Good morning Bob, I communicated with you separately two days ago following the reported breach of security at the Customs office at the Sydney airport on 27 August 2003. I note today that another reported theft took place in the Canberra office of the Department of Transport on 22 August 2003. A swipe card provided access for the thief and it is reported that sensitive maritime data was contained on the HDD of the laptop stolen.

I now wish to make a formal submission to the JCPA.

As I see it there are several issues that should be addressed in regard to 'security'. May I suggest they are;-

* (A) Secure access control to areas within places of Government and it's department's premises.

* (B) Secure log-in procedures to enable authorised access to laptop, desktop and server computer data.

* (C) Complete data erasure of data from hard drive disks contained within laptop, desktop and server computers when that equipment is disposed of through an auction house or by other means.

* (D) Physical security of lone and vulnerable employees within and attached to Government and it's departments.

Let me offer some features and benefits of our products in each of these defined areas;-

(A) Access control;- Precise Bioaccess identifies people, not PINs and passwords, it provides one-to-one matching and instant identification. Bioaccess is a plug and play fingerprint reader that offers unparalleled security for access control. Precise Bioaccess offers the best security on the market at a competitive price, because it requires no new wiring and no software purchases or modifications and is particularly valuable for increasing the effectiveness of existing systems.

I have attached a copy of a press release dated yesterday concerning the Precise Biometrics' President testifying to the US Congress on biometrics and smart cards.

I have added a flash animation link here that better presents the products for physical access control and the second issue (B) above;-
http://www.precisebiometrics.com/products.asp?GROUPID=20020627_135857_50337051

In addition to this concerning (B) above, Utimaco SafeGuard Easy provides perfect Government (departmental or whole) protection for sensitive information on notebooks and workstation HDDs in computers. Boot protection, pre-boot user authentication and hard disk encryption using powerful algorithms make unauthorised access impossible. Not even hacker tools can decipher data protected by SafeGuard

Easy. SafeGuard Easy is simple to install and operates in a way that is invisible to the user.

John Nelson at DPRS Parliament House Canberra would be an ideal person to communicate with regarding this product. We understand that each Minister of Federal Parliament who has a notebook PC now has this product installed on the PC.

(C) Data erasure is not a term that most people are not aware of. There is a misconception that when one hits the 'delete' key or empties the 'recycle bin' by selecting that icon on the desktop, that the data, emails, and secret and sensitive data is disposed of.
Another approach to 'erasing' data is to re-format the hard drive, this is simply a waste of time and money. Some organisations drill a hole through the HDD and others crush them. Most of these approaches are ineffective, time consuming and costly.

Blancco data erasure is a simple to use product that ensures total data erasure and the erased data can not be recovered by any existing technology known at this date of communication.

I have attached a white paper concerning Blancco data erasure and there is also a link provided;-
http://www.comsecent.com.au/Blancco.htm

(D) Physical security of lone/vulnerable workers has become a growing concern with 'duty of care' for employers becoming a major issue.
In an ideal situation, each of these workers would be equipped with a devise that in the case of an emergency, when activated by simply pressing a large button, would notify someone where that person is located using GPS triangulation
and simultaneously a two way line of communication via GSM coverage would be activated. This circumstance would be most effective in areas of GSM coverage where the majority of these workers are located however, there are large and remote areas of Australia that does not have that facility. In those circumstances other equipment would be required and we do not have that solution in our product range.

We understand the Government procurement tender system and we have secured GITC accreditation for supply.

Our organisation is Brisbane based and we understand that in Queensland alone within the State Government that there are in excess of 300,000 computers. If one uses that figure as a base, the total number of computers in Government use must number in the millions. Our philosophy is that there must be a better way of total 'Government' procurement for all that it purchases and consumes. The buying power of 'Government' is massive and millions of dollars could be saved for use in more deserving areas than to have the current state of affairs which determines that each department in each government controls it's own purchases. That subject is connected here however, it may be larger than all of us put together to deal with.

We look forward to the result of our submission.

If there are questions, please come back to me or, in my absence, Mr Hans Axmacher who is the Chairman of our company.
Hans' Email address is hans@swe-tech.com.au

I have copied Hans with this Email and we both understand that until such time as you clear the content of this Email for other use, the content will remain private and confidential.

Respectfully submitted,

Stewart Edwards

Sales Director
The Swe-Tech Group
(Swe-Tech Pty Ltd, Com-Sec Enterprises & Benefon Australasia)
Level 3, 303 Adelaide Street, Brisbane
Queensland. 4000