Professional Information Security Association

Phone : (852) 8104-6800
Fax : (852) 2900-8338
Email : info@pisa.org.hk
URL : www.pisa.org.hk

Mrs. Alice Lau
Commissioner of Inland Revenue
Revenue Tower
5 Gloucester Road, Wanchai
Hong Kong

10 February, 2002

Dear Mrs. Lau,

Further Comments on Amendment to the Inland Revenue Ordinance (Cap. 112)

On behalf of the Executive Committee of PISA, I would like to express our gratitude to your demonstration of the tax return e-filing system testing interface. It was indeed a golden chance for face to face communication to learn more about each other's concerns. We noted from your presentation that IRD has considered:

(1) suspending the implementation of some "sensitive" features of the tax e-filing system until a review by external assessors – like the default personal information screen and the submitted data review and modification function;

(2) enforcing user to read the security statement before making a successful submission;

(3) holding education programme to make people aware of the difference in security levels between PIN and digital signature.

We appreciate very much the effort of the HKSAR Government to make popular the use of electronic government services in the city. We would like to state that while moving in such direction we have to maintain the security of the system and balance the convenience with the risk introduced. Trust and Confidence are pillars of a government. They take tens of years to build up but one day to lose. A recent UK survey proved the importance and sensitivity of the tax online system on the trust of government again:

> In a survey of 200 UK citizens conducted by firewall vendor Check Point found that 93 percent would not file their taxes online for security concerns. [……] Checkpoint argues that many of those who happily pay for goods online can be persuaded to fill out tax

Phone : (852) 8104-6800
Fax : (852) 2900-8338
Email : info@pisa.org.hk
URL : www.pisa.org.hk

returns on the Net if the government does more to build confidence in e-government.

Reference: http://www.theregister.co.uk/content/6/29091.html

We do *not* intend to amend the opinions we submitted on 20 September 2002 but would like to supplement our opinions after getting more information from you.

1. The Electronic Transaction Ordinance (ETO) 2000 sets the basis for the development of electronic commerce of Hong Kong. ETO recognizes digital signature as the **only one** proven technology among other known electronic signatures that satisfies the requirements of authentication, confidentiality, integrity and non-repudiation. In the ETO review in year 2002, use of PIN was proposed for consultation. From the recent conclusion of the ETO review, digital signature remains as the only accepted technology and PIN is not considered to be included in the ETO as an accepted technology. We see the result of ETO review 2002 has addressed the concerns of the public on the inferior security level of PIN to be used in critical services and also the confusion of co-existence of digital signature and PIN would lead to.

2. ETO provides the provision for services to use alternative technology other than digital signature. This provision forms the legal basis for IRD's proposed bill amendment. We note that such provision in the ETO does not state explicitly and clearly,
   (a) The criteria for a service to apply the provision, and
   (b) The security requirements that a service need to meet after getting such provision.
   Our interpretation is that if any service could apply such provision, it at least should not have any adverse impact to the ETO or making it de facto being bypassed. Secondly the security measures of the system should meet up with the one provided by the digital signature. Thirdly, such system should upgrade as the development of ETO.

3. IRD's application is setting the precedence for subsequent applications. If IRD's application should succeed then we cannot see why the applications of any government

Phone : (852) 8104-6800
Fax : (852) 2900-8338
Email : info@pisa.org.hk
URL : www.pisa.org.hk

services should fail, if they can prove they have same or lower risk level with the IRD's tax return e-filing. If government services could easily apply for exemption from using digital signature, we cannot see why the business should take the ETO seriously.

4. It is prudent that IRD should set a good example for the government as well as business when she tries to apply for the provision in the ETO. It is not only to prove that IRD has such a need but also proves that points #2. and #3. above are well considered.

5. Although there is no actual financial transaction involved in the filing a tax return, the information involved in the tax return filing process is regarded as highly personal and confidential. Besides, as we all are aware, submission of untrue, incorrect and incomplete return may incur heavy penalties. Although IRD has shown her willingness to take a very relaxed consideration towards erroneous submission, we cannot see this improved any confidence of the tax-payer because this consideration should have been there already. In terms of risk level, we still consider a system with critical financial information and bearing criminal offense consequence as *sensitive*. If a sensitive system can use PIN why other system should not. And if so many systems can use PIN if they apply for it, what is the ETO for?

6. IRD's proposal cited the example from current PIN-based online banking systems. We would like to point out that online banking systems have to fulfil the security requirement defined in the guidance note "Management of Security Risks in Electronic Banking Services" issued by the Hong Kong Monetary Authority (HKMA), a third party which monitors the compliance of the authorized institutions operation. The guidance covers quite a comprehensive scope of area to protect and secure the electronic services from policies, physical access control to system and network security. HKMA also recommends two-factor authentication in the guidance note, otherwise other compensation security or control measures are required, e.g. educating and promoting sound password practices to customers, making use of different passwords for different types of services, pre-registration for higher risk transactions, establishing limit on transaction amount, etc.

Phone : (852) 8104-6800
Fax : (852) 2900-8338
Email : info@pisa.org.hk
URL : www.pisa.org.hk

We see that the current IRD proposal lacks the equivalent guideline and external assurance mechanism for security compliance. It is a must for IRD's proposal to make up one if she wants to cite online business system as reference. IRD should include in her bill on:

(a) What security requirements are required to meet in implementing the system?

(b) What security requirements are required to meet in maintaining the system?

(c) How can the security requirements be upgraded with further development of the ETO?

(d) How can the implementation include an assurance mechanism involving periodical external assessment and continuous improvements?

7. We would like to point out that currently there is a concerted effort in making the use of digital signature popular with the advent of the Smart ID card. Firstly, HKMA's requirement recommends the use of two-factor authentication. Secondly the new smart ID card to be launched this year will provide incorporation of digital certificate. Thirdly the Hong Kong Post Office has been promoting the usage of digital certificate in the industry and other ecommerce activities before the launch of smart ID card. Lastly, banks that have not employing digital certificates are now considering the feasibility to move to make use of smart ID card with digital signature. We think that this should the RIGHT direction to move forward, instead going back to a less secure technology and possibly undermine the secure infrastructure we had built up.

8. PISA considers PIN based system is **not** suitable for IRD Tax Return Filing system. IRD should continue to use digital signature to sign the filing. However, if IRD is determined to go ahead with her proposal, we would advise that at least these controls be added to the system:

(A) **Minimizing the Risk** of the tax e-filing system by removing the higher risk features like "Default data display on the next entry", "Data review and modification".

Phone : (852) 8104-6800
Fax : (852) 2900-8338
Email : info@pisa.org.hk
URL : www.pisa.org.hk

(B) **Implementing Reasonable Controls** equivalent to the requirements and recommendations of the HKMA's guidance note "Management of Security Risks in Electronic Banking Services":

(1) Implementing comprehensive **information security policies**;
(2) Enforcing adequate **physical security** measures to protect the network and computer equipment;
(3) Controlling the security **risk arising from the external** service or solution **providers**;
(4) Providing an advice to the customers on security precautions in relation to electronic services;
(5) Performing **annual auditing** of the system security, policy and procedure compliance;
(6) Implementing adequate **audit logging** to record security breaches or weakness and consider the installation of "intrusion detection system";
(7) Implementing **adequate system and network security** to protect the internal network resources from the external threat;
(8) Employing a **secure encryption technology** to protect the confidentiality of information during the passage over the internal or external network or storage;
(9) Adopting a **strong password policy** for Internet online system with a long alphanumeric and symbol string instead of the weak 6-digit PIN currently proposed. We have like to cite the PPS, the local Electronic Payment Services successfully implementing a stronger PIN on the Internet payment service although their telephone payment service is limited by telephony technology to use a weak digit-only PIN.
(10) For **sound password practices**, IRD should provide the citizens the advices that (i) enforce to change the initially assigned password during the first login; (ii) not to make use of easily guessable passwords, e.g. phone number, HKID No., birthday, dictionary words; (iii) not to disclose the customer id and password to anyone including the staff of IRD; (iv) periodic change to new password; (v) not to leave the devices during the middle of session; (vi) promptly log out from the services after usage; (vii) disable the auto-complete features in the user's browser if any; (viii) not to install illegal software

Phone : (852) 8104-6800
Fax : (852) 2900-8338
Email : info@pisa.org.hk
URL : www.pisa.org.hk

or open doubtful email that may contain viruses or Trojan horses; (ix) provide guidance to citizens to safeguard against attack using "social engineering" techniques; (x) report any compromise of the passwords to the IRD as soon as possible.

We would like to stress that PIN **cannot** replace digital signature even with these compensation measures. Furthermore, use of PIN creates more management problems, confusions and trust issues. We also like to point out that it is not fair to enforce the many layman tax-payers to determine the technology to use and take the risk they might not have the technical competence to handle. Forcing them reading a statement does not help educating them the difference in security between PIN and digital signature.

We appreciate our opinions be considered by the administration and look forward to your reply. Please contact me at telephone 8104-6800 or email: sc.leung@pisa.org.hk.

Yours faithfully,

Mr. LEUNG Siu Cheong
Chairperson
Professional Information Security Association

Cc:
Bills Committee on Inland Revenue (Amendment) (No. 2) Bill 2001,
Legislative Councillors