By Post and by Fax

Mrs Constance Li
Clerk to Bills Committee
Legislative Council Secretariat
3/F, Citibank Tower
3 Garden Road
Central, Hong Kong

20 September 2002

Dear Mrs Li

Comments on Inland Revenue (Amendment) (No.2) Bill 2001

Thank you for your email date 9 September 2002 requesting comments from Information Systems Audit and Controls Association - Hong Kong Chapter (ISACA-HK) in relation to the above Bill.

First, ISACA-HK would like to express its support in principle for the initiative of the Inland Revenue Department (IRD) to encourage the greater use of electronic services as part of the Government's intention to promote e-Government and e-Commerce in Hong Kong.

When the Bill was first gazetted in November 2001, ISACA-HK raised a number of issues with the Commissioner of Inland Revenue (CIR). Our main concerns at the time related to the security controls of the proposed electronic submission mechanism, specifically the proposal to treat the submission of a tax return through the use of a password as the legal equivalent of signing a return, as well as the adoption of certain technical terminology and concepts.

Rather than re-iterating the points raised, we have attached in Appendix 2 a copy of our correspondence to the CIR for your information.

However, having studied the Legislative Council Paper on the subject (Ref: LC Paper No. CB(1) 2273/01-02), there are a number of additional comments we would like to raise, and these are set out in Appendix 1. In order that our comments can be understood in their proper context, we have copied the relevant paragraphs from the LC Paper to which each of our comments relate.

We would welcome the opportunity of discussing the issues raised with members of the Bills Committee if required.

Yours Faithfully

Susanna Chiu
President, ISACA-HK

Encl.

Appendix 1: Comments on Inland Revenue (Amendment) (No.2) Bill 2001

1: Security Requirements

> *Security aspects*
> *6. According to the Administration, the level of system integrity required or desired in an IT system has to be determined having due regard to the risk involved. The Information Technology Services Department has studied the proposal for allowing the filing of a return under the ESD Scheme by using a password and concluded that such a system will attain a high level of security in the transmission of tax data by meeting the "strong encryption" requirements and protecting the session key against third party access, and that the security level of the system is the same as in the case of digital certificate.*
>
> *Ref: CB2/BC/12/01*

We entirely support the principle that the level of system integrity required needs to be determined having considered the specific risks to which a system is exposed.

It is therefore important to clearly understand the risks relevant to the proposed electronic tax submission system. Clearly tax data will be transmitted electronically through a public network. In this respect, it is essential to protect the session key used to encrypt data during transmission. As we understood from the CIR, 128-bit SSL is to be implemented in the proposed system. As such, we agreed that in relation to the "transmission of tax data", the proposed technical framework does meet the "strong encryption" requirement.

Transmission security, however, should not be confused with the need for properly authentication of the taxpayer who submitted the data. In this respect, the proposed system will only make use of a simple password. It may be true that the password, when transmitted to the IRD's system, will be encrypted - given that the system uses SSL. However, the issue is whether the use of passwords as the sole means of authentication is adequate for a system that process sensitive information and carries legal ramifications for the person who submits such information. As such, the use of a password is not the same as using digital certification as a means of authentication.

The last sentence in paragraph 6 of LC Paper No. CB2/BC/12/01: *"... has studied the proposal for allowing the filing of a return under ... by using a* ***password*** *and concluded that such a system will attain a high level of security in the* ***transmission*** *of tax data by meeting the "strong encryption" requirements and protecting the session key against third party access, and that the security level of the system is the same as in the case of* ***digital certificate****."* seems to suggest that the conclusion on the adequacy of transmission security has been inappropriately extended to the selection of the means of authentication.

This view seems to be corroborated by the comments in LC Paper No.: CB(1)716/01-02(03). Specifically in the Technical Measures section, there were the following comments:

> *Transmission of tax return data through ESD platform by password*
> *4. Internet filing by using a password is as secure as in the case of using digital certificate. Except that the electronic submission will be signed by applying the taxpayer's password, the system can achieve the same level of security for the data transmitted over the Internet because of the use of strong encryption technology. Due to the use of encryption technology, information on the tax return will be end-to-end encrypted on the one hand, meaning the information will be encrypted from the point the return is sent to the point when the return is received by the department by a group of numbers randomly generated by the browser (commonly known as the session key) and IRD's public key. On the other hand, the taxpayer's password will also be encrypted by a different set of randomly generated numbers and IRD's public key for better security control.*

5. The Information Technology Services Department (ITSD) has earlier on looked into the security aspect of the two options, viz. filing of a return under the ESD Scheme by using a password vis-a-vis digital certificate. The department concluded that both options attain the same level of security by meeting the "strong encryption" requirements and protecting the session key against third party access. The use of a password as a signing device will not downgrade the degree of security.

CB(1)716/01-02(03)

Paragraph 4 of CB(1)716/01-02(03) started by referring to the method of authentication, but went on to discuss the *"... level of security for the data transmitted over the Internet ..."*. The fact that the taxpayer's password is encrypted by a different set of randomly generated numbers and IRD's public key does nothing to enhance **transmission security**; encrypting the password merely protects the taxpayer's password so that it is not revealed even should someone gain access to the message. Whether the password is encrypted or not does not change the nature of the means of authentication.

The conclusion by the ITSD as described in paragraph 5 of CB(1)716/01-02(03) *"...the department concluded that both options attain the same level of security by meeting the "strong encryption" requirements and protecting the session key against third party access"* is not incorrect, in that neither the use of password or digital certificate has any bearing on the system "*meeting the "strong encryption" requirements and protecting the session key against third party access".*

In our view, therefore, the considerations on the security requirements to date may be flawed, and that the question of whether the means of authentication chosen is adequate should be assessed separately from the method used to protect data during transmission.

2: Current use of password as means of authentication

Security aspects
7. The Administration has also pointed out that the use of a password for authentication is widely adopted in the Internet especially for most internet banking services, and internet filing of tax returns with the use of a password for authentication has also been implemented in many other tax jurisdictions such as the United States, Canada and Singapore.

Ref: CB2/BC/12/01

There is no doubt that the use of passwords is wide-spread. However, it is also important to consider this in the proper context: the advent of electronic banking pre-dates the wide-spread use of more sophisticated means of authentication, such as digital certificates. That passwords were adopted for Internet banking does not automatically imply that this is good practice. In fact, at the time when banks launched Internet banking services, there was not a robust and mature Public Key Infrastructure to support such initiatives, and to subsequently enhance the many Internet banking systems that exist to support the use of digital certificates is a major and costly undertaking. These and other reasons (both technical and operational) resulted in the use of passwords still being wide-spread today.

It is important to recognise also that there had been significant security breaches of Internet Banking systems around the world, either as a result of deliberate hacker attacks or as a result of security design faults. Indeed, many Internet banking service providers had at times suspended such services. The UK tax authority had also suspended its Internet submission system as a result of security fault.

In our view, therefore, one has to constantly assess the security needs of a system and then select the appropriate security measures to adopt. That something has been the norm to date does not necessarily imply that it is suitable going forward.

3: The use of telephone network

Security aspects
8. As regards the submission of tax returns by telephone, the Administration has advised that the public telephone network is considered to be a "trusted network" and is widely used by banks and public utilities companies for conducting electronic transactions. It is extremely difficult to hack into a telephone network system, and having regard to the nature of data transmitted through the telephone lines, the chance of security risk should be remote. Again, telefiling has been adopted by other tax jurisdictions including the United States, Canada, Australia and Singapore.

Ref: CB2/BC/12/01

When assessing the risks to a system, it is essential to consider the broader risks and not just focus on one particular aspect. It may be true that telephone systems cannot be hacked into easily. However, it remains a fact that PABX systems in general can be compromised. Further, it is not sufficient to be concerned only with data compromise as a result of external attacks. In many case, the aim of the attack may be to cripple the system (as was the case with the DoS attacks in the past). In this respect, the telephone system is not immune: recent complaints over the apparent inability of the telecommunications network to deal with the volume of calls made when the No.8 Typhoon Signal was last raised is a timely reminder.

Security risks aside, one also need to consider other issues such as availability. Given the strict deadlines for tax returns to be submitted, the relevant system will have to handle a surge of traffic within a relatively short period.

In our view, it is necessary to consider the implications in the event of the failure or long delays of either the telephone network or the backend systems to handle the transaction volume, such that returns are received beyond the deadlines or not at all. It would be good practice to plan for such eventuality, and to clearly establish the respective responsibilities of the IRD, ESD, and the individual taxpayers prior to such events occurring.

4: Specific security design

ADMINISTRATIVE MEASURES: Authorization and Authentication Control
12. All password information will be stored in encrypted format. The generation of the encrypted password from its 6-digit format involves the use of a strong encryption algorithm with a 128-bit encryption key. The encryption key will be specified by a Deputy Commissioner of Inland Revenue and no person other than him knows this encryption key.

CB(1)716/01-02(03)

We strongly recommend against the manual selection of any encryption key. A manually selected key is inevitably weaker than a system generated one.

5: System security review

We support the inclusion of access control feature within the telefiling and ESD systems, and that such access and transactions logs will be reviewed regularly. We would recommend that the related systems be subject to regular security review, preferably by an independent third party. Further, prior to the systems being launched, the security design should also be subject to an independent review.

Appendix 2:

Proposed Amendments to the Inland Revenue (Amendment) (No. 2) Bill 2001

The following suggested amendments are designed to clarify the meaning of some of the technical language currently used within the proposed ordinance.

Section 2

2 (a) Interpretation

"password" means any combination of letters, characters, numbers or other symbols selected by a person and ~~approved~~ conform to policies and standards prescribed by the Commission for use in systems designated by the Commissioner for the purpose of authenticating the person's identification in communicating with the Commissioner;

Section 6

6 The Commissioner may by notice published in the Gazette specify requirements as to---

(a) the manner of generating or sending an electronic record or any attachment required to be furnished with an electronic record;

(b) how a digital signature or password or any other ~~signing device~~ means of authentication is to be ~~affixed~~ used to authenticate a return furnished under this section; and

(c) the software and communication in relation to any attachment required to be furnished with an electronic record.

Section 7

7 The Commissioner may ~~approve a~~ prescribe the password policies and standards and to designate any system in respect of any communication with the Commissioner for the purposes of this Ordinance.

Additional Recommendation

In addition, when two contracting parties agree to make use of a particular means of authentication in support of transacting business electronically, both parties are in fact consenting to the other making a particular presumption: that if one party receives a electronic message that conforms to the specific requirements previously agreed (e.g. a message sent using valid a user-id and password - such as a customer using an on-line banking system to initiate a transfer of funds), then in the absence of evidence to the contrary, the receiving party has the right to accept the message as proof of the other party's authorisation, etc., and both parties will be commercially bound.

As such, it is highly desirable to clearly specify such presumptions.

The proposed amendments to the Schedule 1 of the **Import and Export Ordinance** (extracted below) is a very good and clear example of how such presumptions, and should be adopted by the IRD for use within the Inland Revenue (Amendment) (No. 2) Ordinance 2001.

Extract from Proposed Amendments to Schedule 1[s. 2] of the IMPORT AND EXPORT ORDINANCE

[Note: words in square brackets represent annotations by the HKSA to illustrate how the proposed clauses can be applied to the IRO with the minimum of changes.]

Section 2B is repealed and the following substituted -

"2B. Presumption regarding information sent using services provided by specified body

(1) Where information received by the Commissioner or the Director was sent using services provided by a specified body [such as the ESDLife portal], evidence which shows that the identity of the sender of the information was authenticated by the use of a security device [in this case a user-id and related password that conforms to the policies and standards prescribed by the Commissioner] is, in the absence of evidence to the contrary -

(a) proof that the person issued with the security device furnished the information [thus binding the electronic return to the sender]; and

(b) proof that the person issued with the security device made a statement or declaration contained in the information [thus binding the sender to his declaration].

(2) Where information received by the Commissioner or the Director and sent using services provided by a specified body was sent by a specified agent [thus allowing the submission of a return by an agent of the taxpayer] who has obtained an authorization in accordance with section 2D -

(a) a person named in the information as the person who furnished the information is, in the absence of evidence to the contrary, regarded for the purposes of this Ordinance as the person who furnished the information; and

(b) a person named in the information as the person who made a statement or declaration contained in the information is, in the absence of evidence to the contrary, regarded for the purposes of this Ordinance as the person who made the statement or declaration.".

3. Safekeeping of security device

Section 2C is amended by repealing everything after "device -" and substituting -

"(a) shall not authorize or allow any other person to use the device in connection with the sending of information to the Commissioner or the Director under this Ordinance using services provided by a specified body [thus stating that only the taxpayer can use his/her security device for the submission of tax return];

(b) shall take all reasonable steps and exercise due diligence to prevent any other person from using the device in connection with the sending of information to the Commissioner or the Director under this Ordinance using services provided by a specified body. [thus stating the obligation of the taxpayer to keep his/her user-id and password secure]".

We strongly recommend that similar language should be added to the IRO in relation to the use of user-ids and passwords and other means of authentication (e.g. passwords for telefiling).