reduction in security that occurs on existing authentication topology.**

20. **In reference to this we note we have already highlighted to the Committee in our initial submission our concerns regarding the use of single sign on solutions such as the Auskey solution that has already been implemented on some Government networks in deference to a solution such as ours. We wonder if the heads of those Government Departments understand the magnified security risks of those arrangements.**

21. **Our technology is designed to reduce the instances of breaches by strengthening the key point of weakness the authentication of a user onto a network. This in turn will significantly improve online security.**

22. **The technology we have designed will complement existing technologies to make them more effective. The reverse is not true however our technology on its own will provide significantly improved security while all existing methods of trying to protect against the theft of credentials are not effective if the authentication topology in its current form that is used in nearly all situations is not fixed.**

23. **We would welcome more vocal Government leadership on such an important issue both nationally and internationally and again we commend the Honourable Members of the Committee and the Parliament for their continued interest and work in this matter.**

For Armorlog International Ltd

Louis Leahy

Digitally signed by Louis Leahy
DN: cn=Louis Leahy, o, ou, email=asa0010@msn.com.au, c=AU
Date: 2011.01.24 17:20:45 +11'00'