For Information
on 8 December 2008

Legislative Council Panel on Information Technology and Broadcasting

Information Security

Purpose

This paper informs Members about the progress of Government's information security enhancement programmes.

Background

2. Since mid-April 2008, a number of cases involving leakage of personal data in Government bureaux/departments (B/Ds) have caused public concern over the level of information security in the Government. At the Special Meeting of the Panel on Information Technology and Broadcasting (ITB Panel) on 30 May 2008, we briefed Members on the experience gained from these incidents and the enhancement programmes that the Government will pursue. The aim of these programmes is to better protect personal and sensitive data and to ensure that B/Ds comply with the provisions of the Personal Data (Privacy) Ordinance requiring them to take all practical steps to prevent unauthorised disclosure of personal data.

Progress of Information Security Enhancement Programmes

3. The immediate focus of the Information Security Enhancement Programme has been on measures to address the risks highlighted by recent incidents. We are also examining measures to enhance the way in which information security is managed and assured over the longer term.

4. The more urgent activities of the enhancement programmes cover four main areas, namely staff awareness and education, technical and procedural measures, security compliance checking and the review of security regulations, policies and guidelines. We recognise that additional attention should be paid to enhancing staff awareness and education in order to facilitate their compliance with the information security requirements. We have also facilitated B/Ds to acquire additional tools and implemented technical solutions in order to minimise the security risk exposure due to external threats as well as reduce the temptation for staff to compromise the protection of sensitive or personal data. The following paragraphs describe the progress of the enhancement programmes in detail:

*(i) **Staff Awareness and Education***

5. We have accorded high priority to help staff to acquire the knowledge and understanding of data security measures and the need to adopt suitable security mechanisms. We have developed a staff communication programme to reinforce information security for all levels of staff in the Government, issued additional guidelines to provide better understanding and advice on good practices, and conducted a series of seminars to provide updates on developments on information security related matters.

(a) <u>Staff Communication Programme</u>

6. The success of improving data protection relies on staff to comply with the information security requirements. The Office of the Government Chief Information Officer (OGCIO) has engaged an external communication agent to develop a one-year campaign to help Government staff build up and sustain a high level of awareness, working knowledge and good practices, and a commitment to safeguarding sensitive and personal data. The new communication programme will cater for the needs of different stakeholders groups at various levels of responsibilities, including policy makers, departmental management and administrators, IT professionals, end-users and

departmental IT security officers in B/Ds. A variety of communication vehicles and channels[1] will be employed to suit different target groups.

(b) *Reminders and Guidelines to Enhance Staff Awareness*

7. The use of unauthorised software creates a risk of accidental disclosure and subsequent misuse of sensitive or personal data. Government staff are not allowed to use unauthorised software. The OGCIO issued a circular in July 2008 to advise Heads of B/Ds about technical and procedural measures they can use to secure compliance with this rule.

8. To highlight the best practices on information security to different stakeholder groups of senior management, supervisors and front-line staff, the OGCIO has contributed articles on information security topics written in laymens terms to the Civil Service Newsletter which has a wide circulation among civil servants. We have also included key messages on the prevention of data leakage in information leaflets and posters accessible to large numbers of staff.

(c) *Staff Training*

9. The Internet is full of fast changing security threats. It is important that staff keep themselves abreast of the latest IT security issues and developments, technical solutions available in the market to mitigate risks. Since May 2008, the OGCIO has arranged seminars and demonstrations for over 700 relevant staff from 80 B/Ds on topics like data encryption technology, security protection of portable electronic devices, and security measures for staff working outside the office. We have also conducted eight staff induction classes for 200 Executive Officers who are deployed to various B/Ds where their jobs would often require them to handle sensitive or personal data.

10. Besides centrally organised security seminars and training, the OGCIO has assisted many B/Ds to customise training material for their staff to suit their operational needs.

[1] These include publication, training (including e-training, training kits), quiz, promotion videos, smart reminders, best practice forum, management sponsored activities and showcases, etc.

(ii) ***Technical and Procedural Measures***

(a) *Staff Working at Home*

11. In order to achieve work/life balance, many hardworking staff wish to use technology to enable them to do some work at home instead of spending even longer hours in the workplace. A secure working environment is essential to the protection of sensitive and personal data whenever staff work at home. The OGCIO has recommended technical and procedural measures including hardware, software and services available to B/Ds to enhance information security for staff working at home. We have also facilitated them to acquire and implement solutions to improve the protection of computer systems, portable devices, networks and data.

(b) *Prevention and Detection of Breaches*

12. To assist B/Ds that require more sophisticated solutions to meet higher or specific data protection needs, the OGCIO has established close liaison and collaboration with industry bodies and vendors to receive their latest technology updates and technical solutions on data protection. The OGCIO is also evaluating the feasibility of implementing solutions as a central facility to detect violation of security policies or to reduce the chance of users accidentally disclosing the identity of their data subjects through emails or the use of file sharing software.

(iii) ***Strengthening the management arrangements to assure compliance and to provide advice and support to B/Ds, public bodies and NGOs***

(a) *Compliance Audits and Follow Up Actions*

13. All the recent data leakage incidents have involved some form of non-compliance with the information security requirements.

Government requires B/Ds to carry out security risk assessments of their information systems at least once every two years in order to reduce the risk of non-compliance. To assure that these reviews are carried out and to provide B/Ds with an independent view and suggestions for further enhancements, a centrally managed security audit exercise was mounted in May 2007. The latest audit findings show that all B/Ds that have the need to store sensitive data on portable electronic devices have used encryption techniques to protect the data. They have also set up proper procedures for reporting of data loss arising from the use of portable electronic devices.

(b) *Public Bodies*

14. The OGCIO has made special arrangements to facilitate B/Ds and the relevant public bodies under their purview to exchange information and coordinate the implementation of appropriate protection measures against information security exposures in support of major events, for example during the Equestrian Events for the Olympic and Paralympic Games in August and September 2008. We have regularly advised B/Ds who have purview over public bodies to share the relevant policy, guidelines and technical information related to information security with the public bodies to enhance their security posture. For example, in a seminar organised as part of the "Hong Kong Clean PC Day" campaign held in November 2008, over 20 public bodies and 90 SMEs have participated.

(iv) ***Review of Information Security Regulations, Policies and Guidelines***

(a) *Incident Reporting and Notifying Affected Data Subjects*

15. Government has reviewed and updated the existing regulations and policies concerning the handling of security breaches involving sensitive and personal data. Whenever there is a security incident involving personal data, the B/D concerned is required to report the incident both to the Office of the Privacy Commissioner for Personal Data and to the Government Information Security Incident Response Office. Moreover, the concerned B/D has to notify the affected

individual(s) as far as practicable. Exceptions to these rules and procedures are permitted only where there is an overriding public interest consideration, such as a specific risk that the prevention or detection of crime would be compromised. Any such exception requires the personal approval of the Head of B/D. The revised regulations and procedures were promulgated in November 2008.

Findings from the Incidents and Recommendations

16. In the special ITB Panel meeting held on 30 May 2008, Members were briefed on the data leakage incidents and remedial measures taken by the concerned B/Ds and public bodies. The investigations conducted by the relevant parties have shown that none of the incidents had involved malicious or criminal intent such as data theft; the underlying cause was that the concerned staff had not exercised sufficient care and applied prudence in handling the sensitive or personal data.

17. To prevent future occurrences of this kind of security incident, all B/Ds have been required to review their rules for the protection of sensitive and personal data. They have arranged training and promotion programmes to enhance staff awareness, and strengthened their system and technical environments. There is also room for further stepping up the technical and procedural measures to tighten the protection of information assets and facilitate staff to work in a more secure environment. The OGCIO has incorporated the necessary follow up actions into the enhancement programme as described in the preceding paragraphs.

Risk Assessment by B/Ds

(a) *Top Management Support*

18. Creating a culture that protects personal and sensitive data requires top management concern and support. To ensure that B/Ds accord sufficient and high level attention to uphold a high standard of

information security, the Government Chief Information Officer (GCIO) briefed Heads of B/D on the importance of information security and on their personal responsibility to assure this. The OGCIO has also arranged briefings for forty top management staff from various B/Ds by a member of the team that reviewed lessons to be learnt from the loss by the UK Government of personal data concerning several million UK residents.

(b) *Security Risk Assessment*

19. The GCIO has also asked Heads of B/Ds to carry out a special risk assessment on security provisions for their staff in handling personal or sensitive data, including working outside of the office environment. The Heads of B/D have also been requested to work out improvement programmes to avert any identified risks.

20. As a result, B/Ds have worked out appropriate follow-up actions to mitigate identified risk factors. These include, for example, "belief that security breaches will not be detected and punished", "temptation to work on sensitive data at home without authority", and "lack of awareness of the importance of data protection and the associated rules". Based on their assessment, B/Ds have worked out follow-up measures as listed in **Annex-1**.

Update on recent data leakage incidents

21. Since the last status update at the Special Meeting of the ITB Panel on 30 May 2008, the concerned B/Ds have taken rectification measures and adopted suitable risk mitigation safeguards to prevent re-occurrence of incidents. In particular, the Hong Kong Police and Hospital Authority have provided their individual progress reports on the improvements made in **Annex-2** and **Annex-3** respectively.

22. Since that meeting, there have been five new cases of data leakage reported to the Government Information Security Incident Response Office. As with previous cases, these have involved the loss of USB storage devices and the leakage of data through file-sharing software installed on officers' home computers. The B/Ds concerned

have informed the data subjects as far as practicable and taken necessary follow up actions. All cases have been reported to the Privacy Commissioner for Personal Data. Details of these cases are in **Annex-4**.

Information Security in the Community at Large

(a) Information Security Reference Resources

23. Government has taken measures to inform the public about ways to protect their computer resources and information assets. The OGCIO has published security policies and guidelines adopted within the Government on the one-stop information security portal (www.infosec.gov.hk) to share them with the community at large. Public bodies and the private sector can also make reference to them when enhancing their own security provisions.

(b) Teenager Groups

24. Since early 2008, in collaboration with the Police Force school ambassador, the OGCIO have partnered with some professional security associations and visited 30 schools and delivered appreciation courses, provided advice on ethical use of IT and the Internet and information security to over 7,000 teachers and students. Through this activity, we aim to help nurture greater security awareness and a more responsible computer user culture among the younger generation.

(c) Business Enterprises

25. The OGCIO continues to collaborate with Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) run by the Hong Kong Productivity Council, professional security organisations and industry bodies to promote information security to the business enterprises, in particular the SMEs. OGCIO will also provide sponsorship to HKCERT in 2009 to enhance its computer emergency support services to the community.

Conclusion and next steps

26. Information security management is an ongoing process and requires the commitment and attention of everyone. Security challenges continue to exist due to technology advancement, emerging threats and also changing user behaviour and the increasing popularity of social networking. The Government will spare no effort to uphold our security posture and policies, regulations and practices, and helping all staff to comply with the security requirements in handling sensitive or personal data. To keep Members apprised of the progress of our various initiatives on information security and data protection, we plan to provide an annual update to the ITB Panel on the progress of existing and planned initiatives.

27. Technological solutions can make a significant difference to the management of security risks, but their deployment and use requires careful planning and their impact is usually longer-term. The OGCIO will evaluate the case for central or departmental deployment of technologies that could assist B/Ds to manage information security more effectively. These include technologies mentioned in paragraph 12 above as well as those that make it easier for users to manage access rights to electronic documents that contain sensitive or personal data.

28. The OGCIO will continue to assist B/Ds in ensuring continuous improvement in information security management such as adopting tools for evaluating information security management techniques.

Advice Sought

29. Members are invited to note the contents of this paper.

Office of the Government Chief Information Officer
Commerce and Economic Development Bureau

December 2008

Annex 1

ITB Panel Meeting on 8 December 2008

Risk Assessment Performed by B/Ds and Improvement Measures Initiated

All B/Ds have carried out a risk assessment exercise and worked out improvement programmes to avert any identified risks in response to OGCIO's request. A memo on "Risk Assessment for Processing, Storing and Viewing Personal/Classified Data Outside Office Environment" was issued by GCIO to Heads of B/Ds on 15 July 2008.

2. B/Ds will carry out individual improvement measures to avert the risks identified. They are fully aware of the risks and are actively preparing/implementing the enhancements necessary to raise their security posture. There are a number of improvement measures in common as indicated by B/Ds in their returns. The measures are in line with the overall enhancement programme as summarised below.

Security awareness promotion and training

3. B/Ds have organised many activities to promote staff awareness and training. They understand the importance of this area. Specific actions that have been or are being taken include -

(a) Conducting awareness training, workshops and internal briefings;
(b) Re-circulating of relevant rules and guidelines;
(c) Encouraging staff to attend security briefings and seminars;
(d) Providing of information packs and briefing for new recruits;
(e) Sending regular electronic messages to remind staff on security requirements;
(f) Using topical warning messages and screen savers to remind users.

Tightening on the control of work-at-home and the use of portable storage devices

4. B/Ds are aware of the risks of work-at-home and use of portable

storage devices. To facilitate a secure working environment and mitigate identified risks, they have/will set up various controls and/or procedures, including -

(a) Prior approval and recording is required for storing official data on portable storage devices and taking these away from office;
(b) Central control on the provision and use of USB storage devices;
(c) Maintaining an inventory list of all portable storage devices;
(d) Only equipment provided by the government can be used to store or process identifiable personal data;
(e) Enforcement of data encryption and erasure after usage for all portable storage devices;
(f) Surprise inspection of network and portable storage devices;
(g) Regular stock taking of portable storage devices.

Enhancement of IT facilities or resources

5. B/Ds are implementing or planning to implement technical solutions to enhance their security on protection of data, including -

(a) Encryption tools or USB storage devices with encryption features;
(b) Procurement of more notebooks/installation of virtual private network (VPN) solutions for staff to work outside office;
(c) Planning of IT infrastructural enhancement e.g. using "virtual workstation" concept;
(d) Implementation of centralised file servers or centralised managed departmental file encryption solution;
(e) Technical study on systems for detecting/prohibiting use of external web mail or other open facilities that may lead to potential breaches;
(f) Conduct testing on software to minimise the risk of leaking information through mobile phones;
(g) Implementation of end-point security solution or host-based protection software;
(h) Installation of data leakage prevention system or software to prohibit downloading, printing, sending and transferring of confidential information;
(i) Implementation of information rights management systems;

(j) Assigning more staff to oversee information security and data protection.

Review of policies and guidelines

6. Many B/Ds are conducting or will conduct departmental reviews of existing policies and guidelines to provide staff with clear instructions on the working procedures, including -

(a) Updating of policies on use of portable storage devices;
(b) Review of access control on sensitive data;
(c) Review of methods on processing, storing and viewing personal/classified data outside office;
(d) Expand the scope of the next IT security risk assessment and audit to review measures for processing, storing and protection of personal or classified data;
(e) Provision of clearer guidelines;
(f) Review of Internet access policy.

Annex 2

ITB Panel Meeting on 8 December 2008

Actions taken by the Hong Kong Police

Immediate Measures

1. Periodic Noticeboard messages to remind officers of the risk of using P2P software, culpable consequences of using unauthorised USB devices on Force computers, likely causes of computer virus infection, and other relevant information security tips. Since May 2008, a total of 15 such messages have been promulgated.

2. The setting up of a Force level Working Group in May 2008 to steer actions to identify the causes of data leakage and remedial measures to address the problem.

3. To strengthen the control of usage of USB storage devices, the Force has started procuring USB thumb drives with encryption on station charge for shared use by the junior officers since September 2008. The security standard of these thumb drives matches the standard required by the Government Security Regulations (GSR). They can store classified data up to the 'Restricted' level. A guideline on the correct use of Force issued USB thumb drives has also been issued for easy reference by all.

4. In tandem with the use of encrypted thumb drives, the USB ports on all Force Computers were "whitelisted" in September 2008 to ensure only registered USB devices are being used in Force computers. Controlling the usage of USB ports reduces the risk of unauthorised data transfer and computer virus infection. Statistics in October 2008 suggested a significant drop in virus detection at the local workstations.

5. The Force is purchasing 2,800 USB e-Cert encrypted thumb drives for storage of confidential information to comply with GSR. They will be issued to all Inspectorate officers and above on personal charge to enhance secure storage, processing, and transmission of confidential information.

6. Approval has been obtained from the Government Security Officer to allow Force members to transmit classified attachments up to the 'Confidential' level with e-Cert authentication via the PEN system.

7. A Forcewide common terminal sanitisation exercise, followed by a security audit, was conducted between June and July 2008 to remove all Force common terminals of personal, sensitive and/or classified data etc. The second audit will start in late December 2008.

8. To strengthen its IT security framework, the Force has made references to the overseas experience by learning from the study of the National Policing Improvement Agency (NPIA) on classified data handling procedures, the Poynter Review of HM Revenue and Customs (HMRC) on protection against data loss, and the Hannigan Report for UK Cabinet Office on government data handling procedures.

9. The setting up of Work Improvement Teams in October 2008 at Formation level and Working Groups at Regional level to assess operation needs, to seek feedbacks from officers and to make improvements on the measures introduced.

Long Term Solution by Implementation of Virtual Workstation (being considered)

10. To establish a data-centric infrastructure instead of the current system-centric approach for better data protection information security.

11. Deployment of desktop virtualisation facilities and central data storage/processing for users, with remote access and highly restrictive data download.

Training

12. Force-wide training on information security will continue to be provided to all officers to raise their awareness on the need to always ensure information security and data protection.

13. For the benefits of frontline Formations, regular outreach programmes by the Police Headquarters Information Systems Wing will continue to update officers on the do's and don'ts necessary to heighten information security and to address their concerns in situ. 13 similar visits have been held since March 2008.

14. Conducting briefings for trainee officers on matters of information security and data privacy before their graduation.

15. Conducting training for all Force system security managers who have a duty to ensure the compliance of all information security rules. Between October and November 2008, more than 200 such officers of Chief Inspector and Superintendent ranks have been trained. This course will continue.

16. To keep officers abreast of IT developments and good practices on information security, speakers, overseas or otherwise, have been invited along to share their experience with the Force. On 26 November 2008, for example, three guests of PricewaterhouseCoopers lectured the Force on 'Managing and Safeguarding Sensitive Information'. More than 200 officers attended.

17. An action plan to enhance officers' awareness on the protection of personal data, through education and training has been introduced. The plan incorporates 11 awareness enhancement programmes, such as poster design competition, seminars and roadshows, and its first program was launched in early November 2008.

18. On 14 November 2008, the Privacy Commissioner for Personal Data conducted a seminar for the Force on "Protection of Personal Data", focusing on the legal framework, data protection principles and the governance of data protection.

19. A seminar on "Compliance of Personal Data (Privacy) Ordinance" was delivered to the Force by a Chief Personal Data Officer and a Senior Personal Data Officer on 25 November 2008. Over 300 middle ranking disciplined and civilian staff attended.

20. A training day package, designed to nurture a change culture in junior officers on data protection, has been produced and will be rolled out Forcewide in February 2009.

21. The Force IT Society organised two workshops on system security of personal computers at the Police Sports Recreation Club (PSRC) on 15 November. An IT security professional from the private sector was invited to talk on how to enhance Force members and their family's awareness of information and network security of their personal computers. Between 20 and 26 November 2008, the Society also conducted a roadshow on information security of personal computers at the PSRC for the benefits of Force members and their families.

Hong Kong Police
December 2008

Annex 3

ITB Panel Meeting on 8 December 2008

Actions taken by the Hospital Authority

Purpose

This note briefs Members on actions taken by Hospital Authority (HA) since last meeting on 30 May 2008 regarding the series of security incidents involving loss of portable electronic storage devices containing identifiable patient data.

Background

2. In early May 2008, 10 incidents of loss of portable electronic devices which contained patient data had been reported. Concerned with the protection of patient data, the Chief Executive of HA (CE/HA) announced the formation of the HA Task Force on Patient Data Security and Privacy (Task Force) to conduct a review on the existing policies and security system on patient data protection and to recommend improvement measures. Following completion of its work, the Task Force submitted its report to the CE/HA on 5 August 2008.

3. In May 2008, the Privacy Commissioner for Personal Data (PCPD) initiated a series of investigations after receiving reports on data loss incidents in the HA. The inspection of the HA's Personal Data System was carried out at Ruttonjee and Tang Shiu Kin hospitals by the PCPD. PCPD published an Inspection Report on 22 July 2008.

4. The HA Task Force and PCPD made 26 and 37 recommendations respectively on eight areas covering the HA's policy, structure and people, staff awareness and training programme, procedures and guidelines, privacy impact assessment and containment, audit, contracts and technology. The major findings and recommendations from the HA task Force and PCPD are detailed in paragraph 5 to 8 below.

Major Findings and Recommendations from PCPD

5. PCPD recognises that important and significant efforts have been made by the HA to devise a patient data system that facilitates medical care while safeguarding data security. The HA has good and detailed policies in place, but the implementation and coordination is only fair to satisfactory. More efforts are required in monitoring compliance and performing systematic security audit. Furthermore, the general level of privacy awareness shows need for improvement

6. PCPD has made 37 recommendations focusing on the development of more user-friendly security policy & guidelines, examination of the possibility to minimise the use of HKID No. on reporting and data download, implementation of more effective and systematic privacy audit and further raising staff awareness on data security and privacy.

Major Findings and Recommendations from the Task Force

7. In its report, the Task Force recognises that the HA's adoption of new technologies has contributed to important improvements in the quality of healthcare provided, but that it comes with attendant security and privacy risks to patient data. Over years the HA has taken considerable steps to identify and address these risks. Nevertheless, based on their assessments of the lessons to be learnt from the data loss incidents and of HA's Personal Data systems for the protection of patient data, the Task Force believes that more work needs to be done to sustain and enhance the effectiveness of these measures.

8. The Task Force has made 26 recommendations of specific actions to be taken in the areas of Policy, Structure and People, Procedures and Guidance and Technology that are designed to help HA continually improve its information security and privacy measures.

Proposed Action Plan and Progress

9. At the Administrative and Operational Meeting of the HA on 10 September 2008, the HA Board was briefed on the overall findings and recommendations of the reports from the Task Force and PCPD. It also endorsed HA's proposed action plans for addressing these recommendations to further enhance protection of patient data security and privacy. The action

plan with 19 consolidated targets covers the eight areas as mentioned in paragraph 4 above. HA plans to take 12-18 months to complete the targets of the action plan.

10. The following summarises the key actions that have already been taken or are underway in the next 3-6 months:

(a) HA's patient information system has been upgraded so that downloaded patient data with identifiable patient and personal information (including names and identity card numbers) will be protected through encryption;

(b) Mandatory use of advanced USB flash drives with encryption and password 'lockdown' has been introduced for protecting patient data;

(c) System has been enhanced to print a label "Confidential" onto printouts given to patients containing personal data

(d) Appoint the Corporate Information Security and Privacy Officer (CISPO) to head a new HA Office for Information Security and Privacy, establish the HAHO Information Security and Privacy Committee and develop a new one-page HA-wide Information Security & Privacy Policy

(e) Strengthen contractual obligations of information security and privacy placed upon third-parties

(f) Review and reduce number of accounts with access rights of downloading of patient data in major IT systems

(g) Review and reduce the use of HKID / Name in data downloading & printouts

(h) Implement a central email server for clusters supporting secure email as effective alternative of the use of portable storage devices for data transport

(i) Review and strengthen PC security and administration controls

11. It is planned that the remaining action plan targets will progressively be completed in 2009/10.

Hospital Authority
December 2008

Annex 4

ITB Panel Meeting on 8 December 2008

Summary of data leakage incidents in Government since Jun 2008

No.	Incident Date	Bureau/Department	Summary of the Incident
1	2008.06.13	Customs and Excise Department	Local news reported that one statement record from C&ED was found through FOXY. C&ED confirmed it was an internal document of C&ED. The statement includes the name, ID of the customs officer as well as the details of the case, including the name and HKID no. of the suspect.
2	2008.06.24	Census & Statistics Department	A USB thumb drive personally owned by a Census and Survey Officer was lost. The device contained some internal information of business establishments collected in a survey. The two affected business establishments were subsequently informed and accepted the Department's apology.
3	2008.07.06	Immigration Department	Local news reported that sensitive data belonged to the ImmD was searchable on the Internet through FOXY. The information consisted of 11 documents related to Immigration Department. Three affected visitors were not informed (due to insufficient contact information). Privacy Commissioner was informed.
4	2008.08.08	Hong Kong Police Force	Local news reported the leaking of internal information of HKPF to FOXY network. The leak involved five copies of documents, including those believed to be Police internal orders for operations against gambling and violent robberies.
5	2008.09.25	Social Welfare Department	Two personally owned USB flash drives were lost. Both of them with password protection. One of them stored publicity information while the other one contained about 63 clients' personal information. 109 data subjects were affected. The personal data generally include the data subjects' names, addresses, and case file reference numbers. Privacy Commissioner was informed.