



Second Session, 39th Parliament

REPORT OF PROCEEDINGS
(HANSARD)

SELECT STANDING COMMITTEE ON

PUBLIC ACCOUNTS

Victoria

Wednesday, May 26, 2010

Issue No. 7

BRUCE RALSTON, MLA, CHAIR

ISSN 1499-4240

**SELECT STANDING COMMITTEE ON
PUBLIC ACCOUNTS**

Victoria
Wednesday, May 26, 2010

- Chair:* * Bruce Ralston (Surrey-Whalley NDP)
- Deputy Chair:* * Douglas Horne (Coquitlam-Burke Mountain L)
- Members:*
- * Rob Howard (Richmond Centre L)
 - * Richard T. Lee (Burnaby North L)
 - * John Les (Chilliwack L)
 - * Norm Letnick (Kelowna-Lake Country L)
 - * Joan McIntyre (West Vancouver-Sea to Sky L)
 - * John Rustad (Nechako Lakes L)
 - * Ralph Sultan (West Vancouver-Capilano L)
 - * Spencer Chandra Herbert (Vancouver-West End NDP)
 - * Kathy Corrigan (Burnaby-Deer Lake NDP)
 - * Guy Gentner (Delta North NDP)
 - * Lana Popham (Saanich South NDP)
 - * Shane Simpson (Vancouver-Hastings NDP)
 - * Vicki Huntington (Delta South IND)

** denotes member present*

Clerk: Craig James

Committee Staff: Josie Schofield (Manager, Committee Research Services)

Witnesses:

- Dave Campbell (Ministry of Citizens' Services)
- Duncan Campbell (Vancouver Coastal Health Authority)
- John Doyle (Auditor General)
- Malcolm Gaston (Office of the Auditor General)
- Bill Gilhooly (Office of the Auditor General)
- Stu Hackett (Ministry of Citizens' Services)
- Pam Hamilton (Office of the Auditor General)
- Chris Hauff (Ministry of Citizens' Services)
- David Lau (Office of the Auditor General)
- Elaine McKnight (Ministry of Health Services)
- Dr. David Marsh (Vancouver Coastal Health Authority)
- Lorna Pritchard (Ministry of Finance)
- Colleen Rose (Office of the Auditor General)
- Cheryl Wenezenki-Yolland (Comptroller General)

CONTENTS

Select Standing Committee on Public Accounts

Wednesday, May 26, 2010

	Page
Auditor General Reports: Audit of Wireless Networking Security in Government, Phases 1 and 2	115
J. Doyle	
D. Lau	
S. Hackett	
Dave Campbell	
Auditor General Report: <i>The PARIS System for Community Care Services: Access and Security</i>	120
J. Doyle	
P. Hamilton	
Duncan Campbell	
D. Marsh	
Auditor General Report: <i>Electronic Health Record Implementation in British Columbia</i>	127
J. Doyle	
M. Gaston	
E. McKnight	
C. Wenezenki-Yolland	
Auditor General Report: <i>Follow-up Report: Updates on the Implementation of Recommendations from Recent Reports</i>	137
J. Doyle	
C. Rose	
C. Wenezenki-Yolland	

MINUTES

SELECT STANDING COMMITTEE ON PUBLIC ACCOUNTS



Wednesday, May 26, 2010

9 a.m.

**Douglas Fir Committee Room,
Parliament Buildings, Victoria, B.C.**

Present: Bruce Ralston, MLA (Chair); Douglas Horne, MLA (Deputy Chair); Spencer Chandra Herbert, MLA; Kathy Corrigan, MLA; Guy Gentner, MLA; Rob Howard, MLA; Vicki Huntington, MLA; Richard T. Lee, MLA; John Les, MLA; Norm Letnick, MLA; Joan McIntyre, MLA; Lana Popham, MLA; John Rustad, MLA; Shane Simpson, MLA; Ralph Sultan, MLA

Others Present: John Doyle, Auditor General; Cheryl Wenezenki-Yolland, Comptroller General; Josie Schofield, Manager, Committee Research Services

1. The Committee considered the Auditor General's Report No. 15, 2008/09: *Wireless Networking Security in Victoria Government Offices: Gaps in the Defensive Line* (first audit)

Witnesses:

- Bill Gilhooly, Assistant Auditor General, Financial Audit, Office of the Auditor General
- David Lau, Director, IT Audit, Office of the Auditor General
- Stu Hackett, Chief Information Security Officer, Ministry of Citizens' Services
- Dave Campbell, Director, WTS Chief Technology Office, Ministry of Citizens' Services,
- Chris Hauff, Director, Operations Network Services, Ministry of Citizens' Services

2. The Committee considered the Auditor General's Report No. 10, 2009/10: *Wireless Networking Security in Government: Phase 2*

Witnesses:

- Bill Gilhooly, Assistant Auditor General, Financial Audit, Office of the Auditor General
- David Lau, Director, IT Audit, Office of the Auditor General
- Stu Hackett, Chief Information Security Officer, Ministry of Citizens' Services
- Dave Campbell, Director, WTS Chief Technology Office, Ministry of Citizens' Services,
- Chris Hauff, Director, Operations Network Services, Ministry of Citizens' Services

3. The Committee considered the Auditor General's Report No. 7, 2009/10: *The PARIS System for Community Care Services: Access and Security*

Witnesses:

- Pam Hamilton, IT Support Specialist, Office of the Auditor General
- Duncan Campbell, Chief Financial Officer & Vice President, Systems Development & Performance, Vancouver Coastal Health
- Dr. David Marsh, Medical Director, Addictions, HIV/AIDS, Aboriginal Health, Vancouver Coastal Health

4. The Committee considered the Auditor General's Report No. 9, 2009/10: *Electronic Health Record Implementation in British Columbia*

Witnesses:

- Malcolm Gaston, Assistant Auditor General, Government and Accountability, Office of the Auditor General
- Elaine McKnight, Assistant Deputy Minister, Ministry of Health Services

5. The Committee considered the Auditor General's Report No. 11, 2009/10: *Follow-up Report: Updates on the implementation of recommendations from recent reports*

Witnesses:

- Colleen Rose, Manager, Communications, Office of the Auditor General
- Cheryl Wenezenki-Yolland, Comptroller General
- Lorna Pritchard, Director, Financial Management Branch, Ministry of Finance

6. The Committee deferred its consideration of the Auditor General's Report No. 13, 2008/09: *Public Sector Governance and How Are We Doing?*

7. The Committee adjourned at 11:58 a.m. to the call of the Chair.

Bruce Ralston, MLA
Chair

Craig James
Clerk Assistant and
Clerk of Committees

WEDNESDAY, MAY 26, 2010

The committee met at 9:03 a.m.

[B. Ralston in the chair.]

B. Ralston (Chair): We have a fairly ambitious agenda this morning, as you probably noticed. What I'm asking presenters to do is to try to keep their comments relatively brief. I think you can assume that members of the committee have read the reports.

I'm going to be suggesting this rough time allocation: 45 minutes for the first two reports; 20 minutes for the third report, report No. 7; an hour and a little bit for the electronic health record; and then the remainder for the final two reports. That will maybe be overly ambitious, but we'll see.

I'd then ask if the Auditor General could begin his presentation on agenda items 1 and 2.

**Auditor General Reports:
Audit of Wireless Networking
Security in Government,
Phases 1 and 2**

J. Doyle: Good morning, Members.

Wireless security. Wireless technologies have many benefits, but they introduce a whole new set of security risks. The security processes that should be in place are always moving because of that tension between those who want to get into our systems and those who are charged with the role of preventing that from happening.

Unfortunately, countermeasures tend to lag slightly behind the assessment of vulnerabilities. Wireless networks require the same security principles as regular networks, but they also pose some unique threats.

[0905]

The most insidious risk is that information can be captured without the computer users even knowing it. Therefore, a strong defensive security line is needed, and that line needs to be regularly checked for gaps, to protect the systems and the information inside that line.

We're going to go through two different reports today. In last year's audit on wireless security we focused on greater Victoria, all the government buildings, and we noted some serious gaps or apparent gaps in security. We then gave time to government for them to address those gaps before we published our findings. That was a new approach that we had adopted, for obvious reasons.

The second report is the second phase of the wireless security audit. This is where we actually went inside government buildings. We also expanded the review to different locations and into two educational institutions, SFU and BCIT.

Because we have a heavy agenda, I'm going to pass over to the team, but I'd just like to introduce, on my

left, Bill Gilhooly, who's the assistant Auditor General responsible for this aspect of work within the office, and on my right is David Lau, who is the IT specialist, the director responsible for the conduct of this work. Now I'll pass over to David to give you a brief overview of the work and our findings.

D. Lau: Good morning, Chair and Members. I would like to give a summary of what we did on those two audits — our findings, our recommendations and our future plans in this area.

There are many types of wireless devices. It is no longer just laptops or desktop computers that communicate with corporate networks. There are many others, such as smartphones, Bluetooth devices, e-readers, portable music players and even digital cameras. They all have the capability to send and receive data through the air. Wireless networking is a relatively inexpensive and easy solution to give anyone convenient access to the Internet or office networks almost anywhere they go.

Wireless networking has the same risks as wired networking, plus more. Data can be captured intentionally by those with malicious intent or intentionally by those that are just curious. The security of wireless devices can also be easily compromised if not set up properly. Unauthorized access point devices can be installed inside networks without anyone knowing it. The key risk of wireless networking is that all data can be read, altered or copied if the devices are not adequately encrypted. Equally worrisome is that user IDs and passwords can also be identified and used for illegal use or unauthorized access into networks.

Here is an example of the kit needed to carry out mobile scanning or wardriving. You just need a laptop; an antenna; scanner software, which can mostly be downloaded from the Internet free of charge; and some know-how, which is also available on the Internet. You can also download free software to interpret the scans as well as to crack some types of encryption codes.

This is a typical wireless access point that many people have in their homes. It is inexpensive and can be purchased from any electronics store. If the device is not properly configured, when someone brings one of these into the office and plugs it into the corporate network, it poses significant risk to corporate network security. For instance, if the appropriate data encryption is not enabled on a device, all data passing back and forth between the access point and the user's computing device can be intercepted by the hardware shown in the previous slide on wardriving.

In our first phase of this wireless security network audit, we did wardriving in greater Victoria areas outside government buildings. What we found was worrisome. Two-thirds of scanned wireless access points near government buildings used only modest encryption or none at all. Several government sites were receiving or broadcasting information with no encryption. One-third of

access points near a health authority site had no encryption. Government's wireless security policies weren't up to date. This led to our second audit, where we broadened the scope horizontally and vertically.

In our second-phase audit, we selected five ministries and increased the number of government offices visited in the greater Victoria area and in other cities. We included two post-secondary institutes, SFU and BCIT. We did similar wardriving and scanning for signals.

[0910]

This time we did it both inside and outside government buildings. We did the same at SFU and BCIT campuses. In total, we captured over 7,000 signals.

In order to determine whether those signals belonged to the government, we then cross-referenced the captured signals to internal IP addresses and device locations provided by those entities. We also used some specialized applications and specially designed Excel spreadsheets to map and analyze the captured data. We also used conventional audit techniques, including interviewing all key IT staff members and reviewing the document policies, standards, policies and monitoring reports.

In both audits we did not review other wireless technologies, such as PDAs, cell phones or Bluetooth, as they involve different technology and operating standards.

In our second-phase audit we found that the government has implemented many of the recommendations from our first audit. Comprehensive policies, standards and procedures have been developed and adopted. The wireless access devices installed by government in greater Victoria were adequately secured.

However, we found many questionable signals outside the greater Victoria area. We also noted that the government needs to do a better job in monitoring wireless networking activities, ensuring that no unauthorized access points are being installed and ensuring compliance with established security policies.

We recommend that the government, through the office of the chief information officer, establish procedures to monitor policy compliance, update job descriptions of key IT personnel, improve monitoring and detecting of wireless network activities to a real-time basis and keep an up-to-date inventory of wireless access devices.

For SFU and BCIT we found that all of the wireless access devices installed by SFU and BCIT were well-secured. However, both need to improve their policies and standards in wireless networking. They also need to improve management and monitoring of wireless operating activities. SFU needs to strengthen the governance structure of the IT division and establish clearer rules and responsibilities in IT security oversight.

Looking ahead, wireless networking technology is definitely here to stay and will continue to expand. Government is also likely to continue to expand its use of the technology. Therefore, we are planning to embed this type of review on a rotational basis across

the government reporting entity as part of our annual financial statement audit. We also plan to examine the security of audit wireless technologies in the future.

B. Ralston (Chair): Thanks very much. That was admirably concise.

I believe we have witnesses Dave Campbell and Chris Hauff, but perhaps Mr. Hackett would like to introduce them. I'm not sure what arrangement has been made.

S. Hackett: Thank you, Chair, Members. My name is Stu Hackett. I'm the chief information security officer for the province of B.C., with the office of the chief information officer. Today to make this presentation there's Dave Campbell. Dave is the director of IT security operations in Shared Services B.C. And with us, as well, is Chris Hauff. Chris Hauff is a director of network infrastructure, I think, in Shared Services B.C.

With that, I'll turn it over to Dave to make his presentation.

Dave Campbell: Good morning, Chair, Members. We are presenting our response to both reports that were presented by David. You have sufficient background. We received the reports. We did provide some response. The Auditor General graciously allowed us to close some of the gaps before making them public, which was obviously wise, given that we were telling people what our security posture was.

[0915]

In the most recent report, it stated that government has made some progress in securing its wireless network environment. We've adopted more comprehensive policy standards and procedures, and the overall conclusion was that security around government's wireless infrastructure is generally adequate. However, there's some work to do.

There was a total of four recommendations in the February report. We have implemented three of them fully, and one recommendation has been partially implemented. Reconfiguring, upgrading and replacing any of their wireless devices that were found without encryption has been fully implemented. There were three circuits. These circuits were used as backup circuits as part of business continuity for PEP and two other agencies. They have been shut down and replaced with terrestrial circuits.

Having ministries review their wireless access points. The office of the chief information officer directed all ministry CIOs to review their wireless access points. That has been done, and the findings were reported to the government CIO.

Review of security policies and guidelines has been completed, and that information has been published as well as the cryptographic standards.

Regular monitoring of wireless computing practices is being implemented. This is a fairly intense and very

costly endeavour. We are implementing a number of systems that will allow us to do this more fully as part of our payment card industry security standard compliance, which is underway now and will be substantially complete by this time next year.

In the March 2010 report there were five recommendations, three in the area of maintaining effective management of security. One has been fully implemented, one partially, and one is being currently addressed. Both the recommendations in the area of monitoring wireless security are being currently addressed.

Policies relating to wireless network security. Ministries are required to complete an annual information security review, and Shared Services B.C. is assessing the feasibility of implementing technology which will add to our control and provide visibility in reporting in order to support the government's IM/IT policies.

Recommendation update — the job descriptions. The key job descriptions, as mentioned, have been reviewed to ensure they meet current requirements. We're looking at making an annual review of these job descriptions part of the supervisors' EPDP.

Development of a network access control solution. This work is underway. We're currently undergoing a proof-of-concept at Shared Services B.C. headquarters at 4000 Seymour. That proof-of-concept will be complete in June, and it will help us to determine the effort and the cost required to implement the solution across government.

Implementation of mechanisms to scan and confirm that only properly configured devices are able to access the network. This will be addressed by network access control, which will prevent unauthorized devices from being able to connect to the government network.

Development of an inventory with a list of authorized wireless access devices. Shared Services B.C. currently maintains an inventory of network devices, including authorized wireless access devices.

[0920]

Our next steps. We will complete the network access control proof-of-concept, and Shared Services B.C. will seek funding approval to implement the recommended solution. The office of the CIO will continue to work with Shared Services B.C. and the ministry chief information officers to identify areas of risk and ensure compliance with policy, etc.

B. Ralston (Chair): Thanks very much. It's over to the members of the committee for questions.

S. Chandra Herbert: Thank you so much for the presentation. Just a quick question. I wondered if you could provide some background. When an organization, say a ministry, contracts with a non-profit, for example, to do some of their functions, would they be caught up in this review around privacy, security of information,

that kind of thing? I'm just thinking of some non-profits which really are very bare bones and might not have information officers, for example, to look after this kind of thing.

Dave Campbell: The short answer is: I don't know. We don't have control of the infrastructure for those organizations. I believe that through the contract provisions there is a requirement to adhere to government policies, which would include the wireless security, etc. But I don't know how that is enforced.

B. Ralston (Chair): I don't see anyone. I have a question, then. There are levels of encryption that you speak of. What's the process for monitoring encryption? I understand that this is an evolving field and that what may be effectively encrypted at one stage may become outmoded fairly rapidly. What's the mechanism? The Auditor General may wish to comment on this. What's the ongoing mechanism proposed for monitoring encryption?

Dave Campbell: We work very closely with the office of the CIO on standards. We currently use the highest encryption available for our wireless access points, and as that technology and as the threats develop, we constantly work with our suppliers to ensure that we at least have the best security available at that point.

As for monitoring, one of the tools we are implementing for the payment card industry security will ensure that no device on our network can be reconfigured without our knowledge. We have reasonable control over the configuration today. But you know, mistakes happen, and things change, so it is possible that a device that's fully encrypted today can be unencrypted by mistake. Going forward, that will be prevented by this monitoring solution.

K. Corrigan: I am wondering if, during this audit, there were any glaring gaps that revealed that there was particular information that was being accessed. Would this audit reveal that? Was it found that there was any information that had been compromised that was of a sensitive nature or otherwise?

Dave Campbell: I believe not, but I should let the Auditor General answer that question.

J. Doyle: Thank you for the question. One of the problems has been that you can't detect footprints. So if someone had come in and extracted information with the level of monitoring that was going on, it would be very difficult to determine, first, that they'd been there and, second, what had been removed. Hence, the reason that when we detected the weaknesses, we communicated very, very quickly with government in regard to our findings,

and they acted almost immediately in developing processes so that the stable door, if you will, was well and truly closed.

[0925]

But it is a moving target, and hence, the need for constant vigilance. What was a good encryption system several years ago is now well and truly cracked and is available to anyone who wants it on the Internet. As we move forward, once the encryption system is broken, then obviously you have to shift to another layer of security, another encryption.

It's good that the response we were able to see from government was, first of all, very focused, very quick, and I'm particularly pleased that the response has been so fulsome in what they've done. But the direct answer to your question is: we don't know. No one knows. As we go forward with the constant monitoring, we will know, and we'll also be making sure that it doesn't occur.

K. Corrigan: It's not clear from this, but are there areas of government...? I'm thinking of, for example, areas where we're dealing with personal information, sensitive information, maybe patient information. Are there areas where the level of security is higher, where it needs to be higher and, therefore, where the level of security is higher?

J. Doyle: Later on this morning, we'll be talking about the PARIS system, which talks to that particular point.

J. Rustad: Thank you for the presentations. One of my questions has been asked. The second question that I had has already been answered, which is good. So I will go on to my third question. I won't need any supplements associated with it.

Technology changes rapidly, and the pace of change, actually, is increasing as we go. Is it true that there is no way we can have a 100 percent bulletproof system? I mean, there's always going to have to be some level of risk management, I would think, associated with the data. The bottom line is that as technology changes, you just can't possibly keep in front of all of it. I think also that part of that question....

It would be true to say that we're not, of course, the only entity that is struggling with this thing. Both the private sector and other government agencies around the world are all facing this same sort of challenge because of that pace of change.

Dave Campbell: It is possible to have a fully secure system. However, it would be so unusable as to be worthless.

J. Rustad: I guess you're right. If you didn't have access to anybody, then it's secure.

Dave Campbell: Exactly. So it is a constant balance. It keeps a lot of us up at night. The approach we take is that we take a layered approach to security. So we don't just rely on the wireless access control security that's in the device and then assume that whoever is in at that point has free reign through the system.

Just because you let somebody in the door of the apartment building, that doesn't mean the doorman lets them wander the halls. If they were wandering the halls, there are locks on the doors. There are more preventative measures, and we're constantly monitoring the current technologies and the current threats. We stay very close to.... We have great cooperation with the federal government security agencies. We do a lot of work with Microsoft and the major networking vendors to try and keep slightly ahead of the curve and try not to get behind the curve.

S. Simpson: How are BlackBerrys captured in all this in terms of the security of BlackBerrys, since we all use those, certainly around this table, probably more than anything else?

J. Doyle: We excluded BlackBerrys from the scope of this particular work, but it's on our list to have a look at them. I can't answer your question at the moment, but I hope to do so before too long.

S. Simpson: Maybe if the Auditor General.... What's your expectation on the timeline to be able to complete that review and report back or send the information off to the systems folks?

[0930]

J. Doyle: I haven't actually set a timeline at this stage, but it is something that's on our list of things to do, and it's got a high priority, but we need to finish our current block of work, which is focused in on the annual financial report, before we shift over now to this kind of work again.

G. Gentner: I've got two questions. I don't know if the second one is relative to the main argument here, but we'll see.

How many cells or, shall we say, systems were used to avoid firewalls already built into the system? I mean, in land lines you have firewalls. We've got firewalls everywhere. This new technology allows you to do an end run and get around it. How many mobile units — i.e., on a laptop, via a Rogers stick or whatever — are actually used to avoid using government firewalls?

Dave Campbell: Actually, where we place our firewalls doesn't allow for them to be bypassed. We place our firewalls closer to the Crown jewels, if I can use that terminology. It's kind of our last layer of defence around

the servers, where the information is stored. So whether you come in through a Rogers Rocket Stick or a cellular modem or a wireless access point, if it's deemed that that server or that information requires a firewall in front of it, you have to go through that firewall and the other security measures to get there.

G. Gentner: Well, I can tell this body here that I evade firewalls all the time out of my office here in the Legislature by using a Rogers stick. If I can do it, I'm just wondering who else in the province can get away with it.

Dave Campbell: I'm sorry. I'd have to have more detail in order to respond.

G. Gentner: Not that I want — excuse me, Chair — you to start prohibiting my ability to go outside the normal systems.

B. Ralston (Chair): It might be tempting.

G. Gentner: The second question is general. Maybe it's not fair, but as the technology changes so do the carriers. There seems to be a policy when you go down the ledger of each ministry. Some ministries use TELUS, some use Rogers. I don't know. Does government have a protocol on who are the suppliers, and is there a specific modem you use? How do you control that?

Dave Campbell: That I think is beyond our scope. I'm aware that there are standing offers in place. There have been competitive processes to select cellular providers, but I don't think there is a restriction on one or the other, and I think it is up to ministries to choose which they prefer.

G. Gentner: Just one quick supplemental. That's an interesting perspective, because if each ministry is out doing its own thing, it creates more focus or unnecessary work perhaps by you and others.

I can say that I know we're into an austerity kick, and the Auditor General may want to confirm this, but on an annual basis our communications vis-à-vis through cell phones, etc., are increasing by 8 to 10 percent, because in my estimation, ministries are going out not using the norm. They're now using Bell Mobility, using everything else, and there doesn't seem to be a standard whereby we are able to rein in the government's expenditures on this new technology.

B. Ralston (Chair): I think that may be outside the scope of these reports, but I think those are questions that we maybe can address later on.

I'm going to move now, bearing in mind the time, to Richard Lee and then Vicki Huntington.

R. Lee: Thank you for the presentation. In the report by Mr. Campbell, page 10, it says that there were no recommendations in the audit area of "secure wireless infrastructure."

I believe, actually, that some of the recommendations — for example, the network SS control.... You have actually a location to.... Those are part of the infrastructure — are they? Or there are no audits on infrastructures. Then, are there any improvements over the years since those reports? The infrastructure actually has been improved?

Dave Campbell: Not since the report, no. That statement was based on the layout of the audit report. There were three categories. There were, I believe, some recommendations pertaining to SFU in that category, but there were none for government.

[0935]

R. Lee: In that case is it necessary to improve some of those secure wireless infrastructures?

Dave Campbell: I think there are definitely requirements to improve network access control and monitoring. But the basic infrastructure is quite sound — the physical security around it, the way it's implemented, the processes, etc.

V. Huntington: While the response to the recommendations has been very good, I'm concerned about the widespread nature of the gaps in the first instance. I'm just wondering if the Auditor General's office will be following up on these. Can you confirm what the next round of audits might be on the wireless technology in government?

J. Doyle: Thank you for the question. We'll be following up using our usual follow-up process in regard to all the recommendations that we've made. Also, we're looking at what further work may be required. I should say that we do expect the ripple effect to take place. I think it is taking place in that what we have found here is being spread right through the government reporting entity. CIOs in different organizations are asking questions, or should be asking questions, around how well they are managing their wireless networks.

We don't expect to go into any area in government in the future and to find these kinds of problems. If we do, I suppose I would have a very dim view of that, and I'll leave it to somebody else to sort out the debris. But quite frankly, the government CIO has made it quite clear what the standards are, and I know it's his expectation that these are addressed and dealt with quickly.

We will go back and look from time to time. We will do the follow-up, but we don't expect to find anything. We'll probably be moving onto a different topic now that management has responded so well.

V. Huntington: Thank you. Are you getting the same level of response from Simon Fraser and BCIT?

J. Doyle: Universities are a little bit different from some organizations within the government reporting entity. In the report it was quite clear that they had robust wireless systems with a few gaps. We've asked them to deal with those gaps, and we will go back and check to see what actually has been done. As with all follow-up processes, if I'm not entirely satisfied that it's been dealt with adequately, I will be going back and doing further work.

B. Ralston (Chair): I had a further question myself. On page 13 you mention that the network access control is undergoing a proof-of-concept, and this is to devise a solution for monitoring and detecting unauthorized computing devices. Can you explain in a little bit more detail what a proof-of-concept is, and is that still on target to be completed by the end of June?

Dave Campbell: It is on target. It will be complete by the end of June. I was told it would be complete by the 15th. I didn't want to mislead this body, so I said the 30th. They assure me it will be.

The proof-of-concept — we know the technology works. People use it. It has existed for a period of time. But how we interface it with our existing procedures and systems, and how we monitor it and make effective use of that information is really what the proof-of-concept is involved in.

It also gives us an idea of what the scope is required — sizing the solution, cost and what the impact is on support ongoing.

B. Ralston (Chair): Thank you. One further question. On page 15 you talked about an inventory of network devices, including authorized wireless access devices. One can readily imagine that in the government reporting entity, there are thousands of those devices. What's the process for ensuring that, indeed, new devices are registered in a timely way?

Dave Campbell: Any new authorized devices are installed as a result of a request either from our internal groups to handle increased capacity or from a ministry client requiring more service.

[0940]

The order process from start to finish tracks that item until it is installed. Once it is installed, it automatically goes into our inventory.

B. Ralston (Chair): So it's a centralized registry. The ministries don't have their own discretion to access the network and keep their own list.

Dave Campbell: No. The only way a ministry could change the inventory is to request that we remove it or add it.

B. Ralston (Chair): Those are all the questions I have. I don't see any further questions, so thank you very much.

Maybe we could move to the next topic, report 7, *The PARIS System*. If we could allow just a couple of minutes to switch over.

I've allowed a relatively brief period of time for this report simply because most of the recommendations were implemented, and the report was delayed in its publication in order to allow for that. I think maybe as a case study on how rapidly government can respond to serious deficiencies that are identified might be the theme of this report, but I'll leave that to the presenters.

**Auditor General Report:
*The PARIS System for
Community Care Services:
Access and Security***

J. Doyle: PARIS is just one of the many health care systems that are in use within the province. Up to now my office has not done any in-depth assessments of the health care system from an IT access and security perspective. We have focused mainly on the financial systems.

I undertook the PARIS audit to assess the access granted to health care professionals and the level of security within PARIS following a request from the Information Commissioner, who was conducting work on the privacy components.

I was disappointed in the results of both the access management at Vancouver Coastal and also the IT security in the supporting infrastructure in regard to the PARIS system. I expected to see that access to health records, especially particularly sensitive information, would have been granted on a need-to-know basis. My audit team thoroughly understands the balance between accessibility and privacy and therefore use this as a basis for assessing access.

On a positive note, however, changes are being made in the way that access is being managed and addressed. I would leave it to the government side to actually explain that.

Regarding the IT security, I was not expecting to see the extent of security deficiencies, including the network and the database. It worried me that Vancouver Coastal is not the only system with these kinds of problems, although it's the one that we've done the most work on at this stage. We saw some of these issues in a previous in-depth IT security assessment elsewhere in the government reporting entity. Again, I would suggest that the ripple effect should be effective and that issues that

flow from one audit can flow through to other entities within the government reporting entity.

I do not intend to assess all the critical systems in government. I just don't have the resources for it, and I don't think it's necessary. However, I would expect that the recommendations from this report would be a source of learning for other organizations within the government reporting entity. I know there are discussions at the CIO level throughout the system that actually make this communication occur.

[0945]

The audit team. Again, Bill Gilhooly was the assistant Auditor General responsible for this block of work, and to my right we have Pam Hamilton, who is the IT specialist, the director of IT audit. Behind me is Ada Chiang, who also assisted in this particular audit and is also a director of IT audit. I'd like to pass over to Pam to provide a brief presentation.

P. Hamilton: Good morning, committee members and Chair. As introduced, I will be giving a brief presentation on the audit of the PARIS system used in the Vancouver Coastal Health Authority. The topics I will cover are the background, our audit focus, our conclusion, the findings, the results of the assessment in terms of the number of recommendations, and our audit timeline.

I will begin with the background. PARIS stands for primary access regional information system and is designed for community-based health care. VCH uses this system in over 75 community locations throughout Vancouver and Richmond. It enables health care information to be linked throughout the region for more than 620,000 clients. It's used by about 4,000 health care providers across the community programs.

The VCH community programs include primary health care for adults and children, mental health services, addiction services, preventative health care and residential care. The sensitive and confidential client information from these programs is processed and stored in the PARIS system, which is operated in the VCHA network.

This audit focused on the management of access to health information in PARIS and the adequacy of the controls in place to protect this information. The infrastructure and environments that support the processing and storage of PARIS health care records are complex, so many areas had to be assessed to determine the overall protection provided. To properly address the risks, we looked at the security policies; the system security, which are the controls in the network and the infrastructure; the database and the operating system; access granted through the application; the management of user accounts; and the monitoring of access in the network and to the data.

Our overall conclusion, as bulleted on page 5, stated that almost all system users have excessive access to sensi-

tive and confidential client information. Many clients' full health information is accessible to a large number of users. Essential security controls are not in place to detect and prevent unauthorized access or attacks. There is a risk that inappropriate disclosure or theft of information could take place without VCH's knowledge.

These conclusions are as a result of the ten key findings on pages 6 to 10 of the public report. So I will go through each of the ten key findings.

The first one. User access was not based on the principle of need to know. Almost all 4,000 users were granted excessive access through the application, and in many cases the clients' full health information was accessible.

Our second key finding. The system controls were not adequate to secure the system from internal or external attacks. Multiple layers of defence were not in place. For example, intrusion prevention and detection systems were not deployed, vulnerability scans were not performed on the servers, regular reviews of the firewalls were not done, and system patching was not mandatory.

Our third key finding. A comprehensive security policy was not in place. The security policies are important directives from senior management in providing guidance for the security programs that should be in place and for setting the tone of security in the organization.

The fourth finding. The PARIS database was not properly secured, meaning that corruption of data or unauthorized viewing of data could occur.

[0950]

Our fifth key finding. Information could be leaked out of the database without detection. There was insufficient log monitoring, and there were no content monitoring tools to restrict unauthorized extractions.

The sixth key finding. Monitoring was inadequate. There was no log management system to allow visibility into the network for detection of internal or external attacks or unauthorized activity.

The seventh key finding. User accounts were not properly maintained to ensure that employee and contractor access was removed when no longer valid. There were hundreds of former employees and contractors with system access after they were no longer employed at VCH.

Our eighth key finding. Unsecured network access. There were several ways that security controls could be bypassed. There were unaccounted-for laptops that were able to gain access to the internal network. There were unsecured common areas where a non-VCH computer could be used to directly access the internal network.

The ninth finding. There were inadequate network segmentation and access control restrictions in the internal network. This means that there was unrestricted traffic flow to critical servers and that the proper safeguards were not in place to help prevent the spread of viruses or malicious code throughout the network.

Our tenth key finding. There was no data classification system and no retention policy in place to manage records

for archival or deletion. Consequently, records that were no longer relevant were still in the system.

The audit resulted in a total of 127 recommendations, which were included in the detailed management report. All recommendations were accepted by VCHA management. These recommendations were brought forward to the public report and summarized into the ten key recommendations that I just described.

The last point that I'll cover here is our audit timeline. The audit began in October 2008, and we completed it in May 2009. The detailed management report was issued to VCH in June and contained the full set of recommendations. VCH submitted a work plan to our office in July 2009 with estimated target dates for addressing each of the recommendations.

By the end of January 2010 a reasonable level of security assurance was achieved in response to the major vulnerabilities identified in the audit. A public report was then released in February 2010. We are currently monitoring the progress made on the recommendations and plan to issue a follow-up in October.

This concludes our presentation.

B. Ralston (Chair): Thank you very much. I have Duncan Campbell and Dr. David Marsh. I'm not sure how that's going to be divided up.

Mr. Campbell, you're presenting, then?

Duncan Campbell: Yes, I will be presenting on behalf of Vancouver Coastal. First, I'd like to welcome Dr. David Marsh, who will be here to answer questions. Dr. David Marsh is the head of our HIV/AIDS and addictions program and also a faculty member of UBC. I am the chief financial officer and also the executive in charge of IT and the legal and privacy area. I will be responding on behalf of VCH.

[0955]

First of all, I'd like to thank the Auditor General for the work that they did do. We have taken their responses very seriously, and we have worked very collaboratively to actually address the issues and address the recommendations. I'm really pleased to hear that that's been duly noted.

We have implemented 100 percent of the high-risk areas and over 80 percent of the recommendations to date and are moving quickly to close out the balance. I think what is very important is that team-based care is the basis for how we provide care at Vancouver Coastal.

The question of access has been raised, and we have actually checked that as part of our pilot process as we have gone through. We've enhanced and improved the way that we actually deal with access to our staff. Also, we've actually rolled that out to our new system and new teams that have moved forward.

Just by way of background, we have implemented 100 percent of the high-risk areas, 81 percent of the

recommendations to date and 89 percent of the security areas. An important point on this slide is that it has taken time and effort, and we have invested \$1.1 million and expect it to be around \$2 million by the time we finish making sure that all the recommendations are in place.

As we've said, 89 percent have been implemented. Probably the way to characterize our system before the Auditor General came in was that we had one line of defence, which was our firewalls and our networks. It was like a castle with thick walls, hoping that there were no vulnerabilities coming through.

The Auditor General, in the good work, found that there were some areas where that wall could be breached. Then also, as we heard a little bit earlier, the whole area of security has changed, from just a single line of defence to a multiple and layered line of defence. This audit was conducted in terms of the ISO standards, which are best-practice standards. They're not risk-based standards; they're best-practice standards. We are aiming to achieve that as part of what we're doing here.

We have dealt with all of the key areas. Security policies have been implemented. In fact, they were implemented in June while the audit was being completed. From a VCH management perspective, we wanted to send a very clear message that this was and is important in terms of our policies.

We have taken the recommendations from the Auditor General in terms of detection intrusion. In essence, we've put sensors around this wall so that we can actually make sure that if anybody tries to get through our wall, internally and externally, we can actually deal with that and have information at our fingertips to deal with directly. So we've actually taken those recommendations to heart.

A lot of it, in terms of the recommendations, is moving some of our systems way behind the wall — building another wall behind the wall, in essence. That is the way of the world in terms of IT security. We think this is the right way to go.

We have worked on the areas where there was potential data leakage. We've closed down some of the databases where that was the case.

We put ourselves to the test in January, where we asked Bell to come in and actually do an external vulnerability assessment in terms of wireless, in terms of our firewall and in terms of our external security. We were pleased with that report. We not only passed, but we are in the top 25 percent of all businesses evaluated by Bell. Their view was that we were in the top 10 percent of health businesses.

This will be an ongoing process. We heard that earlier today. Security is an ongoing battle between the good guys and the bad guys. Our job will be to continue to evolve as security needs to evolve.

[1000]

In terms of an enhanced access model, we have heard today and we saw in the report earlier that we needed to

have a look at how we granted access to our teams. In the past what was done was that the entire program was given access to the program's clients and the program's data. The residential care team would have residential care information for individual clients relating to specific programs.

What we have done now is we've actually taken those programs and broken them down into teams. At the time that the Auditor General reviewed our team, some of our teams had up to 200 people in them, which was, quite correctly, too much. What we've done is we've piloted and brought it down to a case where only the teams that actually work with the specific clients are authorized to work with those specific clients. So we've really cut down the access markedly.

We are in a position to say today that our clients' and our patients' records are safe. They are dealt with by the people that need to see them. We have strong audit processes to look at any of those areas where it might look suspicious. So we do have all of those things in place.

Probably just as important... One of the things that gets lost in summarization in the executive summary is that the Auditor General did recognize that we did show due diligence in how we set up our access model back in 2001 when we started the PARIS program. At that time the IT functionality, the PARIS functionality, wasn't able to do some of the things that we had wanted it to do. Now with the improvement in technology, we've been able to take that and implement it. That's what we have done.

This one just really talks about that. We've also gone through every single team member, whether they were contractors or past employees, and made sure that we don't have the ability to have people that have left the organization still have access to the organization. We have linked that to our payroll records so that it is not possible now to have someone that's actually left the organization have access to the information. So we've done that.

We've gone through, as part of our pilots, to work out who should know about which patient and what type of information should be there. What we did find was that, overall, most of the people that were allocated roles in PARIS were correctly so. The area where we found that there was some opportunity to improve was around some of the admin and support areas. We're making changes in that regard.

In essence, we piloted with the area where 75 percent of our teams work. We're now in the process of working out whether we can roll it out to teams such as immunization and other teams that have slightly different compositions to the ones we've got here. But we've committed to taking this through and working out the tension between access and privacy.

In closing, we have taken this report very seriously. We believe that now, having completed the ISO stan-

dard review and the work that we've done, we should be in the top quartile performing in terms of security and our standards. We have taken all the high-risk security recommendations into account. We do have an access model which we believe is appropriate, clinically and from a privacy perspective. We are committed to delivering our care based on a team-based model.

B. Ralston (Chair): Thanks very much. We have a relatively brief time for questions. Perhaps if I could just begin.

You've obviously moved with dispatch to implement all of the recommendations of the Auditor General, but if we take this as a case study, the system was initiated in 2001. Obviously, by the time the audit was conducted, there were serious deficiencies. You mentioned some of the technical reasons for that. What lessons would you offer to other agencies or departments in terms of how that came about?

[1005]

Duncan Campbell: What I would say — and then I'd probably hand it over to David, if I could — is that the lesson we learned is that this is evolving all the time. We probably looked at our external firewall as being the solid wall around our castle, and we thought that we were safer than we were. Probably, what I would recommend to my colleagues who are sitting in similar situations is: test it out, get people in to come and check whether that is the case. If there are some vulnerabilities, deal with them quickly and responsibly.

From an access point of view, this is going to be a natural tension between the information that's required to actually manage the client effectively and privacy. This is going to be an ongoing tension. I'm going to hand it over to David, and maybe he'll make some comments on that.

D. Marsh: A couple of quick comments. I have worked with about a dozen electronic clinical record systems in B.C. and Ontario and reviewed many others in the U.S. and Europe, where I've done teaching and consulting. Even before the Auditor General's review, the PARIS system was one of the better systems that I've seen, and it certainly has gotten stronger. So I think that you shouldn't view the review with the misinterpretation that somehow PARIS was uniquely weak.

Secondly, I think that in tight financial times in health care, there's always a tendency to try and preserve funding to direct clinical services and look to support services like IT for cutbacks. It's important for health authorities and other health bodies to ensure they invest enough in their IT infrastructure to maintain that it's up to date and that there are adequate protections for security. As you see, most of the recommendations dealt with database and electronic issues.

Finally, in the design of these sorts of systems, there is, as Duncan mentioned, always a balance between making sure the information is available and retained and accessible. At a point when someone needs that information for clinical care, it isn't always predictable where somebody is going to show up in the health care system or with which problems. So we need to be able to develop, especially access models that allow the important clinical information to be easily retrievable when it's needed for clinical care.

B. Ralston (Chair): I'm mindful of the time, and I'd like to move on.

I have two questioners, now three. One question each, and please be concise. First was Kathy. Then I had Joan and then Shane.

K. Corrigan: I found this report astounding with regard to the level that information was compromised. I thank the Auditor General for the report, on behalf of health care users across the province. I'm particularly concerned....

The key findings on page 21 are a really good example of the report itself, where it says: "Users of PARIS can bypass application controls and enter the database directly through non-password-protected database roles. Although the majority would not know this capability existed, awareness of it could allow users the ability to access or extract sensitive client information."

Then two bullets later: "We found evidence that many connections have been made from non-production servers to the production database environment, meaning that incorrect data may have been entered, data may have been corrupted, or unauthorized viewing of data may have occurred."

I just wanted to ask about a particular scenario. I hope that I'm talking about a user that does exist. I'm thinking of when you're talking about long-term-care facilities.

What essentially you could have had would be a privatized long-term-care facility that may have changed contractors a few times, because we're aware of some that have had contracts changing. The contractors have changed three or four times. All, I assume, would have had access, used the database, and a database therefore had multiple users over time. There was the ability to be able to get in and change the information or extract information.

[1010]

I'm just trying to paint a scenario of what could be a real horror story in terms of access to information, extracting information and misuse of information. I find it quite astounding, actually. I'm concerned, and I asked the question earlier about sensitive data governmentwide, because we're talking about one system, and I just hear now that PARIS is not so bad.

What assurances do we have that this is not being repeated throughout the province and that we haven't had

severe compromising of information? I'm particularly concerned where....

In the earlier question the Auditor General said there was no knowledge of whether or not information had been compromised. Here we see that it was very easy to get information. Do we have any knowledge that data was corrupted, viewed or stolen in any way? It's a big question, but I just was quite astounded by this report.

D. Marsh: I'd like to respond to the question, first clarifying some of your assumptions. Contracted agency employees have not had and do not have access to PARIS. It's only ever been employees of the health authority who've been trained in and provided access to the system.

Secondly, I think that in the brief public version the information is summarized and shortened in a way that might be misinterpreted. What I understand the Auditor General is talking about is that people who had access to the database — if they had the IT skills in order to access it from a data standpoint, as opposed to accessing it in a way that a normal clinician would access it for entering data — may have been able to corrupt or retrieve data. In fact, we have found no evidence of that having occurred, and that vulnerability has been addressed.

Duncan Campbell: Just to add to that, we have an audit process in place. We did have 225 reviews, audits of PARIS and other systems. We found 14 potential areas out of that 225 for PARIS. Seven were confirmed to be incorrect, and we actually dealt with those. There is a process in place to deal with it, so I think the conception that there is no control of the data is not correct, and I think we need to make that very clear to this group.

J. McIntyre: Let me start, also, by thanking the Auditor General for the good work on this. I have to say I am extremely disheartened by the results when a report like this comes across our desks as legislators.

We as government have devolved authority to the health authorities. Certainly, the public and we as legislators put trust in the organizations that these things will be monitored, that the correct systems are in place and will be monitored accordingly. I guess a very blunt question, and it might be sensitive: what are the consequences like? What are the internal consequences of that?

I don't accept.... I think it was Dr. Marsh who said that in tougher economic times, this might not have been a priority. That, to me, is not correct. I mean, billions of dollars.... We've added 90 percent, 95 percent of new dollars, all going into Health — \$2 billion this year alone. These kinds of things are very important. We have to have trust that they're doing....

What are the consequences of an audit like this, in terms of staff, staffing? Can you tell us what...? I mean, I appreciate that you are taking these steps and that

you've had Bell come in and monitor, but it is very disheartening.

D. Marsh: We're talking about, mainly, regulated health professionals. The consequences for me as a physician if I were to inappropriately access somebody's health care records, like my wife's or somebody's, is that I could risk losing my privileges to admit patients to a hospital. That would be available to the College of Physicians and Surgeons and any other college in any other jurisdiction.

I could lose my licence to practise as a physician. Employees of the health authority could lose their jobs. These are issues that are taken very seriously by the health authority and by professional bodies.

J. McIntyre: Sorry, I don't mean hypothetically. What happens...? I mean, there must be staff. Are there IT staff at Vancouver Coastal Health? What are the consequences of...?

[1015]

Duncan Campbell: Let me answer that one. In terms of the security side, we were disappointed with the level of security. We have made changes in that area. We have changed our CIO. We do have a new CIO, Barry Rivelis, who has been charged with this process. We expected it to be better. It wasn't. We've dealt with that.

I think, on the other side, what we need to be very clear is that we have not skimmed because of lack of funds. I sit as a CIO who has to deal with these issues. We know that the government has responded accordingly with funding. We know that there are pressures within the health system to get it done, but this was never one of our areas that got compromised for that reason.

In fact, I'd go further to say that in the summarization of this report.... If you read the full report, you'll get a very, very fair, balanced view of what actually happened. As it got summarized, we ended up with sound bites, such as 4,000 people having access to all information at all times and no consequence around that and that we've not been able to follow up with an audit. That is not true. It doesn't show that in the report, and we did ask the Auditor General to change that in our letter when we responded to the report.

I think we need to be very clear that 4,000 people had access to a summary of somebody's name, their personal health information, some demographic background, any allergies and any risk around security. Those are the five things that they had access to. I don't know if Dr. Marsh wants to confirm that, but that is the case. So to say that 4,000 people had access to health information records or information records around particular case histories — that is not the case.

We want to put on record that we have taken all measures possible in the design of PARIS. The area that I

referred to where there was broadness of roles and potentially inappropriate roles is when we had the whole programs relating to areas having access to that information. We've taken it down and locked it down one level further, which is around the teams that are revolved around each individual patient.

I think we can walk away from here saying that we do have the processes in place, we do have the systems in place, and we do have more than just security and fire-wall security. We have education. We have professional ethics. We have audit. We have all those things in place, and we believe that we do have a system which is good for British Columbia.

B. Ralston (Chair): Perhaps just the Auditor General may wish to respond, since there appears to be a direct disagreement there.

I have Shane, Vicki and Ralph, and then I'm going to cut it off. We're over time for this section. I'd like to proceed. We have another fairly substantive report that we're late in getting started on. So if the Auditor General wants to respond briefly, then those three questioners, and then we'll move on.

J. Doyle: There was a concept in PARIS of particular patients who had a need for a lot of sensitivity around their records for particular reasons. Access to their records was constrained to particular teams that dealt regularly with those patients. The point that was being made was that far too many patients had what was called universal access, and they were basically.... There were no constraints as to which member of staff who had access to PARIS could access those records.

There are about 4,000 people that regularly use the system, and they would have full access right across the board to those patients that weren't clamped down and restricted.

When the functional requirements for PARIS were first put together, it included a level, a concept — I don't think you'd call it a need to know, but the concept was there — that they could narrow down access to either particular care groups by teams to individuals. That, as correctly described earlier, was not made available in the first version of PARIS, but it was made available several years later. When it was made available, we didn't detect or haven't detected any change in the way that PARIS was operated.

I would agree that PARIS is a reasonably good system. Indeed, it's going to be used in other health authorities. What we're saying is about the way it's protected, the way it's used and the level of access to confidential private information that is available to people that in fact have no need to access that information.

[1020]

Even in the newspaper today, you find that people misbehave — this is not a health system; it was a border

guard — and access private information in different ways and use it for inappropriate purposes.

Now, I think that the health authority is moving forward with its access model to see how it can fit care into a process of protecting privacy. Indeed, the Information Commissioner had a few words to say upon that, but this isn't the venue to talk about that.

I don't know quite where the balance lies. I just knew, when we looked at the whole process, that in fact too much openness was there, and all we asked was for management to bring it back. We did decline to change those words, and we still decline to change those words because we think it's a valid and accurate explanation and description of the actual situation on the ground. If you're an individual and you're not categorized in a certain way, 4,000 people can look at your record.

S. Simpson: Thank you for the report. My question is to the Auditor General, and it relates to the PARIS system more broadly in the application. The concerns that the Auditor General found around PARIS — to what degree are these kind of inherent to the system itself and to the requirements? I look at that because I know there are organizations like Community Living B.C. that now have adopted the PARIS system. I think in 2007 they were directed to adopt the PARIS system, and there may be other entities that have adopted it as well.

My concern and, I think, as was said is that the ability of the Auditor General to go out and review every system is not there because of resources. How do we look at things like CLBC, which has adopted this system, and have some assurance that, in fact, they are applying the appropriate safeguards to the system, which have now been dealt with at Coastal Health, to ensure that those groups that are also dealing with very sensitive information on individuals are protected as well?

J. Doyle: Thank you for the question. As I said just now, PARIS looks like a functional, properly appropriate system to hold patient and sensitive information. What we were looking at was the way that PARIS was utilized and used, which was the basis of our recommendations. How it's configured, how the control processes are monitored within the application itself, how different members of staff have access to information are all internal decisions that can be made. You basically use the orchestra the way that you need to use it.

What surrounds that application is a series of controls. I think it was described as a castle wall that surrounds it. It was looking at that access area and how you would actually get into PARIS, but it doesn't actually take away that PARIS was quite functional and was appropriate. In fact, that's obviously been played out with other organizations taking on PARIS as a system that they want to use.

There's always a danger when you bring in a new system and you put it into place that everyone is exhausted,

and that's the end of the process. But I think a message that I'm getting, and I think the ripple effect would show this, is that there's got to be constant vigilance over time, not only when we go out to security but as functionality within an application changes — how an organization should respond to those shifts in functionality and how that plays out and translates to, in this particular case, the care setting and how that could actually mean the best results for patients and for the organization.

So I wouldn't challenge PARIS itself. It was just that when they went in to have a look at things, we felt that they could do better in regard to how they actually used the application. In fact, the recommendations were focused in that way. But it's still up to management to decide how it's being used, what the security is, how the privacy works, how it works best in our particular organization and how they can get best value out of it.

[1025]

V. Huntington: Firstly, let me say that I share Ms. McIntyre's concerns about what has happened here. I have trouble understanding a governance model that allows deficiencies like this to grow and to not be dealt with, so I'm extremely pleased that the audit has dealt with that and that the changes are being made.

My question is on the consolidation of clinical back-room and support services that is presently underway. Number one, is PARIS part of that? And the systems in FHA, for instance — do they use PARIS, and are those deficiencies being discussed if it is part of the consolidation?

Duncan Campbell: I can answer that. At the moment Fraser Health does not use PARIS. It is under consideration. Currently, as part of the Lower Mainland consolidation work, PARIS is not being looked at. We're only looking at back-office and semi-back-office areas, so it doesn't cover the PARIS systems at this time.

V. Huntington: What system is FHA using?

Duncan Campbell: Fraser uses a Meditech system overall. It has a very strong firewall — probably the strongest in the province, as I understand it. We keep trying to get through it to join some of our back-office areas.

V. Huntington: That's just what we don't want you to be doing.

Duncan Campbell: No. What I mean is that there's a great deal of security behind the Fraser Health firewall, and appropriately so. But we obviously still have to share information around diagnostic imaging and lab results, etc., so there's a balance between not doing anything and actually being able to provide clinical services. That's being looked at very seriously by the information technology groups.

B. Ralston (Chair): Did the Auditor General wish to add a comment?

J. Doyle: Just to remind the Chair that we have, in the next report on electronic health records, a representative from the ministry, and they would probably be able to expand on that question if necessary.

B. Ralston (Chair): Once we dispense with our last question, then we'll begin that report.

R. Sultan: I think the concerns of the committee have been well expressed. My question really takes off in a slightly different direction, directed to Mr. Campbell.

It would seem to me, Mr. Campbell, that you have one of the most challenging senior executive positions in the entire province.

On the one hand, you are charged with the CFO responsibility and accountability for the largest operating unit, as I understand it, in the absolutely largest ministry of the province. It's a huge enterprise with all sorts of financial challenges which we hear debated in question period virtually every day, thanks to our friends on the opposite bench. So we appreciate that that job is anything but simple and, of course, is fraught with all sorts of human consequences if the right decisions aren't being made — emanating, in many cases, fiscally.

On the other hand, you're the chief information officer of another vast enterprise which deals with the most personal of our information. I suppose the largest segment of our population, in fact, is under your domain in a rapidly changing and technological environment.

I can imagine the docs want to look up the latest blood pressure reading of somebody on their BlackBerrys as they rush down the hall. Who knows where this technology is heading? The Auditor General concedes he hasn't even begun to think about the security problems of all these little gadgets we seem to love carrying around in our pockets.

This is a bewildering world, and you are the chief information officer, as I understand it, guiding that development. It's not flawless, as we've learned this morning, and that's quite understandable.

My question is: aren't both of these tasks so enormous in their span and consequence...? To find both of those assignments embodied in one man must mean that you're the superman of all time in British Columbia. Is it possible?

B. Ralston (Chair): You'd be able to take the transcript to your boss for a raise.

Duncan Campbell: Probably, to respond to that, it is a challenging role. But we do have a chief information office, Barry Rivelis, who now provides that service on behalf of ourselves; PHC, Providence Health Care; and

our provincial health service agency. We do have a really good team under Barry, so that does take the load off.

The one area that you did not mention is that I also have legal and privacy as part of my responsibilities, and that is an area which does take a lot of time and will continue to take a lot of time.

[1030]

Fortunately, we do have really good people, so it's not me; it's the team. It's not just the team at an executive level. It's all the people that have actually built PARIS and built the systems down on the front line. They have done an amazing job in building a system that's good for our citizens.

It's our responsibility now to make sure that we deal with the Auditor General's report — not only now but, as he quite rightly says, on an ongoing and vigilant basis to make sure that these issues are dealt with and addressed as we redesign the castle as the enemy tries to get in.

I am pleased to say that we have managed to balance all those responsibilities, including balancing our budget and including spending close to \$2 million on fixing PARIS. Finally, this juggling act has been a tough but rewarding process.

B. Ralston (Chair): Thank you very much, and thank you to all the presenters.

I'm going to suggest to members.... There were some possible further questions. If they wanted to put those in writing and pass those on to the Clerk, we can forward them and solicit written answers to the questions.

I'm going to suggest we adjourn for five minutes, and then we'll begin with electronic health records.

[1035]

We're about to consider the *Electronic Health Record Implementation in British Columbia* report of February 2010, the Auditor General presenting for.... I'm not sure if the Auditor General has a brief introduction he wishes to make. Then I believe he'll be introducing Malcolm Gaston, who's the assistant Auditor General. Elaine McKnight, who's the Assistant Deputy Minister of the Ministry of Health Services, will be responding.

**Auditor General Report:
*Electronic Health Record
Implementation in British Columbia***

J. Doyle: Thank you, Chair.

Electronic Health Record Audit. This was an audit on how well the Ministry of Health Services is managing the implementation of the electronic health records program.

It was a collaborative audit. Five other provincial audit officers and the Office of the Auditor General of Canada each conducted similar work at roughly the same time, reported separately, and then there was a joint report produced in April 2010. We will be discuss-

ing here a provincial report which was published earlier on this year.

What are electronic health records? It's a record which is secure and private. It speaks to an individual's health history and care, and it's intended to be collected over the person's lifetime.

The expectations from a fully implemented electronic health record system is faster, safer and more efficient treatment of patients. By 2013 the ministry expects to have deployed the six core components and to have spent over — I think it is — \$222 million, of which half is refundable from Infoway.

Our overall conclusion, when we conducted this work, is that the ministry now has in place most of the mechanisms required to effectively guide, manage and report on the performance of the initiative, but there's still a long way to go. I won't go through the findings in detail, but I will observe that, looking forward, the long way to go is an important factor that needs to be considered in regard to electronic health records.

Progress has been made in building the individual components, but to then make sure that they are integrated within the health sector and then regularly used by health professionals is the next major challenge, the new frontier if you will. And that is going to be difficult and long and fraught with risk that needs to be managed.

As a by-product of this particular piece of work, we have asked for the ministry to provide my office with regular updates regarding progress which we will publish in our follow-up reports and make available to this committee through the usual channels.

[1040]

I'd like to introduce, to my right, Malcolm Gaston. Malcolm is an assistant Auditor General within the office. He's taking the place of the Auditor General who is not here at the moment, Norma Glendinning, and has volunteered to step in and do the presentation.

Malcolm, over to you.

M. Gaston: Electronic health records are being established across Canada. In 2001 the federal government set up the Canada Health Infoway to support and accelerate the development of an electronic health records system that will be compatible across the country. It's important to appreciate that B.C.'s initiative is not one project but the end result of multiple individual projects.

It's planned that electronic health records will solve a number of persistent problems in the health system. Health records in electronic form should be more legible and more easily retrieved than paper records, as well as providing complete and up-to-date details. This offers potential benefits including decreasing risk of patients receiving inappropriate or duplicate treatment. Other potential benefits include better planning, monitoring and research information.

However, benefits will not be fully realized just by making the technology available. Actual changes to how work is done in the clinical setting must also be achieved, which means that providing support as health care providers adopt new technology is important.

So why do we choose to look at electronic health record implementation? First of all, it's very complex. It involves both provincial and federal resources. It has compelled the health sector across the province to collaborate closely. It depends on participation and support from multiple health organizations and stakeholders, each, of course, with their own priorities. It's high-risk. The move to sharing electronic information raises concerns about the privacy and security of personal health information. The technology for managing electronic records of this scope is new and sometimes untried.

The shift to electronic health records is a significant change for a sector that has traditionally relied on paper records. As the Auditor General has just mentioned, it involves significant public funds — over \$220 million of capital spending. It also has a national impact, which of course resulted in concurrent auditing in six provinces and at the federal level.

The purpose and expectations of our work was to assess whether the ministry has appropriate and effective mechanisms in place, particularly about setting clear direction, coordinating multiple projects as well as managing each project individually, and then reporting on progress and outcomes.

It's important to look at the audit timeline. One of the challenges we encounter as we conduct audits is that the world is rarely static. Systems and processes are evolving as we are conducting our audits. Our audit reports represent a point in time, a snapshot of what's sometimes a moving target. As well, organizations begin addressing issues while we are conducting our audit work and before it's completed. It would be true to say that both of these scenarios occurred in this particular piece of work.

So the audit teams identified, at the completion of their fieldwork in May of 2009, four recommendations: that the ministry should finalize its strategic plan, complete its tactical plan, enhance progress measures and report publicly on the outcomes of the electronic health record initiative. We reviewed our initial findings and recommendations with the ministry at that point, and that included their short-term action plan to address the issues identified.

At that stage we decided to extend the evidence-gathering period until November of last year. As a result, many of the significant issues we initially found have now been addressed.

In terms of our overall findings and conclusions, even though the electronic health record initiative had progressed slower than initially planned, the ministry now has most of the mechanisms in place or in development

to fulfil its role of providing appropriate and effective guidance, management, monitoring and reporting on the performance of the electronic health record initiative. But there's still a long way to go before British Columbians fully realize the benefits of having an electronic health record.

[1045]

Looking ahead, given the challenges and risks in developing and implementing electronic health records for British Columbians plus the significant investment involved, the undertaking is clearly one that needs to be done well. For this reason, our office will ask the ministry to update us regularly on their progress in implementing the initiative.

We have recommended that every six months the ministry provide our office a progress update on its results against planned measures of time, cost, quality and outcomes as well as an explanation of these results. We will review and report this information to the Legislative Assembly. The first follow-up is scheduled to be reported in October of this year.

That concludes our presentation.

B. Ralston (Chair): Thank you.

I'm going to ask Elaine McKnight to respond now, and then we'll open up for questions.

E. McKnight: Just with the permission of the Chair, I'd also like to introduce one of my colleagues in the gallery, Paul Shrimpton, who is part of the initiative as well.

In response, I do want to just say thank you to the Auditor General for the comments that it was a collaborative audit. We did work very, very specifically and closely with the Auditor General to ensure that we got the best value out of the audit.

Today we're just going to talk a little bit further on the EHR context, some of the findings from the audit, and bring a little bit of a status update as to where we are with the initiative and also what we plan to get to for the completion over the next couple of years.

I think there was some background in the report. Certainly, electronic health records are a global trend, with more than 40 countries implementing or developing electronic health records.

Canada is a small part of the countries considered challengers in the electronic health record progress, space and momentum. We look to jurisdictions such as Denmark, who are world leaders. I think the thing that we look to is for lessons learned and how we get to the point where they are with electronic health records and the benefits perceived from those.

As of November 2009 Canada Health Infoway ranked B.C. third out of Canada's 13 jurisdictions in terms of EHR. Our colleagues in Alberta would be considered leaders in this space. They have been at it longer than

B.C. has. The second-ranked jurisdiction is Prince Edward Island, a much smaller jurisdiction in the progress overall.

We do feel like we are making fairly significant progress. Out of the large jurisdictions, we're considered in the top groups.

As reflected in the final report, we did respond very quickly to addressing a number of the interim recommendations. We want to talk a little bit about the following actions that are complete or underway to address the report's one final recommendation overall.

Specifically, the core recommendation was to have a revised tactical plan for e-health completion. In the report it talks about an overall strategic plan and publish. We did publish that over a year ago. In the processes of... We felt we had a tactical plan in place, but it was expected to be enhanced and to be integrated further.

We did publish that report in November, as our first one, and we're under a second review now with those tactical plans. The purpose of the tactical plan is to...

[1050]

What the Auditor General alluded to was that each individual project is managed on its own merits. It's with great project management discipline, but the tactical plan is meant to bring all of those initiatives together to ensure that we understand what the interrelationships are with the projects, to ensure that we understand the risks involved with each of the projects and how we ensure that we're able to bring the benefits collectively together. So we have responded to that, and we will be updating that plan on a quarterly basis.

I think one of the things that... We certainly took the guidance from the Auditor General's office. In response to saying, "Yes, the world changes, especially in the space of electronic health records. So if it changes, what do we need to do to adjust our plans accordingly and appropriately...?" That is what the quarterly tactical plans are meant to do.

We've also enhanced our quarterly reporting to executive reporting to key executives and broadened that group. In the report it demonstrates a governance body, our governance mechanism that we deal with. We have our e-health strategy council. It's a large group of multi-disciplinary individuals from the BCMA, College of Physicians, senior folks within the health authorities, pharmacies, First Nations. We have a broad mix. It is a senior group to guide us as we go forward.

We also share that quarterly progress report with the CFOs of the health authority. We're doing that on a regular basis, and of course, we do that with the CIOs across the health authorities.

We are also looking to continue to enhance that quarterly progress report so that we're really clear on progress made on the defined outcomes. We still have a little bit of work, but we think that we're getting closer, and we'll look forward to the Auditor General's comments in the fall to see if we are meeting those expectations.

Completed a benefits evaluation plan and working towards establishment of baseline measurements. This is an area that continues to be a challenge and will be. The biggest issue is not having the baseline measurements in the very beginning, in the 2000, although with that there is a basis of a significant report that Canada Health Infoway completed at the time of the initiatives, and that is what we're using.

We also have a number of studies that were done within the health authorities, within the Ministry of Health, in the early 2000s to basically establish baselines. So we're trying to get agreement among our many stakeholders to say: "Is this an effective measurement or not?" There are various opinions out there of what a baseline measurement should look like. We are working with Canada Health Infoway to ensure that we have collected progress across the country, and this is an area where we want to ensure that we have baseline measurement in comparison to some of the other jurisdictions.

Just as a little bit of background as well — I did mention it's not the scope of this report — as part of the bigger EHR audit reports in the other provinces, the Auditor General of Canada did publish the report in April of this year. Several of the provinces have certainly been challenged to plan effectively for electronic health records. It is a complex initiative, and it is new territory, but I think, as many of the jurisdictions, we have learned a lot over the last few years and are now being able to make some significant progress.

B.C. was identified as the only province with component plans linked to the strategic plan, so I think it was significant to say that we have those ties. In B.C. it was identified that project planning, monitoring and risk mitigation, and reporting are in line with best practices. We took those as favourable in comparison to some of the other jurisdictions.

Just as a bit of a status overall, just for context, one of the things that's challenging for electronic health records is that they are not like a building or something, where you can actually see the actual progress of development being made. It is a challenge for systems; a lot of development work and time goes by before people get to actually touch the systems and use them effectively. So we just want to make sure that people have a good context of what is in place.

Two of the pieces, the provider and the patient registry.... They're basically registries to collect for all providers in the province and for patients within the system. They have been in operation for a number of years now. We have a lab, and our public health systems have been built, so from a development point of view they have been built, and we are now in the process of implementing those within the province.

[1055]

The electronic health infrastructure has been completed, and we have integrated that. We have done integration work with the registries, labs and public health systems.

I mention the public health systems, although they are not part of this audit. It is a big, key part of our B.C. e-health initiative. We are working on that, and it is a part of our overall plan.

The lab and diagnostic imaging components are currently being trialled by health professionals in the Lower Mainland. We've had some components in the lab in place since last year within the Provincial Health Services Authority. Now within the diagnostic imaging we have that being trialled within Fraser Health and Vancouver Coastal, and the lab system is now being trialled within Vancouver Coastal as well.

So we are making some significant progress. We are going through the discipline stages of ensuring that it does the job that the clinicians need to do and that we have all the pieces in place. We will be, over the next year, putting those into a broader kind of implementation once we have, over the next couple of months, gone through some of those clinical trials.

Getting to completion over the next two fiscal years is the thing that I think is the challenge for electronic health records. They will go on forever, like most systems for enhancing where we will go in the future, and the world will evolve. We have a plan for the next two years, to be able to deal with completion of specific projects to meet our Infoway targets. The money.... As a federal funder, there are targets with those areas, and we are working to be able to finish these initiatives.

Major activities include how we integrate remaining health authority lab systems to our provincial lab solution. We are working on that right now, and we will be looking to complete those over the next two-year period.

We're looking, also, to deploy our e-health viewer to some of the remaining health authorities and deploy some of the diagnostic imaging functionality beyond the Lower Mainland. We're also looking to deploy our public health system for aspects like inventory and immunization, and we're in the process of upgrading and integrating our drug system to be able to work with electronic health records.

We do have a lot to do. I think, as the Auditor General pointed out, there are many of the questions in the back of the audit report that look to the future. I will be candid to this group around how we ensure that all of those benefits are realized. It will take significant collaboration among the different stakeholders, the health authorities. Over the next year or so we are looking to ensure that those integrated plans begin to outline how we ensure those effective results overall.

B. Ralston (Chair): Thanks very much.

N. Letnick: I'll first say my mea culpa. Over the long weekend I didn't get a chance to read the entire report. So if this is in the report, let me know.

So 20 percent to 30 percent of incidents in hospitals, according to some research, are because of errors made by people. If we can do anything to improve information, it will greatly reduce the cost of health care — and, of course, people's lives.

The electronic health record is obviously something that can move in that direction. As we evolve over the next few years and decades, whether it be putting our records on little chips or planting them in our CareCards or maybe somewhere in our bodies, if we get in an accident, we have the electronic health record with us. I think we'll see that convergence happen.

With the Auditor General's review of the electronic health records and the PARIS system, I'm just wondering. Did you find any opportunities to converge the information that we are getting right now into one where we can improve quality of information, where we can lower our cost because we're not duplicating different systems and where we can balance the need for information for clinicians as well as the privacy of patients?

E. McKnight: I'll attempt to answer. The comment from the Auditor General around looking to take the PARIS audit, in particular, and making sure that the learnings and the findings are applied across the health sector — that's a significant role within my responsibility that we work with. It's on a collaborative basis.

[1100]

But we have initiated, within all the health authorities, a process that core government uses, which is like our health check. It's called the systems health check. It's an annual process. We have committed to the Auditor General that we want all the health authorities, and we have asked all the health authorities, to do that assessment.

That certainly came in as a result of the PARIS audit. We want to look at: what are the learnings from the roles-based access model within the PARIS system? How does that relate to what we have been designing and developed within the provincial systems on the electronic health record? We do need to ensure that those are aligned. I would say that we have taken every opportunity that we can to ensure that we are taking those learnings overall.

It was one of the goals of our integrated health sector IM/IT plan, which we published a year ago. The purpose of that report was to take a look at the landscape. As we implement these electronic health records, we needed to understand what is out there within the health authorities — what systems are in place, what infrastructure needs to be upgraded, what security areas, all of those things — because the electronic health record is kind of a layer on top of all of that. In the end goal it is a layer on top. Right now there are specific initiatives, but we certainly wanted to bring that together. I think that we are working hard to take all of those opportunities.

I don't know if the Auditor General has anything else to add.

J. Doyle: No, it's a very good answer. It seems to me that the more the health authorities can work together to have their systems fit for purpose in their own particular areas, the greater the economy and efficiency and effectiveness that will develop into patient care.

I'd just remind the member that we've actually done some work on patient safety, and we're actually currently doing some further work on patient safety. A different audit will come out later on this year in regard to that. The adverse events that do occur and the cost to the health system that flows from that are large. If those can be avoided in any way, shape or form, then there would obviously be major savings which can be deployed for further patient care.

N. Letnick: I agree. I think I heard you say that you are looking at working with the regional health authority systems so that there isn't duplication — overlap, two sets of records that maybe don't agree with each other — and that's good to hear. Thank you very much.

S. Chandra Herbert: I guess we're often very polite in this committee, and we just deal with the numbers. I'll try to be polite, but I've got to say that I find this report shocking, really, and scandalous.

I'm concerned that while there have been steps taken to deal with the fallout from this — and I appreciate that; that's something you have to do — that doesn't deal with the fact that this problem started and, from what I can read about this, we're five years behind schedule. In terms of provincial taxpayers' cost on this, we're about four times over budget from the earlier estimation. That doesn't even include the health authorities and, from what I understand in the report, that in fact there are compatibility concerns and that seven different health authorities basically could be seven different systems, when we're talking about viewers.

It's a concern to me. I had hoped that given what happened with the convention centre — nearly \$500 million over budget there, because there was no clear business case when it started — that we would have learned that lesson. But it seems from this report that there was no comprehensive tactical plan in how to create the system when we started moving on it. Really, if you don't have a good plan to begin with, it's going to cost you a lot more in the long run.

I guess I've really got two questions. How do we ensure that this kind of thing doesn't happen again? Has there been discipline at the ministry level right on up to the minister, I suppose? That's the first question: how do we stop this kind of thing from happening again? Because it's a big waste of taxpayers' money when we take on a project without appropriate planning, and it costs us in the long run.

[1105]

Also, what are the costs that relate to the health authorities, if they ended up paying out, and where are we

ending up on the hook for that? Because the health authorities, in the end, are paid for by taxpayers as well.

E. McKnight: It's important to correct that the project is not over budget. It was very clear in those estimates, and it's been on record many times.

The initial approvals in the early stages for the electronic health record. There was blanket approval. It did go through Treasury Board. We did have approval. Each year we have gone back to Treasury Board to request funding, as appropriate, as we move down the initiatives.

The initial figure that was outlined in 2002 and 2003 was an estimate. It was not a final budget. If we use relationships to other jurisdictions, we would say that the initiatives have delivered significantly within the budget scope. If we look to our counterparts in Alberta, I don't have their specific numbers, but I know they have invested significantly more within the electronic health records in consideration. It's important to clarify the record around budget.

As to the significance of the question around what plans are in place to prevent this in the future, I think that the comments for the federal Auditors General.... This is an area that's new. Our Auditor General here had said that electronic health records are a challenging new area specifically within the health sector, which has traditionally been within the paper-based world.

I think we have worked hard. In hindsight, it was probably very ambitious to think that the initiative would be completed. I think that now, with the detailed integrated plans across the health sector and our tactical plans.... We have always been rated very high in the individual project management pieces within the ministry. This is talking about bringing it all together and having all of these initiatives come together to be able to gain benefit.

I'm very confident and I think the ministry is very confident that we have good mechanisms in place to ensure good management going forward.

B. Ralston (Chair): Kathy.

S. Chandra Herbert: Sorry, there was a secondary question that wasn't answered.

B. Ralston (Chair): Okay. Well, you did ask a double-barrelled question, so I'll let you ask one more, but then that's it.

S. Chandra Herbert: Thank you. The question was around the health authorities and their different operating systems for e-health and what their costs on that side would be, since we understand the government costs. But in the end it's the same taxpayer.

E. McKnight: That's true. For the audit and for the preparation today, those costs are out of scope, and the

response is not part of the overall audit. We do have projections within the audit for the operating dollars as it relates to these, and within the health authorities.

There are other dollars that they're spending on other clinical systems which are within each authority and that they are accountable to respond to for what they're spending within the electronic health records.

K. Corrigan: I'm trying to decide. There are so many questions I'd like to ask. I'm going to ask a question about process, then.

I'm trying to understand how all of this is going to fit together and what the overall costs are going to be. I guess my question is: what is the process for whoever is actually doing the work? Is this contracted-out work, and if so, how is the work being contracted by government? Are there bids going out to do individual pieces of work? If that's the case, how is it all being put together, and by whom? Is that another contracted piece?

I just have visions.... I've read some of the IT disasters in other jurisdictions — in England, certainly, where it just ended up being mound upon mound of various contractors getting huge contracts and then those contracts increasing in scope and size. I'm trying to get a sense of how the work is being done.

[1110]

E. McKnight: We have not had any recent procurements. All of the procurements for the initiatives that are currently underway were completed, I believe, in 2007. All of those were different. They were large.

There were two or three that were large, complex procurements. The one for the provincial lab information system, which was within government's procurement arm, assisted us within the alternative service delivery areas. It was a large initiative that went through huge due diligence and process to be procured. It follows a strict protocol within government of how those initiatives have to be reported on. So there are annual audits within those.

We have three of those that fall into that category. There is a large contract with Sun Microsystems, which is now Oracle. There is a large contract, not part of this audit but within the public health system, with IBM. We have others where part of the work is done by one of our other large vendors, which is Maximus on our e-drug side. They each have very specific deliverables that they had to deal with for development and system integration.

Our job within the ministry, which is my area of responsibility within the division, is to ensure that we have the good governance in place and that we are monitoring and have those mechanisms in place for each of those vendor relationships.

We also have the assistance of our e-health strategy council as a governance. We have sort of three bodies

that we work with. We have our strategy council. We have a CIO forum within the health sector to assist us as well, and we also have our clinical integration adviser group that we look to as a body for pieces that we need to judge overall.

We have annual audit reports on all of those large initiatives. Those are made publicly available on an annual basis for progress overall, and we have regular kind of reviews. We feel quite strongly that we have good governance in place to manage those.

B. Ralston (Chair): If I might, on page 7 of the report it mentions the already completed procurement processes is being audited at present by the comptroller general. I know she's present here, so perhaps either through the Auditor General, or she can respond herself.

When might that audit of the already completed procurement process be completed and available publicly? I wonder if there is any comment from either the Auditor General or the comptroller general on that. Certainly, the procurement process has not been without its difficulties on occasion.

C. Wenezenki-Yolland: That process is underway and will be completed shortly. As to the report being public, that will be determined once the report has been tabled and government has had an opportunity to review it.

B. Ralston (Chair): Is there any estimated timetable on that? Are you able to give something a little bit more specific?

C. Wenezenki-Yolland: I can't give you a timetable on that at this point.

S. Simpson: As has been mentioned, there are an awful lot of questions here, but I'm going to focus a little bit on the money side. Now, my understanding is the initial cost projection was about \$150 million. That then grew by about 50 percent to \$220 million, I believe. More importantly, the provincial share grew from about \$30 million to about \$110 million, roughly. So it's grown dramatically more than the overall cost, because the federal government put up the first block of money.

The Auditor General has said that as of the time of the writing of his report, the work had not been done to identify the percentage of work done versus the percentage of budget that had been expended, roughly. Are we now firm there? Has that work been done, and are we firm that the provincial share of costs on this is not going to exceed \$110 million?

E. McKnight: That's correct. I just want to make sure, because if we have in the record \$110 million.... This report does not include the public health information systems, so we have to be very careful in the total.... The

total for the e-health overall projection is actually at a number, which is \$262 million. That is the completion overall, with a percentage for government's share.

[1115]

You're correct on.... Infoway's share of commitment is capped at \$110 million. But I think it's really important for the record, again, to say that those were planning estimates for the different initiatives at the very, very beginning. That was not an envelope to work within. We went back every year to Treasury Board to request additional dollars.

So it is not like the estimates that were within an approval envelope. We actually had approval to enter into contracts with Infoway as we went through it on an annual basis as the projects and initiatives evolved. It wasn't a window overall, but we do have a firm estimate on what it's going to take to deliver within the next two years.

S. Simpson: Just a supplemental. What I hear you saying is that the \$110 million is now a firm number in terms of the provincial expenditure. That does not include, though, I believe you said, expenditures by the health authorities on their share of these costs, which of course will also be a provincial taxpayer expense, because we'll pick that up as well.

Do we know what the projected costs for the health authorities will be for them to complete their share of the work?

E. McKnight: Just as a correction, the \$110 million is a recovery amount from Canada Health Infoway. The difference between.... When we look at the full initiative, including the public health initiative, the capital expenditure is estimated to be at \$262 million with \$110 million recovered from Canada Health Infoway. That is a known number that's to be completed overall.

The dollars for the health authority. We are working with the health authorities, and have for the last couple of years. Many of their costs to actually implement are included in that \$262 million.

Current work right now that we did to bring provincial health services on to the lab initiative. Some of the work that we did with Vancouver Coastal with the viewer. We've already paid for that work under that dollar amount.

There is ongoing work that the health authorities would need to do, such as some of the lab standardization. But lab standardization has a multipurpose benefit, not just for this initiative but within their own areas as well. That's an example of lab standardization.

We have an estimating cost of the \$27.4 million of operating costs. Each health authority has a number of e-health initiatives within their own areas. We need to be able to look to them for what their planned expenditures are.

B. Ralston (Chair): I have a couple of questions.

In the federal Auditor General's report she speaks of implementing computerized systems in doctors' offices and references a 2007 study that shows that relatively few Canadian physicians — I think B.C. is no exception — have used computerized systems in their offices. I think that's a fairly common experience when you go for your annual medical checkup.

The question that's posed in that report is: how can the number of primary care doctors using computerized systems be increased significantly? What is the plan as part of implementing this record system to encourage individual family physicians to participate?

E. McKnight: Certainly, in B.C. we do have an initiative with the BCMA. It is outside the scope of this audit, but we do have an initiative.

We had an agreement with the BCMA to fund for incenting practitioners to convert to electronic medical record systems. It is an agreement of \$108 million of funding over a four-year period for physicians. Those dollars go directly to physicians. In consultation with the BCMA, there is a formula that decides how to fund physicians to convert. B.C. is one of the few jurisdictions that has a planned program in place right now.

[1120]

Currently there are over 2,000 physicians enrolled in the initiative. It's called the Physicians Information Technology Office initiative. Over 2,000 enrolled, and we have, as of the other day, almost 1,000 who have actually converted. We now have over 1,000 converted to electronic medical records. It will be, as the Auditor General pointed out in his report.... It's in some of those future questions.

For the province to be able to get the benefit is to ensure that those continue and that we're able to integrate the electronic health records with those electronic medical records in the physician offices. B.C. is in a good position to be able to have that initiative be successful overall.

B. Ralston (Chair): Then a further question from the federal Auditor General's report. She speaks of compatibility. One thing spoken of often is labour mobility, and an aspect of labour mobility is your ability to move your health records. What's the plan to set national standards that would enable that transfer of health records from one jurisdiction as people move or go to university or take a job in another province? What's the plan to set national standards?

I notice that in the national audit Quebec was not a part of it, but that's probably not a surprise. Could you just describe — I understand this would be in the area of future work — what the plan is to set national standards, to ensure that the productivity benefits of a national transferability of health records are available?

E. McKnight: With the initiative with Canada Health Infoway as a federal funder, one of the largest significant criteria for funding is to ensure that we are following and adopting the Canada Health Infoway blueprint. Canada Health Infoway has a blueprint of how electronic health records are to be developed and designed. It is certainly not an easy task to develop to that standard. It's complex, but B.C. has worked very hard to ensure that we're meeting those criteria.

We did receive a letter last year from Richard Alvarez, who is the head of Canada Health Infoway, commending B.C. on being the first jurisdiction to implement the integrated access layer and the first jurisdiction to actually meet the blueprint. We have developed those systems to meet that blueprint. That's a technology kind of success, but it's a huge success overall that lays the foundation for us to be able to ensure that we continue to meet the standards.

Standards are a complex area. It goes right through to not only technology standards and data standards for flow but, as we've certainly realized over the last couple of years in implementing the provincial lab system, lab standards. There are national standards that we are now having all of the health authorities comply with. There are standards within diagnostic imaging. There are even different standards within the lab field itself.

I'm certainly not skilled to speak to those areas. There's a lot of complexity, and we're working with all of our colleagues to try to determine what the best standards are for interoperability.

B. Ralston (Chair): I don't see anyone else having another question out of the federal Auditor General's report.

There's an estimated savings of \$6 billion a year nationally from electronic health records. The question that's posed is: will the cost savings and efficiencies be realized for Canada? When will jurisdictions establish baselines to start measuring the benefits? Have you had an opportunity to consider those questions?

E. McKnight: Yes, we have, and we have looked at various estimates around potential cost savings and in addition, from a patient safety point of view, on benefits. As I did highlight, we have done work to ensure that we have agreed-upon baseline measures.

It's the area that is one of the most challenging under the initiative to get agreement on — what baseline we are working from. We can attempt to do that, and it would be challenging within B.C. It continues to be challenging across the country to agree to what the baseline was overall. Canada Health Infoway — we are looking to that organization to assist us in this area, and we're working very closely.

[1125]

We've also identified in our integrated health sector IM/IT plan one of the biggest components to ensuring

benefits overall. We can put the systems in, and we certainly need to ensure that health authorities have the change management skills, staffing and training in place to be able to ensure that we can achieve the benefits.

That is something that we are working on very, very closely with the health authorities right now to ensure that we actually can accomplish that. Over the next year we need to have the benefits.... We have the plan developed. We need to have it confirmed and signed off with Canada Health Infoway over the next few months, and it will be a big part of what we know the Auditor General has asked us to respond to over the next number of months. So we certainly have work well underway.

S. Simpson: I just want to come back to the money for one more minute. Just so I understand correctly now.... We're saying that the capital cost is now \$262 million, of which \$110 million is federal dollars. The \$152 million is a provincial commitment, and you're saying now that that number is one that the ministry is confident with, is a firm number and is not going to increase.

I believe you said a little over \$27 million of operating costs for the authorities. Are you firm with that number as well?

E. McKnight: On the first part of the question, yes, the ministry is confident on those capital numbers. As I said, that includes the public health system cost as well. That was not part of the audit. Those numbers have been consistent for the last couple of years, and it was a conscious choice to exclude that project out of the audit just for comparison with other jurisdictions. We've been confident with those numbers, and that is what we have gone on record with.

The annual cost we talked about as operating is operating costs out of these initiatives, and we are firm on those operating costs. There are potentially additional operating costs that are outside of the Ministry of Health's jurisdiction, which is in the health authorities. We are working with the health authorities to confirm what that might be. The reason why those aren't firm is because we are looking at a number of multiple initiatives to gain benefits from the electronic health record that will have potential to reduce overall costs.

For example, with the Lower Mainland consolidation, one of the initiatives is within the lab initiative. We have costs that may increase to the health authorities on one side, but they will also have some significant decreases.

Another example is with the DI. On the IT side, they are going to have IT expenditures to ensure that the systems get implemented, but they will have some significant reductions on the test side. So we have not confirmed what those numbers would be overall.

S. Simpson: When will we have the health authority costs, either capital costs for the health authority applied to this or the operating cost as it applies to e-health?

E. McKnight: I can't commit to that number. I think we need to be able to say that we have a good governance mechanism in place. We have a number of initiatives. We are working to continually update the quarterly plans. As we look to the best opportunities to take advantage of benefits overall, if we can bring greater benefits sooner, then we'll look to do that. But I'm not in a position to commit to that operating cost within the health authorities.

R. Lee: Part of my question actually was asked regarding the patients. You know, most of the records previously are on paper in the physician's office. I think the uptake for this system.... Of course, the expenses on system integrations, system development and everything in hardware and software.... But the success of the system is dependent on how many physicians actually are going to use this system.

The numbers compared to other provinces.... What are the uptakes in this province compared to others in terms of percentage? Also, how far should the record for each patient go back — in terms of, say, from birth in hospital — to be relevant to the success of the overall efficiency?

[1130]

Those are my questions. And the costs to the doctors — how much cost would that be? I believe this is not in our budget, so somehow they have to take care of it.

E. McKnight: That's sort of three questions, but I'll try to answer.

B. Ralston (Chair): I can't help that they keep adding on.

E. McKnight: Okay. The first question around how we compare to other jurisdictions. I believe your question relates to the electronic medical records within physician offices. B.C. would have been similar to many other jurisdictions, whereas as a country we lag significantly behind other jurisdictions. Canada would have a poor record in the number of physicians with the EMR usage.

Currently as it stands right now, again, Alberta would be considered a leader in this area. I don't have their numbers, a percentage overall, but their initiative has probably been in place three or four years longer than ours. Our Physician Information Technology Office initiative has been in place on the ground for approximately two years. It matches the four-year BCMA agreement, so it has another two years to go.

As I reported there, we had a target implementation of.... The numbers vary depending on who you talk to, but our target in the initial was to 4,500 physicians in the province. That was the target outcome, and the reason for that is there are many physicians who will not adopt — those who are close to retirement. There are

some in the specialty camps that will not adopt because they are using health authority systems currently today. We have 1,000 that have been converted, and so we do have the 4,500 physician target.

Just with the target, there were — and I don't have that number today; I'd have to get that for you — a number of physicians in the province that were implemented on EMRs before those initiatives started. So the goal at the end of two years is that B.C. would be considered one of the country's leaders in the area of adoption for EMRs.

The funding for that — there is an agreement. It's outlined on the BCMA website with the PITO initiative around what physician compensation, reimbursement, is. There's the whole criteria — what physicians need to be able to meet and respond to. That's all laid out — the dollars. Basically, the initiative is meant to deal with bringing technology in the place but dealing with some of that operating cost, especially for startup, and to deal with some of the complexity for system conversions. That is all outlined on the PITO website in discussions with the BCMA.

I can't remember the third question, so I'll just stop.

R. Lee: I think the third question is: how far do you go back in terms of the patients' records?

E. McKnight: I'm certainly not positioned to answer that question at all. There are many other clinical folks in a position to answer that. We do look to our clinical integration advisory group to assist us in some of those decisions, and we'll continue to work with them. But I certainly couldn't answer that question.

B. Ralston (Chair): One question each. I want to finish up, and then we have one more report, the follow-up report, that I'd like to complete. So if we could head along, beginning with Guy Gentner.

G. Gentner: I'll be to the point. It looks to me that on October 2010, the AG's department will be doing a follow-up. I'm hopeful that we'll have all the costs ready by that time, including the operations side. Maximus, Oracle, IBM.... Well, we're talking startup costs. They'll be looking at the operating and maintaining of the system itself — whoever gets the contract.

A question I have, though, is: how long will the contract extend to? Are we looking at a five-year contract, or is it a ten-year contract?

[1135]

E. McKnight: They all vary depending on the initiative. The Oracle one now, which was previously Sun Microsystems, was a ten-year deal. They had certain aspects for development and some maintenance. The other ones, such as IBM, are a development cost only. It's not a maintenance criterion.

Some of the ones with Maximus.... Again, it's a mix. Some of it's more just on development. So each of the initiatives have an outline of what the vendors are accountable and responsible for and the contract details there.

G. Gentner: This contract or this system has a life span of ten years, and then it's out the window — if the contract is for ten years?

E. McKnight: The initial contract was for ten years. It's not out the window. At the end of the day, the province owns those assets, so those assets will reside within the health authorities. We pay some licensing fees. As I said, they do vary from initiative to initiative. They're not all under the same standard, just because they're all very different initiatives overall. The ones that we deal with just for development — those are kind of standard costs overall. Those assets we'll be able to maintain long past the ten-year period.

S. Chandra Herbert: This question might be more appropriate for the Auditor General, but I guess the question that I have is: how do we get to a place where we don't have a situation again where something like a comprehensive tactical plan isn't put in place before we start moving on a project like this?

I think the lesson here can be applied to any number of ministries. I guess the question to the Auditor General is: how do we have that plan in place, given that we've seen similar situations happen with other ministries? Thinking of the convention centre as one of them.

J. Doyle: I think it's quite straightforward. Whenever any organization or entity walks into or moves towards a major change in what they're doing, they should be properly planned. That's just basic good governance. The application of those principles consistently is the secret. But if things go awry, then what becomes an issue is the response.

I think what we've got in this particular situation is that there has been a good response — from a shaky start to a good response — to a situation where, whilst there's lots of work to be done, I think they have every expectation of it being successful. So the simple answer is good IT management, good project management, skills deployed, setting people up to succeed and making sure that the risks are managed during the conduct of any project. I think that's just a vanilla answer to any work that needs to be done by any organization anywhere in the world.

K. Corrigan: You were mentioning a few minutes ago that some specialists, particularly, are not buying into this system and mentioned that some of them, for example, are using the health authority systems. The question I have is: are we not, at the end of the day, going

to end up with a standardized electronic health record that is accessible everywhere by all the different agencies involved, including individual doctors' offices, and that is going to look the same and function the same?

E. McKnight: Again, sort of two questions there. I think it's important to note that I didn't say that these specialists weren't buying in. There are a number of cases where it's not appropriate for specialists to be using the EMR records and implementing them. They don't need to operate.... This is my understanding. I'm not an expert in this space, but this is what we have, certainly, been provided feedback on.

They are some specialists' tools, but many of the specialists, depending on their discipline — and others can speak more effectively to that — would largely use their health authority clinical system. That could be anything from a specialty lab system, specialty cancer system. It could be a number of different applications. There are multiple applications out there in health authority land to provide those services. I think that's an important factor.

[1140]

We did focus on the GPs within initiatives within the PITO initiative. We continue to work with the BCMA to look at what is appropriate for specialists and the types of specialists that would most benefit from the electronic medical records within their offices. There are some of the specialities, like ophthalmology and some other areas, that have a more standard scope of practice that would work well with electronic medical records.

The answer, I think, is what I alluded to earlier around.... It's important to think of the electronic health record as being a subset of information that is available to physicians anywhere, that they can access that. It is not all the detail. I think we had conversations around the appropriate need to access overall.

There will always be multiple clinical systems within the health authorities. Those will not go away. There always will be medical records within your physicians' offices. The question, at the end of the day, is that we are looking to say: at an integrated level, what is the smallest amount of subset information that would be available on a provincial electronic health record that is, basically, not a detail about your health history? It is more about: you were in a hospital in the last two weeks, and therefore, your physician needs to follow up. That's the goal.

It will not be one system, but it will be an integrated system overall. That is the concept. It's certainly a layer over top.

I think that there are other initiatives going on which were addressed earlier within the Lower Mainland consolidation — some of those areas where the health authorities are looking to ensure that they can standardize different clinical systems. That will certainly assist us in how we integrate over the next few years.

B. Ralston (Chair): Thank you very much to all the presenters.

We have two further items on the agenda. We're obviously not going to get to both, but I would like to attempt to deal with item 5, the follow-up reports. It's relatively straightforward. In the time that remains perhaps we could have two brief presentations. I don't know whether we'll have time for questions, but we can probably deal with that one.

Please begin anytime you're ready.

**Auditor General Report:
Follow-up Report: Updates on the
Implementation of Recommendations
from Recent Reports**

J. Doyle: The follow-up process that's in place has been in place now for a couple of years. Briefly, it is that every six months my office goes back to agencies who have previously been the subject of a report and asks them regarding the progress of the recommendations they've agreed to and that this committee has approved — if that report, indeed, has been through the committee at that stage.

What we get is their responses, in detail, against each recommendation that was originally provided, and we provide a number of pieces of information — each report, summaries and then details of any follow-up work which we may have done.

Recently we've moved to producing these reports in an electronic form. We don't actually produce a copy, although if hard copies are required, naturally we'll be prepared to print one off and provide it to you.

I have with me today Colleen Rose, who's the manager in our communications area — that's the area that actually collects and organizes this particular report — to present our findings for the 31st of March, 2010, follow-up.

[1145]

C. Rose: Over the next few minutes I'd just like to explain a little bit more about why we do engage in follow-up reports; three different forms of follow-up reports; the results of the spring follow-up report, which we just did recently issue; and, of course, the results of a cumulative look at our follow-up reports — in fact, the last four of them.

Taking a look, first, at why we follow up. It's not enough for the Auditor General to simply issue recommendations and just hope that they will be followed up on and acted upon. As such, both the audited agency and Public Accounts Committee have the opportunity to review and, of course, engage with the recommendations.

Following up is a critical step in ensuring that the recommendations have a positive influence and that British Columbians do receive full value from our services. Therefore, beginning in October 2008 we did begin to issue follow-up reports every six months.

Taking a look at the three forms of follow-up reports that we do issue, they look like action plans, agency self-assessments or progress audits. We'll just take a look at each of those individually very briefly.

The first form of follow-up is the action plan. Within three months of publishing the initial report, agencies are asked to provide an action plan describing how they will implement the recommendations and by when. Often we're able to publish the action plan as part of the formal report — in fact, in the entity's formal response within that. If not available at that time, the response is published on our website as soon as it's received.

The second form of follow-up, the agency self-assessments, is exactly that. It's where agencies provide self-assessments of the progress they have made in implementing our recommendations and, of course, their plans going forward. These submissions are published unedited and in their entirety so that readers can assess, themselves, whether or not that progress is satisfactory.

To be clear, they are management's representations. While we read each update and, in some cases, discuss them with the entity, they are not audited in any way, and we cannot offer any assurance concerning fairness, completeness and accuracy.

The initial follow-up is conducted approximately six months to one year after the report is issued, and we expect that most recommendations will be cleared at that time. Subsequent follow-ups may be required on outstanding recommendations and would be published within one year of the initial follow-up. Of course, these, too, would be unedited self-assessments from the agency.

The third form of follow-up involves auditing the self-assessment of certain recommendations. These are progress audits. Although we have yet to select any submissions for this level of examination, we anticipate doing so as we go forward.

Moving on, taking a look at the results of our spring follow-up report, as you can see in the pie chart, the two green pieces of the pie represent 33 of the 51 recommendations that were included in this report — ten specific reports that were published in here. That represents about 65 percent of the recommendations that are already fully or substantially implemented or where the agency chose to take alternative action to address the recommendations.

In the blue piece of the chart the 33 percent of the recommendations have been partially implemented, and only 2 percent, or one single recommendation, has had no substantial action taken.

Finally, looking at accumulative results. This is going back four years, since October 2008. At that time we're looking at 28 individual reports that form these statistics, totalling 467 recommendations. When you roll the results up — if you look at the green pieces of the pie — 430 of the 467, or 92 percent, of the recommendations followed up on since October 2008 have been fully

or substantially implemented or alternative action has been taken.

In blue, 35 of the recommendations, or 7 percent, have been partially implemented, and just under 1 percent, or two, of the 467 recommendations have had no substantial action taken.

That concludes our presentation at this time.

B. Ralston (Chair): Thank you very much.

Once the report of the comptroller general is finished, I think we'll be at 12 o'clock, so I think, by dint of the time, we'll have to adjourn. I know that members may be disappointed, but there we are.

[1150]

C. Wenezenki-Yolland: I think you might find I can go quite quickly through this presentation. Some of it is probably a little repetitive of the Auditor General's report, and I guess his report kind of said it all.

I would like to start out by saying that the government takes the Auditor General's recommendations extremely seriously. As the B.C. Public Service continually tries to improve its programs and its service delivery to the citizens of B.C., we are absolutely happy to receive whatever feedback and information we can to continually improve those programs. I believe that the action taken substantially demonstrates the seriousness with which we take those recommendations and the commitment to continuously improve.

In the context of the recommendations with these reports, it is the ministries' responsibilities to actually follow through on the reports and implement the recommendations. As a central agency, I'm here to reply on behalf of government on the progress, but I cannot speak to the specific recommendations that have or have not been implemented or speak to the specifics of the programs in the follow-up reports. I certainly can tell you that there has been substantial progress made and continues to be made.

As the Auditor General said, 94 percent of the recommendations are fully or partially implemented. In cases where the ministry has found a better way or an alternative way of addressing the recommendation, because some context and things do change, there is six percent where there has been an alternative action, with only — if you look at the 467 recommendations — two recommendations remaining not acted upon at this time. That is extremely significant progress.

In the context of the follow-up reports, there were actually ten follow-up reports requested by the Auditor General's office. Eight of those were provided. I understand that for one of those, the B.C. Arts Council, there was a response provided, but for some reason, it missed the time frame or did not get captured in this report. I have asked Lorna to follow up to see if perhaps that could be included in the Auditor General's next summary of these reports.

Also, there was one follow-up report in which case the ministry did not provide a response to the Auditor General, and I believe the ministry needs to respond as to why that was. I cannot speak on their behalf.

We do believe this is a valuable process. It provides good information to the Public Accounts Committee and government in monitoring the actions of the ministries and their accountability for responding to the recommendations that they have received. It also provides us, as central agencies, with a good understanding of where the ministries are and also allows information for us in our governance and oversight roles. So we do find this a very valuable process overall and are happy to participate in the process.

Then just a concluding summary of the results, and the recommendations and our commitment to continuing to improve.

B. Ralston (Chair): Thanks very much. In the couple of minutes that remain, I suppose there's time for one question, or two maybe.

S. Chandra Herbert: Just a quick question. I understand these are follow-up reports on audits done on certain government ministries or government agencies. The question I have is.... Of course, the hope of these audits is that other ministries and other agencies will adopt a number of the findings here. Has there ever been any thought given to just doing spot checks on other ministries or other agencies just to see the effect of these kinds of reports on them?

[1155]

C. Wenezenki-Yolland: We could probably both answer from two different perspectives. I can answer from being responsible for governance internal to government, and then the Auditor General can answer from his external perspective.

Internally, yes, we do. Lorna Pritchard, who is here with me today, is my director of governance in my financial management branch. We do share information, observations and findings from the Auditor General's reports with broader groups. You heard people speak earlier about the avenues that are open for the CIOs across government to share that information.

We have similar ways of sharing that information with the chief financial officers from across government, as well as a group of ADMs of corporate services across government who have responsibility for IM/IT, finance,

typically strategic planning within the individual ministries. So we do that.

We also look at the Auditor General's reports to see opportunities for systemic issues as part of continually improving the governance within government. We do go through the reports. We look for opportunities. We use that information to share back with the ministries. We use it to refine our policies and our governance.

We also use it to inform our education. We provide a lot of training for B.C. public servants. Information that we glean from these processes is then incorporated into that training to continuously improve the organization. We do a lot in that regard.

B. Ralston (Chair): This will be the last question, and then we'll adjourn after the answer.

V. Huntington: Basically, I wanted to know whether the Auditor General's office was satisfied with either the alternate solutions that are made or with the ministry's responses to the recommendations. Do you audit those at all, given that they're separately accountable?

J. Doyle: It's management's responsibility to respond to the recommendations. What we've done here — or what they've done — is document their response. The next stage of this process is to actually go and check the assertions made by management to see whether the evidence exists underneath that.

We will be doing some of that over the next period of time. Every six months, when I've produced one of these reports, I've asked members of the committee if they have any particular suggestions as to which ones we should look at. I'll be willing to receive them. I can't guarantee that we can do them all, but I'm certainly willing to have a look.

B. Ralston (Chair): Thank you very much. I think that will conclude the proceedings. Thank you to everyone. It was a fairly vigorous agenda today, but I think we did accomplish a fair bit.

The next meetings will be June 9 and 10, I believe. The agenda will be circulated a little bit further in advance than the one that was circulated for this meeting. I apologize for that, but it has been fairly hectic here in the Legislature in the last little while.

Thank you, and we're adjourned.

The committee adjourned at 11:58 a.m.

HANSARD SERVICES

Director
Jo-Anne Kern

Manager of Print Production
Robert Sutherland

Post-Production Team Leader
Christine Fedoruk

Editorial Team Leaders
Laurel Bernard, Janet Brazier, Robyn Swanson

Senior Editor — Galleys
Heather Bright

Technical Operations Officers
Pamela Holmes, Emily Jacques, Dan Kerr

Indexers
Shannon Ash, Julie McClung, Robin Rohrmoser

Researchers
Jaime Apolonio, Mike Beninger

Editors
Anton Baer, Aaron Ellingsen, Deirdre Gotto, Margaret Gracie,
Jane Grainger, Betsy Gray, Iris Gray, Linda Guy, Barb Horricks,
Bill Hrick, Paula Lee, Nicole Lindsay, Donna McCloskey,
Bob McIntosh, Anne Maclean, Constance Maskery, Jill Milkert,
Lind Miller, Lou Mitchell, Karol Morris, Dorothy Pearson,
Erik Pedersen, Peggy Pedersen, Janet Pink, Amy Reiswig,
Heather Warren, Arlene Wells, Glenn Wigmore

Published by British Columbia Hansard Services, and printed under the authority of the Speaker.

www.leg.bc.ca/cmt

Hansard Services publishes transcripts both in print and on the Internet.
Chamber debates are broadcast on television and webcast on the Internet.
Question Period podcasts are available on the Internet.