



HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Accounts

PACP • NUMBER 129 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, February 26, 2019

—
Chair

The Honourable Kevin Sorenson

Standing Committee on Public Accounts

Tuesday, February 26, 2019

• (0845)

[English]

The Chair (Hon. Kevin Sorenson (Battle River—Crowfoot, CPC)): Good morning, colleagues.

This is meeting 129 of the Standing Committee on Public Accounts for Tuesday, February 26, 2019.

We're here today in consideration of report 4, "Physical Security at Canada's Missions Abroad—Global Affairs Canada", of the 2018 fall reports of the Auditor General of Canada.

We're honoured to have with us from the Office of the Auditor General, Jerome Berthelette, assistant auditor general, and Carol McCalla, principal.

We also have, from the Department of Foreign Affairs, Trade and Development, Ian Shugart, deputy minister of foreign affairs; Heather Jeffrey, assistant deputy minister, consular, emergency management and security; and Dan Danagher, assistant deputy minister, international platform.

We welcome you all here. I would also remind members that we are televised today.

We will turn to Mr. Berthelette for his opening statement.

Mr. Jerome Berthelette (Assistant Auditor General, Performance Audit, Office of the Auditor General): Mr. Chair, thank you for this opportunity to discuss our fall 2018 report on physical security at Canada's missions abroad. This audit examined whether Global Affairs Canada had physical security measures in place at its missions for the effective protection of its staff and assets.

Physical security measures include safeguards such as fences, and vehicle barriers or alarm systems to prevent unauthorized access or attempts to cause harm. As an employer, the department is responsible for the safety and security of its staff. More than half the mission's staff members work in dangerous locations that require protective security measures.

Overall, we found that Global Affairs Canada had not kept pace with evolving security threats at its missions abroad. Over the past decade, the department received \$650 million to upgrade the physical security of its higher-threat missions. We found insufficient documentation to demonstrate how its physical security projects were prioritized to ensure that the most critical needs would be met. The department had identified more than 200 security measures that

were urgently needed across all its missions, but it did not yet have a plan in place for their implementation.

We found weaknesses in the security assessments conducted by Global Affairs Canada at its missions. For example, more than one-third of threat assessments were out of date and many of the vulnerability assessments were incomplete or failed to recommend safeguards to resolve identified weaknesses. In fact, baseline security standards that specified the safeguards needed to protect missions against direct physical attack were still under development at the time of our audit.

Without these standards, Global Affairs Canada cannot comprehensively assess the measures needed for the effective protection of staff and assets across its missions, yet the department is responsible for the safety of its staff working at missions abroad, and security upgrades to its many missions are urgently needed.

• (0850)

[Translation]

We examined the security measures in place at six high-risk missions and found significant security deficiencies at all six. The department had known about several of these deficiencies for years, yet it had not put in place all the recommended measures to resolve them, such as improved video surveillance, alarms or vehicle barriers.

Security officials at these missions didn't know the status of the approved physical security upgrades or what interim measures were needed to mitigate the identified security risks. Most of the department's capital projects to upgrade security were at least three years behind schedule and were taking almost twice as long to complete as originally planned. We found that these delays were caused by weaknesses in the department's project management and oversight. For example, construction project plans didn't sufficiently assess and build into the schedule the risks unique to the host country, such as the time needed to obtain permits.

Other federal entities, such as Defence Construction Canada, have specialized knowledge and experience in international construction projects that could help Global Affairs Canada ensure that important security upgrades are delivered on time and on budget.

Finally, we found that more than one third of the staff members working in some of the most dangerous locations hadn't taken mandatory security awareness training. As a result, Global Affairs Canada didn't have assurance that its staff members had the appropriate level of security awareness needed for their effective protection. We made five recommendations, and Global Affairs Canada agreed with all of them.

This concludes my opening remarks. We would be pleased to answer any questions the committee may have.

Thank you.

[*English*]

The Chair: Thank you very much, Mr. Berthelette.

We'll now move to Mr. Shugart.

Welcome.

Mr. Ian Shugart (Deputy Minister of Foreign Affairs, Department of Foreign Affairs, Trade and Development): Thank you, Chair, and good morning, ladies and gentlemen.

I would like to say before giving my official remarks this morning that I am accustomed to sitting beside the late Michael Ferguson. Through you, Chair, could I extend our sympathy to Mr. Ferguson's family, but also to his colleagues and to members of this committee who worked so closely with the late Auditor General?

At Global Affairs Canada, serving Canada and Canadians abroad is our mandate. To deliver on this mandate we regard our responsibility for the protection of our staff, visitors and assets at Canada's international mission network as our key priority.

To this end, we continually review our security posture, procedures and systems to ensure they are robust and effective, and that they respond to the latest developments in the security context. This review process involves not only the physical security measures that have been assessed in the OAG audit, but also our operational security procedures and our security intelligence information. Collectively, these three security pillars work together to create layers of protection required for staff, visitors, information and physical assets. We believe that no one pillar can be viewed in isolation, and in many contexts specific elements, for example deploying guards, can be strengthened to compensate and provide mitigation for another area that may not be as strong. This interlinked approach is consistent with that taken by other foreign ministries.

Global Affairs Canada welcomes the Auditor General's report on the physical security pillar, and as Mr. Berthelette has said, we have accepted all of the recommendations. These recommendations are broadly aligned with those made in a recent 2018 internal audit conducted by the department under its current risk-based audit plan. The internal audit made five recommendations, which were tabled before our departmental audit committee in March of last year.

We are particularly pleased that the Office of the Auditor General relied on internal audit results to inform its observations, findings and recommendations. As members of the committee know, that does not always happen. In particular, the Auditor General relied on the internal audit work conducted at four of our missions abroad and

then conducted its own independent work at two more missions. We appreciate the collaboration and welcome the consistency of the findings.

Last year the department began to implement the recommendations made in the internal audit and has since deepened its action in the process of implementing the Auditor General's recommendations. The action plan in response to both audits is largely being addressed through the \$1.8 billion in funding—that's over a 10-year period—the department received in the 2017 fall economic statement as a part of the duty of care package to improve security at missions abroad.

To ensure that these investments are effectively prioritized, tracked and implemented, Global Affairs has established a new global security framework. The framework explicitly integrates risk management principles into security policy development and decision-making and enables risk-based priority setting and resource allocation. The framework also provides the flexibility to adapt more quickly to the changing international security environment and to address future security needs as they emerge.

In addition, security assessments, which include both threat assessments and vulnerability assessments, have transitioned from a one-size-fits-all cyclical approach to a risk-based approach that prioritizes more frequent assessments of our highest risk environments. This change has also been supported by more regular and proactive communications and linkages with mission security teams on the ground. For example, part of the duty-of-care investments has been used to acquire and implement an enhanced security information management system that is being used to document and track security requirements by missions to ensure that they're effectively monitored and efficiently addressed.

● (0855)

As well, in line with the audit observations related to strengthening governance and clarifying roles and responsibilities, we have strengthened and will continue to strengthen our internal governance to better coordinate decision-making and enhance the consistency and effective delivery of physical security projects at our missions abroad.

More specifically, decision-making for the allocation of resources to all major capital projects has been streamlined with senior level oversight by an ADM level committee. The committee meets monthly and includes the departmental security officer as a key member, which is in line with one of the audit recommendations.

The DSO's membership in the committee reflects the fact that many of our real property projects include physical security aspects. The committee is critical to ensuring strengthened project management for real property projects and for improving their timely delivery. As well, project delivery is being supported now by a recently created project management office. The office is responsible for maintaining quality assurance, the timeliness of project delivery, and monitoring and reporting on results.

The AG's report also highlighted the need for the department to initiate discussions with other government departments and to adopt best practices. In this respect, we continue to learn from our federal colleagues as well as with respected project management divisions of our foreign counterparts worldwide. These lessons will also contribute to, and benefit from, the Government of Canada's project management community of practice.

While the new governance structure is strengthening project management oversight, and best practices continue to be adopted, it is also true that physical security projects abroad are often undertaken in complex and, at times, unstable overseas environments where foreign laws, policies and other local conditions are outside our control. Events and changing circumstances can seriously impede project delivery and sometimes call for alternative mitigation. New tracking systems will monitor and flag those areas where such alternative mitigation is required.

● (0900)

[Translation]

Finally, an additional area covered by the Auditor General that wasn't included in the scope of our internal audit relates to security training.

In line with the recommendations, and as part of the duty of care investment package, we have work under way to strengthen our security competencies and capabilities.

The security training program has been revamped and will be broadened to improve the preparedness of departmental staff and locally engaged staff. A new mandatory five-day security training course has been added to the learning curriculum for staff heading to hazardous environments. Other courses have been updated to keep pace with evolving security needs. All training is designed to respond to operational needs and to mitigate risks abroad. A tracking solution has also been implemented to document and monitor training completed.

In closing, I would note that the physical security function examined in this audit comprises only one component within a broad range of measures that are employed in an integrated fashion to enhance the protection of our staff, visitors, information and assets abroad.

Additional security measures, such as security briefings, security equipment, real-time intelligence, personnel movement protocols and guard protection provide critical security enhancements and additional layers of mitigation.

In extreme cases, where risks are elevated, or where physical security measures require enhancements that can't be achieved, restrictive movement protocols and adjustments to mission posture

are implemented to compensate, up to and including staff withdrawals and mission closure as required to ensure the safety and security of all our employees. This has recently been the case in our missions in Caracas, Venezuela and Havana, Cuba.

Unquestionably, the safety of our employees is our duty and my foremost preoccupation. The modernization of our approach to all the elements required to operate securely, effectively and safely abroad is well under way and the full implementation of the audit recommendations is being facilitated through the duty of care investments recently announced.

We're already seeing the real impact of these efforts. The Auditor General's support for this direction is both valued and encouraging.

● (0905)

[English]

I will be assisted by my colleagues. Dan runs our international platform, and Heather is specifically charged with our consular program, as well as our security operations and emergency management. Heather and I were before the committee recently.

Thank you, Chair.

The Chair: Thank you, Mr. Shugart.

We'll now move to the first round of questioning, a seven-minute round.

We'll go to Madam Mendès.

[Translation]

Mrs. Alexandra Mendès (Brossard—Saint-Lambert, Lib.): Thank you, Mr. Chair.

I want to thank all the witnesses for joining us this morning. I apologize for being late.

Mr. Shugart, I'll start with the elephant in the room, even though it's not covered by the study in question. I'm talking about Cuba, which is of interest to the media. You just told us that Canada has withdrawn diplomatic staff from Havana. Since this case directly concerns the security of staff and therefore the content of the report that we're studying, could you tell us more about it, knowing that there may be limits to what you can say since the case is before the courts? That would be appreciated.

Mr. Ian Shugart: We're undoubtedly very concerned about many aspects of this case. The case clearly shows the limits that we face, in part because of privacy legislation and the fact that the issue is before the courts.

In addition, we must note that we have limited knowledge of what happened and the nature of the risks faced by our employees.

[English]

We are perfectly happy to answer questions in this regard, notwithstanding the limits.

I can tell you that we have learned as we have proceeded. We have worked with the Cuban authorities to the maximum degree possible. We have worked with our American colleagues to learn as much as we can. And we have applied more measures to safeguard our employees in Havana, including restricting the footprint in Havana to respond to continuing concerns and incidents there. We will continue to apply that standard of care.

We don't always know where the threats are going to come from. In this particular case, it is especially troubling that we don't know precisely what the source of the problem is. We have provided the appropriate diagnostic testing and care. We continue to meet with the staff concerned. Those cases represent a wide variety of circumstances and of reactions within those families, our staff and their dependants, so there is no single pattern that points very clearly to a problem and/or the nature of the problem.

As I said, we have learned as we've gone; we know more than we did in the early days. But this is an extremely troubling situation and we are open to whatever technical advice we are receiving from medical personnel and from our colleagues, as well as from other agencies we're working with, such as the RCMP and so on.

● (0910)

Mrs. Alexandra Mendès: That brings me to the question of the precise physical security of staff in our missions. Because of the very incomprehensible, if you wish, nature of the problem that affected staff, it's almost impossible to ensure complete security when you don't really know what's threatening you.

There's still a huge investigation going on. I'm presuming that has not stopped. Have we taken all personnel out from Cuba? Are there still staff there?

Mr. Ian Shugart: We have a reduced footprint.

Mrs. Alexandra Mendès: Are they in the same buildings?

Mr. Ian Shugart: Yes. I think you'll appreciate that I want to be careful about going into too much detail, but as far as we know, we have full information about where staff have been affected physically—what locations—and we take that into account.

We have reduced the footprint to provide the core support to Canadians who visit Cuba. As you know, that is very substantial, as Canadian companies work in Cuba. We have, in prudence, not exposed more staff. We continue to assess the nature of the exposure, and we do that virtually continuously with the staff in Cuba. We have all—Heather particularly, and the ADM responsible for the geographic region—been in touch with the head of mission and with the staff who have returned.

Mrs. Alexandra Mendès: Speaking of the head of mission, what is their authority to change the nature of the security around the mission when instances like this erupt?

Mr. Ian Shugart: I think you're referring now more generally—

Mrs. Alexandra Mendès: More generally. Yes, absolutely.

Mr. Ian Shugart: The head of mission is effectively the CEO of Canada corp. in that location.

However, it is a collaborative effort between headquarters, which has to apply standard protocols and also has some objectivity of distance that can look at the data and the assessment and make final

decisions on security posture, and the mission. But on the ground, the head of mission has considerable scope, including authority with respect to other departments located in our missions, to manage the security posture.

I think we would empathize that it's a highly collaborative thing between the mission and headquarters.

Mrs. Alexandra Mendès: Thank you.

The Chair: Mr. Kelly, please.

You have seven minutes.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): The ongoing news on this Cuba episode really brings into focus the very real dangers and threats that exist to our missions.

Your answers to the questions by Madam Mendès about trying to quantify or to understand the threats that exist, I think are going to be cold comfort for the 7,800 employees in Canada's foreign missions. We have an Auditor General's report that is full of examples of failures to address known threats. We're not even dealing with the threats we know about, never mind new threats that are only beginning to be understood.

I bring to your attention, under paragraph 4.24, the following:

security measures recommended for implementation at each of the six missions had not been tracked or prioritized for action. For example, at one mission, the perimeter was identified in 2011 as a critical vulnerability requiring very urgent attention. But during our site visit in 2018, we found that this issue had not yet been resolved....

You identified a critical threat in 2011, and in 2018 it hadn't been addressed.

This is a committee where we demand accountability for how the funds authorized by Parliament have been spent to execute the policy of the government. We have a report full of examples of failures to protect our own employees in foreign missions.

Please explain why there have been these failures to implement known security mitigation measures.

● (0915)

Mr. Ian Shugart: First, I would say that we accept all of these findings and the implications of the findings. As I said, we found them ourselves in our own internal audit.

Second, we make use of the resources that we have available to us at any given time, and we have to allocate those resources on the basis of current need. In some cases, the more urgent security needs would account for the delay in identified projects or the pacing of projects.

Third, as I indicated, and as the Auditor General's office indicated, the documentation of projects both for tracking needs and for tracking implementation was, as is so often the case, not there. We have now put those tracking systems in place.

These cases that are described are accurate, and we have put in place, as I indicated in my comments, the measures to know exactly where we are in our projects and to make decisions on the basis of risks as they emerge over time.

Mr. Pat Kelly: The report identified that some of your funding almost lapsed or had to be retained by special applications. I do understand that you must deal with what is allocated, but you didn't even spend what was allocated. I don't find it an acceptable reason for not having implemented known security improvements when you have lapsing money. It's good that your internal audit appears to at least match the Auditor General's. That's positive, and it contrasts with some other studies that have been before this committee.

Mr. Berthelette, you visited two sites yourself and relied on their audit. I'll have you comment on the congruency of the internal audit and what you found. This is an important point if it's just not practical for you to audit these physical sites in most cases.

Mr. Jerome Berthelette: Mr. Chair, I'll ask my colleague, Ms. McCalla, to answer that question.

The Chair: Ms. McCalla.

Ms. Carol McCalla (Principal, Office of the Auditor General): Thank you, Mr. Chair.

We did rely on the the recent internal audit done by Global Affairs on physical security. We had worked with them very closely to ensure we could do that. In our and their view this would provide the most value to Global Affairs. They had done a series of site visits. The objective of their audit was to determine, out of the past tranche of funding Global Affairs had received to upgrade physical security, what upgrades had indeed been done. They developed a test program in their various missions to identify the status of the physical security measures that were on the books to be implemented. We had developed a similar audit approach with Global Affairs to go to additional sites and rely on their sites, and together we would have a much better picture with six sites.

● (0920)

Mr. Pat Kelly: I want to get back to Mr. Shugart about how we got to this point. The Auditor General said the department's capacity to deliver its security projects was limited. Many positions that dealt with capital projects at missions abroad were vacant, and the department had not conducted lessons learned or studies on past failures. Failures of project oversight and project management were identified as problems in the security shortcomings. Again you were here to account for the department and for the funds allocated for that. How do you explain these kinds of failures?

The Chair: Mr. Shugart, please be quick.

Mr. Ian Shugart: Chair, I think it is well known to this committee that project management has been a vulnerability across government operations for many years. In many places those lessons are often being learned the very painful way. At Global Affairs we are learning those lessons and have put measures in place to improve project management.

The Chair: I think we'd better leave it there; we're over time now. We can come to that a little later.

We'll now move to Mr. Christopherson for seven minutes, please.

Mr. David Christopherson (Hamilton Centre, NDP): It's good to see you again. Thank you all for being here.

Starting with the focus of the audit, it states the following in paragraph 4.6:

This audit focused on whether Global Affairs Canada met its physical security needs at missions abroad to protect its staff and assets.

The overall message in paragraph is:

Overall, Global Affairs Canada had not taken all measures needed to keep pace with evolving security threats at its missions abroad.

Further, in the conclusions in paragraph 4.78, it states:

We concluded that Global Affairs Canada did not fully meet its physical security needs at missions abroad to protect its staff and assets.

I find this really surprising for a whole bunch of reasons, not the least of which is that in terms of governance, like it or not, security is a huge issue. In your department, it's what you do. I was really surprised and disappointed that something so important in a department that deals with security as its major focus would have these problems with obvious stuff. This isn't like deep intelligence and the analysis going wrong. These are basic things. It's really disconcerting when you think about how easily things can turn.

One of the greatest examples—and it's an extreme example, but a real one—was Iran in 1979. Going from no problem at all to all of sudden a crisis that can bog down a government and a nation for years, if not decades, can happen in a blink. These are the first lines of defence. I just find it passing strange.

I'll just leave that there. If you want to comment on that in some way, you can. Otherwise, I'm just going to move on to my questions.

I'm going to pick up where you were just recently. You talked about managing projects. There's been a vulnerability for governments for years, as we know. However, the Auditor General makes reference in paragraph 4.63 to the following:

Other federal entities that deliver security projects internationally have knowledge and expertise that, in our view, could benefit Global Affairs Canada. For example, Defence Construction Canada runs construction and engineering projects internationally, many with unique security requirements. It delivers most of its projects for National Defence, but it also provides services to other government entities, such as Communications Security Establishment Canada. In our 2017 special examination, we found that Defence Construction Canada did a good job

—shout out to them—

of managing construction projects and contracts. For example, it carried out contracts according to the client's requirements, and it met deadlines and budgets.

How about that? You said there are vulnerabilities, but the Auditor General was able to point to a major player in the development of projects that does a really good job. From what I know about security, when you're starting to talk of Communications Security Establishment Canada, we're getting into some really serious stuff. These have to be trusted folks.

Why didn't you go down this road? Why did you let yourself...?

The last thing I'll say concerns the chart on page 13. Holy smokes. Where were the grown-ups in the room?

● (0925)

The Chair: Mr. Shugart.

Mr. Ian Shugart: Again, we do audits and we put this on our risk-based internal audit plan precisely so that we have an accurate picture of the vulnerabilities in our performance on security. While I fully accept the conclusions that have been made in both of these audits—ours and the AG's—we are not in any way minimizing those faults and vulnerabilities.

Equally, I don't want Canadians to have the impression, through our discussion this morning, that no security provisions are made or that no extensive work has been done. These are vulnerabilities and faults that are important and have been identified. It is not an indictment of our security posture across our mission network.

I'd like Dan to comment on the defence organization and the role it could have played in the past, and is playing now as we have accepted the audit recommendation and work with them.

Mr. David Christopherson: Just before you go there—and I'll give you that opportunity—I want to comment that I wholeheartedly support your comment about the security. These are issues to be dealt with, but they do not reflect the overall.... I've been to a lot of the hot spots and embassies. I've been very fortunate to have done a fair bit of travel to what is on your list there. I've been to the Egyptian embassy twice. That's a hotbed, and yet the security is fantastic.

Nonetheless, if I may also say this, some of us were talking, too, and are a little concerned about what are the implications of this out in the public domain. Does it suggest to folks that there is a free-for-all on Canadian international assets? That's not the case at all. I agree with you entirely that this is a maintenance check and not a need to overhaul the transmission and the engine. I agree with you on that.

I'm sorry. Go ahead, please, sir.

Mr. Ian Shugart: There's rust too.

Voices: Oh, oh!

Mr. David Christopherson: Yes. That's my next question.

Mr. Dan Danagher (Assistant Deputy Minister, International Platform, Department of Foreign Affairs, Trade and Development): Very simply, on the Defence Construction, we accepted the recommendation from the auditing team last year. We've already started construction—roughly a year ago—with Defence Construction to learn lessons about how they do it—

Mr. David Christopherson: Is there a reason why you wouldn't just use them? Is that just not a practical thing for you?

Mr. Dan Danagher: It's really not their mandate or their expertise to build missions that provide the range of international programs

that we do in our missions abroad. Nevertheless, there are things that we can do together, and we can learn from them. We're taking it in a very open way.

The Chair: Your time is up, David. We'll come back to you.

We'll now move to Mr. Arya, please, for seven minutes.

Mr. Chandra Arya (Nepean, Lib.): Before coming to this particular part of the report, I would like to go back to the situation in Cuba. I understand that there are many unknowns there. In the court case that has been filed, there was one sentence that really bothered me. I hope it is not true. Let me read it:

The statement of claim contends that Global Affairs "actively interfered with the plaintiffs' attempts to receive proper health care, including going so far as instructing hospitals to stop testing and treating them."

I hope it is not true.

The Chair: Mr. Shugart.

Mr. Ian Shugart: Chair, I will defer to Heather on this point, but I would say, with respect, that I don't think this is the forum for me to respond to specific claims in the suit. I don't say that to withhold information, but it is a legal action that has been taken that the claimants are perfectly entitled to take. But I think we should respond through the appropriate venues.

Is there anything we could say in addition to that? I think we should be very careful.

● (0930)

Ms. Heather Jeffrey (Assistant Deputy Minister, Consular, Emergency Management and Security, Department of Foreign Affairs, Trade and Development): I would just add that as part of the whole-of-government approach we've been taking, we have worked with a number of different medical institutions—hospitals, primary physicians, health care providers, including Dalhousie University, which is very involved in a research program—as well as with our international counterparts to put in place the best possible service we can for our staff.

The Chair: I will just say, on counsel from our clerk here, that we fully understand that something that is before the courts does not have to be disclosed here. If we did that, we would go in camera, and that would be a longer process. Cuba isn't mentioned in the report. We used that as an example.

This is not being taken off your time either. Just make sure that we stay focused on the report. Carry on, Mr. Arya.

Mr. Chandra Arya: Thank you.

My next question is for the Auditor General's office. I know this report deals with the physical security part of it. There are two other parts of the security pillars, as Mr. Shugart mentioned. Are there any reasons why you didn't look at security as a whole and why you limited yourself to the physical structure?

The Chair: Madam McCalla.

Ms. Carol McCalla: Our audit did focus on the physical security, knowing that it indeed does work in tandem with operational security and intelligence to make up the entire security posture of a mission abroad. We focused in on physical security because Global Affairs had received substantial funding to upgrade its physical security at missions abroad, and in 2017 it received another \$1.8 billion to upgrade its physical security at missions abroad.

We wanted to understand how well it had worked over the past decade to upgrade its security and what needed to be done to ensure success for the next tranche of funding. We focused in on what was the physical security in place at its missions and then to understand why what improvements needed to be made for the next tranche of funding.

Mr. Chandra Arya: Having lived and worked in several countries, I understand the complexities involved in construction of project implementation related to physical buildings there. As the department has mentioned they were aware of some of the things that were required to improve the physical infrastructure, did you look into the alternative mitigation measures the department may have undertaken to work on this?

Ms. Carol McCalla: In our six missions that we examined, we looked at what security measures had been recommended by Global Affairs security staff. We looked at their threat and vulnerability assessments, and those examined both the physical and operational security measures. They made a number of recommendations for what needed to be put in place at the missions, given the threat environment.

We understood that those assessments did identify critical vulnerabilities. As a result, it also identified several interim measures that needed to take place, such as additional operational security, additional guards and additional surveillance in general across its missions, and in each of the vulnerability assessments we had looked at.

What we found, though, was that at the missions there was not a good understanding of what those measures needed to be. Everyone was quite clear about what the critical vulnerability was, but they weren't necessarily clear about what mitigating interim measures needed to be in place, and we did find that some of those interim measures were not in place. Some of them were in place and some of them weren't, but there wasn't an understanding of why some were in place and why others weren't in place so that there would be an overall understanding of the security posture of the mission. Therefore, we recommended that that be well documented. Especially in an organization like Global Affairs, where there is cyclical rotation of the staff, we recommended that staff be very clear about what's required—particularly as these vulnerability assessments are not necessarily done every year—so that there would be a good understanding across heads of mission and with the security officials within the missions as well.

• (0935)

Mr. Chandra Arya: Mr. Shugart, do you have a comment on that?

Mr. Ian Shugart: I would be delighted to. Indeed, I was wondering about asking the chair if I could make a comment on this.

My experience as deputy minister in three departments now points to a tendency across government that I think would be of broad interest to the public accounts committee. It is that frequently these faults that are exposed—rightly—in audits point to an inclination to do things rather than to plan, track and document things. As well, when you're dealing with finite resources, often putting in place the information systems and documentary systems is seen, or has been seen, as less inherently valuable than actually spending the money on the core purpose.

However, when you don't do that, what we have found over and over again is that you actually pay for it, sometimes through really bad AG reports, but also in an ability to know exactly what you're dealing with.

The proper planning and documentation actually does help manage the risk. Also, I think, as a general proposition, that is something we have been learning across government—painfully—and you can see how that lesson is driving our way forward in this particular case.

The Chair: Thank you very much, Mr. Shugart.

We'll now move into the second round of questioning. I'll remind you that they're typically five-minute rounds.

Mr. Kelly.

Mr. Pat Kelly: I'm going to let Ms. Kusie take my time.

Mrs. Stephanie Kusie (Calgary Midnapore, CPC): Thank you, Mr. Kelly, and thank you, Mr. Chair.

[*Translation*]

Thank you all for being here this morning. It's very nice to see you.

[*English*]

I was very fortunate to have a career at Global Affairs Canada for 15 years and to have served as security officer at mission twice. So this is something that is very dear to my heart.

I am encouraged by the recommendations within the report and the explanation we've had here today, but my former colleague Madame Jeffrey certainly knows that a lot of the time, when the rubber hits the road, it comes down to these nuts and bolts types of things.

When I reflect back upon my time at mission, there were generally three obstacles. I want to address each of them briefly, because they are a little bit more in the weeds, and of course give my colleagues from Foreign Affairs a chance to address each of those.

The first one is personnel. Certainly as MCOs, we were often in charge of three or four programs at a time—human resources, property, finance—and finally, often we were the security officers as well. While the training certainly encourages me, of course our colleague Madame Cameron, who served as head of mission in Lebanon, comes from my... I consider her a contemporary. Have we addressed the capacity situation? Have we put the numbers in place for people to effectively address these problems? That's the first thing.

The second challenge I always encountered—out of fairness to the Government of Canada, the people of Canada—was procurement. Of course, this is something that is always incredibly complex and incredibly time-consuming. Procurement processes in the Government of Canada do not happen overnight; they take a lot of time. I was there during the time of MERX, which I want to say had a \$75,000 threshold, so you could certainly achieve things like installing minor alarm systems, but anything that was larger required an extensive, month-long process, especially when we're looking at major missions.

The third, which Monsieur Shugart addressed briefly, was money, of course. Historically, this went the other way, where it was difficult to move from capital to operations, rather than the other way.

It sounds as though these things have been addressed, but I wanted to put forward these three obstacles that I continuously faced as a security officer at mission. That's the capacity of the personnel, the procurement processes and then finally the financing, although I am encouraged by this process you outlined.

Mr. Shugart, could you please comment on those three things, because when the rubber hits the road, those were the three obstacles I found in terms of implementing the necessities required to keep my people safe?

Thank you.

● (0940)

The Chair: Mr. Shugart.

Mr. Ian Shugart: Perhaps, Chair, we could address people, procurement, then money.

Mrs. Stephanie Kusie: Excuse me, Chair, just briefly, I will take 30 seconds at the end for one more question—a minute and a half, please. Thank you.

Ms. Heather Jeffrey: We agree that our management consular stream is the engine room of our missions abroad; they have a large number of business lines. In the complex security environment that we're dealing with, it has been very important to supplement that capacity with dedicated readiness and security program managers. This is being facilitated through the duty of care investment.

This year alone, we have more than 35 new dedicated security program managers deployed to missions abroad, fully trained. The training of those new security-dedicated staff is also funded through the new duty of care investments, freeing up staff in our highest-threat missions and also providing regional expertise to missions in their areas.

The readiness aspect is particularly important because, as you pointed out, it's about the protocols, exercises, training and having the right reflexes when a crisis or security deterioration occurs, so that we can respond. That personnel enhancement is a big part of the new investment plan.

The Chair: What about procurement?

Mr. Dan Danagher: We have also increased our capacity in procurement in headquarters. I don't know the time when the honourable member was an MCO out in the field, but in recent years, we've developed these common service delivery points in seven parts around the world. That has served to strengthen our

responsiveness with respect to being able to procure in the missions and to track it and get the headquarters assistance for those larger procurements out in the missions. We're still measuring the impact of that, though.

The Chair: Mr. Shugart.

Mr. Ian Shugart: It does still remain a major challenge.

On the money, I'll leave aside the question of whether we have enough. I have no complaints about the resources the government is currently giving us to deal with mission security. The way this works with the Treasury Board is that often these funds that are focused on particular programs are in special-purpose allotments, and we can only draw them down for those specific purposes.

On an earlier question raised by Mr. Kelly, sometimes what happens is that, based on the speed with which a project is being implemented, if we can document that, we can go to the Treasury Board and ask for reprofiling of funds so that they are not lost, even though they are spent in a subsequent fiscal year. Our objective is, of course, through project management and improved governance, to be spending more and more of the money allocated for a year in that year, and we're making progress in that regard.

The Chair: I think, in response—and we're going to go to Mr. Sarai next—what Mr. Kelly was referring to was paragraph 4.59 in the report, which referred to the “Timeliness of physical security projects”. Of the \$652 million in funding provided to Global Affairs Canada over the past decade to upgrade physical security at missions, about \$425 million was slated for capital projects. Although these projects were to be completed within 10 years, by 2017, about one-quarter of the funding, \$103 million, had not been spent. The department had to obtain special permission to retain \$82 million of the \$103 million in order to complete the security projects. Later they went and asked for more money when that money hadn't been spent. I think that was where the committee was questioning the allocation of funds.

We'll move to Mr. Sarai. If there's something in there you want to refer to later, you can.

Mr. Sarai, go ahead, please.

Mr. Randeep Sarai (Surrey Centre, Lib.): My concern is that you audited the upgrades to security and that in almost all of the cases, they were at least three years behind schedule. They're taking almost twice as long to complete as originally planned. Who does the original assessment of the timeline? Is it your contractor? Is it your internal assessment? Do you use Defence Construction Canada in that regard? I find it alarming, if it's a pattern, that every single time it takes twice as long and is at least three years behind.

Mr. Ian Shugart: Our goal, Chair, is that you won't read that in future reports of the Auditor General because of improvements in our planning capacity. For those, we would have—as for all of our projects—worked with our contractors in the implementation, but they would have been planned internally, often in consultation with other departments, depending on the particular project. That planning would typically be internal with expert-based capacity within the department, and that is what we are seeking to improve.

● (0945)

Mr. Randeep Sarai: Is it contracted out to contractors in that territory or is it Canadian contractors who go out and do that work?

Mr. Ian Shugart: I'll let Dan expand on that.

The Chair: You have one minute.

Mr. Dan Danagher: We use a combination of contractors, but typically we would use local contractors. Most projects go out to tender. We would evaluate bidders based on their competencies, price and those sorts of things. Typically it's local construction companies.

Mr. Randeep Sarai: Have you thought of using a government-based...somebody like Defence Construction Canada, who would know the operations, know the security parameters, and be able to do this in a maybe more timely and perhaps even more cost-effective manner? Or has that not worked in the past?

The Chair: Mr. Danagher.

Mr. Dan Danagher: What we're learning from Defence Construction is some of their practices in project management. They're not a construction company per se with an international reach. We do use a combination of really qualified local contractors, really good ones. It depends on the size of a project. You can have a project that's \$10 million, \$20 million, or \$30 million and a project that's \$2 million, and they have different scopes.

Mr. Randeep Sarai: You also spoke about a risk-based approach versus a one-size-fits-all. How would you do this? Do you use internal assessors or outside assessors? Is it Global Affairs or Foreign Affairs? Is it Defence? Is it the RCMP or private? Who will determine the risk-based approach versus...in these situations?

Mr. Ian Shugart: The main change here is to move from a planning approach that would see projects being renewed on a cyclical basis. To take the analogy of a car, that would involve replacing the car every five years, for example. The approach we're taking is more based on a recognition that the world doesn't actually work that way and that in some cases, with respect to the life cycle of facilities, a cyclical approach might be right, but for security, a risk-based approach.... So you might have to replace that car every two years if the security environment is changing. If it is not, you might not have to replace that car for 10 years.

The planning is done internally and we compare notes with other like-minded countries in the various locations, as well as with others like DND and RCMP and so on, to gather all of the relevant inputs for planning. We also have expertise within the department, under the departmental security officer, and in the branches, which understand that risk environment. We also get the information from the missions. It's a fairly elaborate process but it's now risk-based rather than just having routine turnover.

Mr. Randeep Sarai: Are you taking into account the comments and suggestions from staff who are working in those environments?

Mr. Ian Shugart: Absolutely.

Mr. Randeep Sarai: Lastly, do you believe the new funding commitments will help ensure these problems will be less frequent in the future?

Mr. Ian Shugart: I absolutely do. The resources, as we've indicated, cover not just the physical circumstances, the physical capacity, but also the training, documented and tracked with information systems, that we are giving to our staff when they go out, as well as the operational measures we've put in place. The expenditure on guards or relatively inexpensive equipment such as closed-circuit TV can be medium-term risk mitigation, as opposed to a major reconstruction project.

We're very confident that we're on the right track.

● (0950)

The Chair: Thank you, Mr. Sarai and Mr. Shugart.

We'll now move back to Mr. Kelly, please.

Mr. Pat Kelly: I want to turn to a common thread that has come up throughout the Auditor General's reports we've received at committee. It is around problems of data collection, data retention, and being able to respond or react to data. Much has been made of evidence-based policy-making, but there is no evidence-based policy-making without evidence. I bring to your attention, Mr. Shugart, some items from the report:

In paragraph 4.12 it says:

...security assessments were missing or incomplete.... Global Affairs Canada did not have the information it needed to prioritize investments....

Again, at 4.24, we have:

...had not been tracked or prioritized for action.

We see at 4.44:

...rationale behind funding decisions was not properly documented to ensure that the most urgent security needs would be met.

The report indicates throughout that there were failings to respond, or even have the information with which to make proper decisions. How was that allowed to happen?

Mr. Ian Shugart: First of all, this typically—and in this case—doesn't arise through conscious decision. I think it happens because of a practical focus sometimes on moving resources out. When the proper planning and documentation systems aren't in place, they're not used. It does take a conscious investment to put those systems in place, and that is what we are now doing.

As I said earlier, I think this is a broad problem. But during the period of those funding programs, one of the missions that had enormous security requirements was Kabul in Afghanistan. The needs there were obvious; they were patent. In the absence of a documentary system that will hold you to a plan, sometimes the urgent needs act as a big magnet. The resources are put where the practical, day-to-day assessment is needed.

We're not being blind to the circumstances as they evolve. We have in place the systems that will track what we're doing, whether we are on schedule, how the needs have changed, and we're evergreening those risk assessments so that we will not have this kind of finding in the future.

You're absolutely right, but we've put in place the systems that will prevent that from reoccurring.

Mr. Pat Kelly: Yes, and we can't have that. We can't have the scenario that we've seen in others, where we'll come back five or 10 years from now with another audit with the same failures. Having had this audit tabled in the public domain places a particular urgency on getting this together and getting these known security lapses addressed as soon as possible.

I know that my colleague, Ms. Kusie, had one quick question she didn't have time to ask, so I'll let her do that right now. I have about a minute left.

The Chair: You have about one minute.

Mrs. Stephanie Kusie: I just want to state briefly, as a former foreign service officer abroad, that I feel that the government truly has the deepest obligation to keep its employees safe abroad. I know there has been a lot of discussion this morning about the situation in Havana, but what is apparent to me through the media is that the Canadians serving there did not feel safe and did not feel that the present government protected them as soon as it should have, especially compared with the Government of the United States—which also political comments while ours made none.

What have we learned from this? I want to give you the opportunity as representatives for Global Affairs Canada here today to say what have we learned from reacting to this so slowly, so that we never put our people in harm's way like this again? Furthermore, should something like this occur, how do we recognize and respond to it sooner to stem the problem as quickly as possible?

• (0955)

The Chair: Very quickly.

Mr. Ian Shugart: I'm not, at this point in my comments, going to accept all of the assertions made. I would say that I think it is too soon for us to have learned all the lessons, because we still don't know a great deal of what we're dealing with.

The test is always based on what you are finding. First, are you taking it absolutely seriously? Secondly, are you applying a reasonable standard of care given all of the circumstances, including the need to continue to serve Canadians in the field? Are the actions you take meeting the reasonableness test in the legal understanding of the duty of care? That is what we are striving to do.

The Chair: Thank you, Mr. Shugart and Mrs. Kusie.

We'll now move to Ms. Yip, please.

Ms. Jean Yip (Scarborough—Agincourt, Lib.): Thank you for coming.

I'm concerned about the security training for staff. Two in five employees at high-threat Canadian missions had not taken either the personal security seminar or the hazardous environment training, or both. GAC had not routinely provided enhanced security awareness training at high-threat missions.

Why are Canadian staff members posted to missions operating in high-threat environments not given the training and the seminar before their departure?

Mr. Ian Shugart: I don't want to quibble, but I would say that the tense is important. It is an absolutely valid question, why were staff not given the appropriate training, but it wouldn't be accurate anymore to say why are staff not being given this adequate training, because this is something that we have worked very hard to correct. I'd invite Heather to elaborate a little bit on our training program.

Ms. Heather Jeffrey: We have a number of specialized course offerings for high-threat missions—the hostile environment training and the personal security seminars—which are multi-day, very specialized, very well-regarded courses.

The issue we had faced in the past was that, while people were being trained going out to mission from headquarters, it was very difficult for operational reasons for us to train people moving between missions abroad, which is frequently the case with our rotational staff. Under our new duty of care investment program, training offerings have been prioritized. We've increased the quantity of those offerings by 40% this year. We've also piloted new ways of offering these courses. For example, they can now be offered abroad in the local environments there. Rather than bringing people back here, we're able to offer the courses on site in the local environment, which also enhances the training. We're well on track to implementing that recommendation.

Another aspect of the recommendation was, of course, the ability to track this. Our new security and information management system and a dedicated training tracker are already in place and functioning to make sure that we have adequate oversight of the completion of that training.

Ms. Jean Yip: What is the difference between standard and enhanced security awareness training?

Ms. Heather Jeffrey: What I would say is that all departmental staff receive on a regular basis a basic level of security training—the types of document classifications, entry protocols, access. However, in travelling to a high-threat environment, as would be the case, for example, in Afghanistan or Iraq, we found that our officers required a much higher level of training on some of the threats our diplomats face when they are in areas of high conflict. There is a five-day training program offered by the Department of National Defence on how civilians operate in militarized environments. That is our hostile environment training course. That's an example of the type of enhanced training we're offering for people who are exposed to those types of threats.

Ms. Jean Yip: So there isn't a progression of training in response to the increasing threat in the environment? By that I mean training done more on an emergency basis, as opposed to just five days of training here and then trying to deal with whatever emergency or threat in the immediate environment?

● (1000)

Ms. Heather Jeffrey: On an annual basis, we review the security postures and evolving threats in our missions abroad and we adjust the course offerings. There are quite a number of courses of graduated importance. Some focus more on information security and environments where espionage could be a problem. Some are much more focused, as I mentioned, on combat risk. Others are focused on personal security. High-crime environments are actually much more prevalent than the militarized ones I was speaking of. There is a very wide range of missions.

I would say that almost three-quarters of our missions abroad require some form of enhanced training above the normal security baseline. That's looked at on a regular basis to make sure it's adequate to the needs on the ground. In addition, when staff are deployed on missions, they receive a very detailed local security briefing on the threats specific to their mission environment and also in the outlying regions. Our staff don't just work at embassies; they also travel throughout countries working on humanitarian or other projects, for example. It's very important that they understand the risks not just at the mission but also out in the wider country.

The Chair: Thank you very much, Ms. Yip.

I'm being told that the House will open, the bells will start, and a vote will disrupt us today. Since we're in the same building where the vote will take place, with everyone's permission we'll go a little bit in. I'll still give at least 10 minutes for us to get up there and take our places.

Mr. Chandra Arya: Last time, I remember, *[Inaudible—Editor]* minutes and you were late.

Voices: Oh, oh!

The Chair: I was late. Okay. Well, we'll try to speed it up again. I'm probably slower than any of you in getting up there.

We'll now move to Mr. Christopherson, please.

Mr. David Christopherson: Great. Thanks, Chair.

This is just an observation. One of the challenges of dealing with security issues in a democracy is that accountability and transparency don't necessarily go hand in hand with security and preparation. I just want to say that I think we've done a pretty good job, all of us

concerned: you, representing the department; the Auditor General's office; the committee itself; and the governance by the chair. I think we've done about as good a job as we can on transparency without doing damage to the very entities we're trying to help. I would just make that observation.

The second thing I want to say, and this is really important, is that I really, really liked what you said, Mr. Shugart, at the beginning of your answer to a previous question. As you know, I am likely the least academic member who has ever sat, and who likely ever will sit, on the public accounts committee, but one thing I've learned from my years on this committee is that there's the planning ahead of time, the processes, the checks and balances, the evaluations, and then, when you're done, there's the starting all over again, the re-evaluating, and the going back and examining. You know the old tradesperson's proverb, “measure twice, cut once”. That is so important.

Given your broad experience in recognizing that this is not an area where the government has been as effective.... The Auditor General's office has been pounding it and pounding it and pounding it, certainly to the point where I get it, and as I said, my knowledge based on that is the least. So I'm so glad to hear you say that, because my experience tells me that that's where it is—that and the other part of what we do, which is the follow-up to make sure you honour the commitments you make. Those two things really make a huge difference. I just wanted to emphasize that.

I have one more question. As Ms. Yip already brought forward, 41% of the staff had not completed the mandatory personal security seminar, and 35% of staff had not completed the mandatory hazardous environment training course. Now, when we're dealing with security and with mandatory, that seems pretty important to most people. When did Global Affairs decide that they can create their own definition of mandatory? Where else in your organization is mandatory not being treated as mandatory? Do we need a new word?

My understanding is that “mandatory” means “must do”. You didn't do it. Even in your response you said that you're going to start doing it, playing with your tenses. You say here: “Mandatory training for staff being posted abroad, especially to designated high and critical threat missions, is a key element of Global Affairs pre-posting practices.” But you didn't seem to believe that before you were held to account by the Auditor General's report.

So what's the deal with “mandatory”? When did mandatory in Global Affairs, as it relates to security, become not mandatory?

● (1005)

The Chair: Thank you, Mr. Christopherson.

Mr. Shugart.

Mr. Ian Shugart: Very simply, it always was mandatory, and not living up to that was a failing. As Heather indicated, we have increased the offerings of that one particular enhanced training program by 40% this year alone. More importantly, we have put in place the tracking system so we will be able to follow. Any slippage in our performance on that mandatory standard will be very obvious to managers. It will be corrected much more rapidly, and we will be able to stick to that commitment. We did not have that kind of tracking in place before.

To find out the degree of gap, of slippage, the audit staff had to examine the records. We now have in place a tracking system that will tell us our performance in real time.

Mr. David Christopherson: I appreciate that. That's good news.

As it deals with security and is mandatory in your organization, can you assure us that nowhere else is mandatory being treated so haphazardly and as so unimportant?

Mr. Ian Shugart: We will have that conversation to add suspenders to the belt, Chair, but I believe that as a result of the approach we have taken to our management of security in the last couple of years, we can give you that assurance. In one of our regular and frequent meetings, we will have that discussion. If I'm wrong, we will readily correct it.

Mr. David Christopherson: Thank you.

The Chair: Thank you, Mr. Christopherson.

[Translation]

Mr. Arseneault, you have five minutes.

Mr. René Arseneault (Madawaska—Restigouche, Lib.): Thank you, Mr. Chair.

Mr. Shugart, I'll continue along the same lines as my colleagues Ms. Yip and Mr. Christopherson.

Perhaps as a result of my professional background, since I was a trial lawyer for 23 years before being elected, I have one burning question.

Are we clearly informing the employees—our fellow Canadians—sent to our diplomatic missions abroad, in addition to locally engaged staff or subcontractors, that they'll be working at missions where certain security standards aren't up to date and where security upgrades are behind schedule?

Mr. Ian Shugart: I would ask Ms. Jeffrey to elaborate. I gather that you're talking about transparency. Is—

Mr. René Arseneault: I apologize for interrupting, but I don't have much time.

If I'm hired to work at one of our missions abroad, am I told whether the facility where I'm being sent to work meets the minimum security standards? Am I told whether certain security work is behind schedule?

Even though the employees take the brief course for five days or I'm not sure how long to prepare for emergencies, are they informed of these weaknesses? That's what I want to know, and a simple “yes” or “no” will do.

[English]

The Chair: Ms. Jeffrey.

Ms. Heather Jeffrey: On arrival at mission, all of our staff are fully briefed on the situation and the measures in place. That includes not just the physical security measures that they're aware of—gates and access—but also the operational security, which can supplement and in some cases compensate for physical security that needs to be enhanced. That includes movement protocols, go/no-go areas in their mission locale, the type of escorts, the local guard service required for moving outside the mission environment, radio protocols, communications check-ins, all of these types of things.

[Translation]

Mr. René Arseneault: Are you telling me that the weaknesses identified by the Office of the Auditor General are explained to them, perhaps not in detail, but that at least they're informed from the start that they'll be working at a mission abroad where not all the security measures have been fully developed? Are they informed?

• (1010)

[English]

Ms. Heather Jeffrey: Yes, they're advised of the operational and physical security measures in place around their mission and the need to respect them to ensure the safety of not just—

[Translation]

Mr. René Arseneault: That's not what I asked you.

Are they informed of the weaknesses in the security measures and infrastructure?

Mr. Ian Shugart: I would say that our colleagues are generally well informed of the situation. For example, when we're strengthening certain measures, we inform them that certain projects are under way, but that the work isn't finished. This type of information is available to them. However, you're asking a very specific question and we'll look into it because—

Mr. René Arseneault: I must interrupt you, Mr. Shugart, because I don't have much time left. I want to thank you, and I invite you to send your response to the committee through the clerk.

I have a second question. How much time do I have left, Mr. Chair?

[English]

The Chair: You have two minutes.

[Translation]

Mr. René Arseneault: Mr. Shugart, thank you for agreeing to answer the question, which was becoming obvious.

There's a lack of planning when we open a new mission abroad. That's it. In short, that's what I understood. We don't open a new mission abroad every week. However, I read in the Auditor General's report that the lack of planning for these new missions isn't something new, no matter the government of the day. This has been going on for at least 10 years, or since 2011.

Can you provide an example of a new mission planned in accordance with the best practices? Are you about to open a new mission somewhere? If so, has the establishment of the mission been properly planned?

[English]

The Chair: Mr. Danagher.

[Translation]

Mr. Dan Danagher: We've recently opened new missions. In Brussels, for example, the process took only a year and a half and was a great success. In New York, our new mission opened on time and on budget. We've been very successful recently in this area.

Mr. René Arseneault: Okay.

In terms of security, Belgium and the United States aren't considered very dangerous countries. Do any countries pose more risks and require more effort to ensure mission security?

Mr. Dan Danagher: It's difficult to answer this question because we're completing the planned missions and projects. However, we've been very successful in some of the more dangerous countries, including Afghanistan. We have many similar recent examples.

Mr. René Arseneault: Thank you.

[English]

The Chair: Without trying to interpret all of what the Auditor General said, I think that some of those places listed on the front page here—Burkina Faso, Afghanistan, Egypt—are all recognized as needing security. However, sometimes, as the Americans found out in Benghazi and in other countries, an attack can happen anywhere.

I have one more questioner, Mr. Zimmer.

I'll just tell the committee that we have a very short issue with our public accounts budget for travel through the summer, our conference with the provinces, that we want to deal with so that we can get the budget and go to the Liaison Committee.

Mr. Zimmer.

Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC): As the chair of our ethics committee, one thing we've studied exhaustively is how groups can organize quickly around the world now on platforms like Facebook, etc.

I respect you, sir, as a servant of the public, but I'll read paragraph 4.18. This is what all of this comes down to:

This finding matters because physical security vulnerabilities must be resolved in a timely manner for the effective protection of staff and assets at missions abroad.

You sit here and survive this committee meeting and you go away to your normal life. You don't come back here maybe for another four years—I don't know—but we have a fence that hasn't been fixed for eight years. Who do you answer to?

I've been in bosses' offices before, answering for something that I haven't done properly. It's been rare, but it has happened.

What's your commitment to seeing this fixed? Are you going to be here maybe next year, and maybe the next year again, and it's not fixed for the next 20 years?

At what point do you actually get it done and answer what this audit report is challenging you to do? What's your response to, "Okay, I've just been taken to the cleaners here; I'm going to make sure this problem is resolved"?

When is that going to happen?

• (1015)

The Chair: Mr. Shugart.

Mr. Ian Shugart: I think the member's question is a more general one. If it's about the specific fence, I'll ask Dan to handle that.

I guess I would say that I don't regard coming to this committee and the time we spend—and I think the chair will back me up on this—as just surviving and then going back to my ordinary life. In fact, my ordinary life is about the implementation of the funding that we've received for these purposes, guided by the Auditor General's report and by our own internal audit. The Treasury Board holds us accountable for those funds.

Mr. Bob Zimmer: I know you're short of time, but you're starting to talk about generalities. I'm asking for something specific, namely, what you are going to do as a department to go back and look at all the Auditor General's recommendations and get them done within a reasonable time.

The Chair: Mr. Zimmer, let me jump in here.

They have already given us an action plan, which we will follow up, but I think the question is still good.

You have given an action plan. In your opinion this action plan is on time and you're going to be able to fulfill what you have committed to in this, correct?

Mr. Ian Shugart: Absolutely. We are on track with every one of our commitments. Frequently the OAG does follow-up audits, and we do follow-up audits of our internal audits.

The Chair: Thank you.

It's a good question, Mr. Zimmer.

Mr. Ian Shugart: It is.

The Chair: That can be a question that a lot of members are concerned about, because we see departments commit to something time and time again and then don't do it.

Let me say that in this public accounts committee we've now taken on a follow-up approach so that deputy ministers—and Mr. Shugart is not one of them—will not come in and have a "one and done", that is, doing one meeting and thinking they're done for another year.

We will follow up on these with our analysts. I have already been told by our analyst at this meeting that he is confident that the timelines in the action plan can be met and are reasonable. But if they are not done, then we will invite departments back. I know Mr. Shugart knows that the second time on one issue is not a good meeting typically.

Thank you for that question. It gives us the opportunity to explain it a little bit.

I want to thank our guests for their testimony today, the Auditor General for his good work on this, and the department for being here and being accountable.

We're going to suspend this meeting. I'm going to ask those who don't have to stay to leave fairly quickly so we can have this in camera committee meeting where we have two items we want to quickly discuss.

[Proceedings continue in camera]

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <http://www.ourcommons.ca>

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : <http://www.noscommunes.ca>