

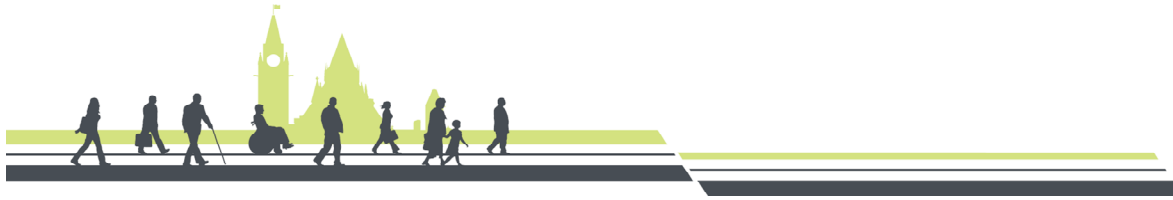


Public Services and
Procurement Canada

Services publics et
Approvisionnement Canada

Canada

Serving
GOVERNMENT,
serving
CANADIANS.



Public Opinion Research on the Contract Security Program (Part 2 – Interviews)

Final Report

Prepared for Public Services and Procurement Canada

Supplier: EKOS RESEARCH ASSOCIATES INC.

Contract Number: EP243-200270/001/CY

Contract Value: \$17,622.92

Award Date: May 9, 2019

Delivery Date: June 19, 2019

Registration Number: 008-19

For more information on this report, please contact Stephen Ayres at (613) 946-3077

Ce rapport est aussi disponible en français



www.pspc-spac.gc.ca

Public Opinion Research on the Contract Security Program – Part 2 Interviews

Final Report

Prepared for Public Services and Procurement Canada

Supplier name: **EKOS RESEARCH ASSOCIATES INC.**

Date: June 24, 2019

This public opinion research report presents the results of a series of one-on-one telephone interviews conducted by EKOS Research Associates Inc. on behalf of Public Services and Procurement Canada. The research study was conducted with 20 Canadian businesses between May 14 and June 11, 2019.

Cette publication est aussi disponible en français sous le titre Recherche sur l'opinion publique au sujet du Programme de sécurité des contrats (Partie 2 – Entrevues)

This publication may be reproduced for non-commercial purposes only. Prior written permission must be obtained from Public Services and Procurement Canada. For more information on this report, please contact Public Services and Procurement Canada at: tpsgc.questions-questions.pwgsc@tpsgc-pwgsc.gc.ca or at:

Communications Branch
Public Services and Procurement Canada
Portage III Tower A
16A1-11 Laurier Street
Gatineau QC K1A 0S5

Catalogue Number:

P4-89/2019E-PDF

International Standard Book Number (ISBN):

978-0-660-32697-9

Related publications (registration number: POR 045-17)

EKOS RESEARCH ASSOCIATES

Contact: Susan Galley

Ottawa Office

359 Kent Street, Suite 300

Ottawa, Ontario

K2P 0R6

Tel: (613) 235 7215

Fax: (613) 235 8498

E-mail: pobox@ekos.com

www.ekos.com

TABLE OF CONTENTS

1.	Introduction and Objectives	1
2.	Interview Findings	5
2.1	Role in Organization and in Managing Securing Screening	5
2.2	Description of the Approach to Security Screening	5
2.3	Issue Areas	9
2.4	Costs and Driving Factors	15
2.5	Changes with an Impact on Efficiency/Cost	20

APPENDIX A: Email Invitation and Registration

APPENDIX B: Interview Guide

1. INTRODUCTION AND OBJECTIVES

Public Services and Procurement Canada (PSPC) is examining the contract security screening process to help improve its practices. PSPC has identified the need to conduct research among a target audience of companies currently registered with the Contract Security Program (CSP). In particular, PSPC has identified Key Performance Indicators (KPIs) to assess CSP program outcomes. The KPIs are as follows:

- Average company cost to manage security screening applications has decreased;
- Company representatives believe that the process is simpler and quicker and improved.

A 2018 survey established a baseline on current performance and satisfaction among a target audience of companies currently registered with the Contract Security Program (CSP). The current study involves qualitative follow-up research to better understand how the CSP's target audience understands and calculates the average time, effort, and direct cost incurred in order to obtain and manage individual security screening applications.

Methodology

EKOS conducted qualitative interviews with individuals responsible for management of the security screening function within their organization. Recruitment was based on responses from a question placed on the 2018 survey, in which respondents expressed willingness to be re-contacted for a follow-up interview. A total of 121 Company Security Officers (CSOs) were sampled because they reported in the survey that they submit security screening applications at least once every three months, ensuring enough experience and continuity with the process to make them good candidates for the interview. These survey respondents were sent an email explaining the objectives of the current study and inviting them to register their interest in participating in a 60 minute telephone interview. A total of 24 declared an interest and were subsequently contacted to set up a date and time to complete the interview.

The interviews were conducted using a semi-structured guide, consisting of issues identified by PSPC and questions developed collaboratively between the client and EKOS. The interview guide was developed in English and translated to French and interviews were conducted in the interviewee's official language of choice. An honorarium of \$150 was offered to participants. Of the 24 interested, a total of 20 interviews were completed between May 17th and June 11th, with two conducted in French and the remainder conducted in English.

The following table provides some information about the sector, region and size of organizations represented in the interviews. The table also provides some indication of the frequency with which security screening is managed in the organization and volume of applications processed annually.

Table 1: Profile of Interviews

Table 1a: Sector

--	Number of Interviews
Construction	7
Information Technology	3
Professional and Temporary Help/Staffing	5
Security/Defence Production	2
Industrial Goods and Services	3

Table 1b: Region

--	Number of Interviews
Atlantic	2
Quebec	2
Ontario	14
Prairies	2
British Columbia	0

Table 1c: Size of Organization

--	Number of Interviews
Fewer than 10 employees	1
10 to 99 employees	8
100 or more employees	11

Table 1d: Frequency of Activity

--	Number of Interviews
Once a month or less	7
Several times/month	3
Several times/week	7
Daily	3

Table 1e: Annual Volume of Applications

--	Number of Interviews
10 or fewer	7
11 to 50	4
51-100	3
101-500	3
More than 500	3

2. INTERVIEW FINDINGS

2.1 ROLE IN ORGANIZATION AND IN MANAGING SECURITY SCREENING

In all cases, the security screening function is managed in-house, by the organization, rather than contracted to another firm. The role and level of seniority of CSOs working on security screening ranges considerably but generally the level is between a mid-level project manager/administrative manager to a senior officer. In a few cases the responsibility is held by a Vice-President or Chief Executive Officer. Most participants serve as the CSO, with the exception of two very active Alternate Company Security Officers (ACSO)s, who are largely responsible for all tasks, with some minimal oversight from a CSO. In the case of the larger organizations, where the annual volume of applications is sizable, some have one to three ACSOs. In all cases, the CSO interviewed is responsible for training ACSOs.

With the exception of one participant, everyone described the security screening function as one of several responsibilities they hold, although for about half it is their primary function. The amount of time dedicated to security screening ranges from about 15% to as high as 70% of their time.

2.2 DESCRIPTION OF THE APPROACH TO SECURITY SCREENING

a) Beginning and End of the Process, Average Length of Processing Time

The start of the process is considered to be the request for a security screening. Sometimes this is requested by the employee, but most often it comes from the hiring/human resources manager or an employee's supervisor. For professional service/temporary help agencies, it is typically when the individual contacts them requesting that the security screening process be initiated.

"Beginning is when a manager requests that an employee obtains a clearance. It's better for me when an employee requests for themselves because it means they are more keen to do it. After the request, the first step is to go get fingerprints if

they don't already hold a clearance. If they already hold a clearance, we can transfer or duplicate.”

For many, the “end” of the application is signalled when the approval is received from the CSP. Some, however, described the added process of briefing the employee/contractor and obtaining the signed copy of the clearance, and in a few cases, logging this into their system/CSP reporting. At the same time, many participants spoke of the ongoing function of monitoring for renewals, which involves regular upkeep on a weekly or monthly basis to be sure that all renewal applications are submitted well enough in advance to ensure that their security status does not lapse.

The length of the processing time varies considerably from participant to participant, even for the same type of clearance. For Reliability, for example, some spoke of a one to three day turnaround, while others said it typically takes three to four months. Overall, about a third said it takes two weeks or less. A few said it takes a month or slightly longer and a handful said it typically takes three months or a little longer. Most said that renewals typically have a much quicker turnaround. Most also note that less complex cases, where the applicant has been born in Canada and/or has done little travel or work outside the country are the most likely to be processed quickly, unless there were errors or omissions in the application that were not caught prior to submission. Virtually everyone also noted that the processing time has become much shorter in the last two years, with the Document Control Number (DCN) system and fingerprinting, and that wait times were much longer prior to the last year or two.

For a Secret clearance, a few spoke of quick turnaround; within a few weeks, but responses are more consistently measured in months. Most spoke of two to three month waits, particularly if the applicant was born in Canada, with limited travel or work outside the country and no significant gaps in timeline. Many said, however, that approval can take six to 10 months for more complex cases and, in a few instances, over two years. Again, most agreed that the turnaround is shorter than it used to be. Some also said that it can be difficult for their organization in terms of hiring, planning and work flow, not to be able to predict how long an approval might take. One organization indicated that hiring is contingent on obtaining clearance. For some, the one-month mark is the interval at which they start to follow-up to find out with CSP if there are issues or questions with the application that need to be addressed.

b) Approach

There is variation in how organizations approach security clearances, but by and large, there are a few central differences. About half of the organizations interviewed rely on paper copy applications which they give to employees/contractors and have them complete the application on paper. Once these are received back, the CSO/OLISS

reviews them for issues and gaps, and works with the applicant to make sure they are complete. The CSO/ACSO then enters the application into the Online Industrial Security Services (OLISS) and reviews it once more before submitting it.

“The good thing about the way we do it is we do all that ahead of time. So the forms are usually quite complete and have all the information we need once we submit it in OLISS. So when it’s submitted we don’t get as many requests for additional information or anything like that.”

In the other cases, the organization requests an application from the CSP, asks the applicant to obtain finger prints, enters the number into the case file and then asks the applicant to complete their own application online, directly into OLISS. Some CSO/ACSOs stated that they provide the applicant with instructions to fill in the application form, with guidance on areas that often cause problems with the application (such as a lack of thoroughness or gaps in dates). In all cases, the CSO/ACSO still reviews the file for comprehensiveness in this scenario and submits it. In all cases the CSO/ACSO also resolves any issues and questions based on feedback from the CSP to finalize the application. Whether the employee completes the application on paper or directly into OLISS, the CSO/ACSO always receives the approval notification and briefs the employee about their responsibilities.

Many organizations take the approach of making applications and requesting security clearances as soon as the employee/contractor is hired. For some, this is even built into the hiring and training process, to the extent that candidates unlikely to obtain a clearance can be flagged prior to the hiring decision. In these cases, completing applications is a standard part of the entry/training process. In many cases candidates/new employees with no previous clearance are automatically asked to apply for Reliability. In a few cases there is an expectation that once the first clearance is obtained they will likely be asked to subsequently apply for Secret within a matter of weeks or months. For those with an existing clearance, the transfer process is also initiated right away.

“For us, whenever we get new employees, depending what their job is, we’ll get them started with the process right away. We do a lot of work for Public Service so we want to have people on hand that are ready to go, so we’re not waiting until we have a job and then getting clearance.”

Among organizations obtaining clearances for their own employees, often the employee is paid to complete the application and also to obtain finger prints (i.e., on company time), and the company assumes the cost of finger prints. In a few organizations, employees are asked to complete the application and obtain finger prints on their own time. With organizations that are

working with sub-contractors or independent (temporary or professional service) workers, they are typically not paid for their time, although sometimes the cost for finger printing is covered.

2.3 ISSUE AREAS

A number of issues were identified by participants, largely falling under half a dozen broad themes.

Lack of Transparency/Information

Lack of transparency and information about unresolved problems with applications is the number one source of frustration expressed by participants. More than half of participants spoke of the difficulties of not knowing or being able to predict if or when there will be issues with an application. Even greater frustrations were expressed with the lack of notification when there is an issue. Many said that it is only when they follow-up that they are told there is an issue to be addressed. Many referred to the process and steps as the “abyss” or the “black box” saying they have no understanding of what the steps are, or where or when applications can get hung up. Some expressed frustration with not having an informative code regarding the status of the application, other than “in process”, and not being given an estimate about the likely turnaround time for the application.

“The most common with individual clearances would be, if it’s a ‘complex file’ that’s all they can tell us. We have no way of knowing if it’s going to take a month, 6 months or if it’s going to come through at all.”

“If we were able to somehow have access to say if they’re cleared or not cleared or if they’ve been denied. That would make it a much smoother and easier process for us.”

“The only status you get is pending and it could be pending the day they receive it, it could be pending 6 months later but you don’t know where it is in the process.”

“From when it leaves my desk to when I get it back I don’t know usually what’s going on in the middle because they don’t tell me.”

“The process is a little complicated in the sense that there’s no specific location where instructions are clearly indicated. The website doesn’t tell you anything or list the steps to take.”

“There are actual cases we need to solve, so we need to know how it works. There’s no one who can help, and each time you call Ottawa you get a different answer. They put junior staff on the helpline.”

“There should be a process of providing an update once a clearance goes over a certain number of weeks. It would be nice to get updates as opposed to calling in to get an update. We can go online and it will say pending or cleared, but there is no other information. We sometimes call in and they will confirm it’s pending, but say there is no other information. That’s when I wonder if it got sat on, because they will say it’s pending and then it will be cleared in three days. They should assign levels of review so that we can understand more about the phase.”

“I can track the status of a pizza delivery, why can’t I know the state of an application?”

Access to Information and Assistance

In a related theme, many participants expressed frustration with their inability to obtain information about the status of an application, or to obtain answers and assistance in addressing a problem. This was expressed in terms of:

- **Lack of access to the person reviewing the application and flagging an issue.** Several said that it is difficult to be reliant on the call centre; having to ask about a type of situation in a very generic way, rather than speaking directly with the specific individual who reviewed the file and indicated the problem.

“We get a fax in from them with a question and it never says who it was from. Would be great if there was a name on the form and we could call back with a quick answer or ask to clarify their question. You never know if we fax it back if it just sits there in a queue again.”

“The biggest challenge is the inability to reach out to the specific person working on the file. A question is asked from CSP, but must respond to call centre and get a generic person who may not even understand the question that was asked by CSP.”

- **Limited knowledge of call centre staff.** Related to this, a handful described the knowledge level of call centre staff as limited or poor. This results in call centre staff having to note the issue, go find the answer and subsequently return to the organization in a more protracted and disjointed process.

“I find the skill levels (in the call center) vary; maybe half the people you talk to are very knowledgeable and half are not.”

- **Lack of proactive assistance.** Several said that it can be frustrating to be told that the application is with another department (e.g., in the case of a transfer) and they have no further information. The complaint from participants is that call centre staff would have access to and should be able to dedicate the time to go find out and provide an answer, given that

organizations themselves do not have access to do this. Similarly, several said that the OLISS system should automatically notify you when there is a problem with an application, with a flag on the system and email sent to communicate this, rather than CSOs having to call in to find out if there is an issue.

“I can’t call the contracts department or I can’t call the SRCL department, we have to go through the call center and sometimes we don’t get calls back at all.”

- **Access to call centre/response time.** Although a few were positive about access to the call centre and response time, many expressed concerns about the inability to access staff, including wait times of 20 to 45 minutes on the telephone to speak with someone. Reporting of response by email varies from 1 day to “rarely” receiving an answer at all, which was not described as an uncommon occurrence.

“Sending a question by email is probably the worst. No matter what it is, whatever the question is, they don’t get back to you very quickly. And they encourage email questions but the results are very poor.”

“The call center takes 40 minutes on average, they really don’t know the answer, and I would describe the “transparency” of the process as zero.”

“It would be nice to have a live chat option on the website, rather than calling into the website and wait on hold. Would prefer, even if after a wait, for a chat box to pop up when they are ready. Would be nice to have communication by e-mail rather than fax machine. Seems sort of archaic and don’t use the fax machine for anything else. There are positive things such as that they travel to regions to do annual training.”

“I never need assistance, but I’ve been doing this forever. I try my darnedest to not have to call in because you can be on hold for 20 minutes. I will call in to learn about a status if a clearance is pending for too long.”

Lack of Clarity/Organization Issues

A number of issues described by participants relate to a lack of clarity or clear instructions, or a lack of organization at CSP.

- **Need for updated forms and clearer instructions.** Many participants said that application forms are not clear enough in some areas about the nature of the information required, arguing that clearer instructions are required. Several organizations said that they have created their own additional instruction and review sheets to compensate for this lack of clarity, which can be frustrating for applicants. Additionally, at least a few said that there are information fields in OLISS that are not reflected on the paper copy application forms. Similarly, a few also said that paper copy forms do not include some of the newer, background

check requirements of organizations (see more detail in later section). One participant said that forms and instructions are not always available, necessitating calls to the call centre.

“When you go through the electronic [version] there just seems to be more information required than on the form itself.”

“One of the other challenges we have is that the form you print off doesn’t actually quite match the questions that are asked on the electronic version. I think in the past it’s been that citizenship hasn’t been the same as well as employment and I believe travel as well.”

- **Lack of organization.** Many participants alluded to a lack of organization of CSP staff, including the use of faxes to communicate an issue, given that fax machines can be located in common spaces, and faxes can be easily lost or misplaced. Participants also pointed to the lack of security/privacy of personal information being sent through a fax in shared space. Several spoke of the need to be very organized because CSP staff frequently lose files.

“You need to be extremely well organized in all your paperwork and emails and exchanges with the CSP. You need to be very well organized because they are not; they lose files, they misplace files. So at least twice a year I’ve had this issue.”

“The next thing you know they say they’re closing the file cause they didn’t receive some of the information they were asking for. That usually happens because I’ve sent it and then a month or so later they’re telling me that I didn’t send it. Usually when that happens I send them an email of the trail I already sent.”

“First thing is scrap the fax process. It’s cumbersome, it’s antiquated and it can be unreliable.”

“The challenge with it coming in by fax is we are a smaller office so I’m not sitting by the fax machine. So I’m dependent on someone to see the fax, recognize what it is and then get it to me. But then it’s also people’s personal information involved that is then out for the office.”

“The most frustrating part is getting the “DCN required” letter. It seems to me that there is some kind of communication problem with the fingerprinting company and entering in the information properly. It’s difficult for us to figure out what that back end process looks like.”

“The way CSP communicates is massively inefficient (faxes, general response, etc).”

- A few described the need to submit applications by email but also enter them into OLISS adding more work, but also room for error.

Length of Time and Delays in Obtaining Approval

Although many noted the significant improvement in the turnaround time in the last two years, some still find the processing time unacceptable, particularly given the lack of predictability and information about the expected length of time required to obtain approval. A few said that some applications can drag on so long that updated information or signatures are required (i.e., if an application is more than a year old). Causes of delays were described as not being proactively informed of a problem that needs to be resolved, and lack of clarity/response about how to resolve an issue.

“Every now and then I’ll get a thing from Public Works; they want me to have somebody re-sign something because the date they signed it is a year old. So public works has had it for a year and now they want me to chase down this guy and re-sign because the date is old.”

One source of delay noted by several participants is when applicants try to submit a copy rather than an original. If this could be flagged by OLISS right at submission it would also save time, according to a few participants.

One participant said that, in some cases, issues with an application can be identified one at a time; each following a new set of revisions, adding to delays. This participant suggested that having an exhaustive list of all issue areas for one application would be more helpful. This was not mentioned by other participants however.

“One of the frustrations that I have about issues that come back is that we get a comment about one issue and you fix that issue and then they come back with another. Just list all the issues at once so we can address it whereas they tend to review it until they find a mistake, reject it and send it back.”

When participants spoke of unexpected delays, they often talked about the impact. For some, this was about opportunity cost and loss of work, but more spoke of losing good candidates who walk away and take other jobs after a few weeks of waiting for clearance. A few also said that it is unfortunate not to be able to take advantage of previous clearance information (e.g., in the case of a pending application for a renewal, or an application transfer from another organization/departments, or for a retired public servant who must obtain a new clearance in order to work in a new capacity).

“During the time it takes to complete the process, people end up finding jobs elsewhere. They’re also concerned about the type of information they have to provide, question what it will be used for, and find the process so long that they

give up. If you don't make an offer to a potential employee within two or three weeks, you've lost them."

Online Industrial Security Services System

Almost half described issues with OLISS, including one saying that it is very slow to accept entered responses, prolonging the time it takes to complete an application. Entry of dates and flagging of gaps is another example raised by a few, whereby a new start date in the next month after an end date is considered a gap, but OLISS does not specify that this gap is the source of the error. Others also said that the system is not generally user-friendly and forgiving of errors. An example given was when there is simply no information that can be provided for a field (e.g., current contact information unknown), but will not allow a blank or an explanation to be provided. One participant described a scenario where a dash was illustrated in the instructions but yet not accepted as an entry in OLISS. That said, a few participants commented that OLISS does flag gaps and missing information and documents, which they find to be very helpful.

"OLISS is also not very forgiving of errors and gaps. There could be reasons why you can't provide some information but you can't tell this to OLISS. It won't accept it and will just come back incomplete. So then you have to call and speak with the call centre and tell them that you are going to send the paper copy through with explanations for missing pieces. It takes time. OLISS needs to deal with exceptions a bit better than it does."

"What happens now is with OLISS you do the completeness check and it flags anything that's missing so once you've got everything completed there should be no problems. Whereas before we would fill out the form manually and send it in, it was easy to have something missed."

Others spoke of requests of the CSP to issue a new application, where no email with login is sent. Sometimes CSOs find this out a week or two later when they follow up with the applicant, because when emails are sent they are not sent to the CSO, only to the applicant, which results in lost time. Similarly, one participant described that they occasionally receive an email to submit an application that they have already submitted, but resubmitting causes a duplicate entry and confusion.

Several participants said that the system can be unavailable (e.g., for maintenance) quite frequently which also results in delays.

Several participants stated they would like to have all activity, including application submission, status, and issues raised by the CSP contained strictly within OLISS so that everything

is kept in one place, with a complete automated record of all activity and communications. This could also be used to flag estimated times for processing. It would also reduce significantly the volume of calls to the call centre.

Other issue areas raised included the webinars, which were described as not particularly informative or useful for their organization's needs, but could be an opportunity to obtain information and clarity about common situations, according to some.

“They need to provide better training that includes information on specific points. Every time I’ve attended a webinar, it never answers any of my questions. The process has become so complex.”

“There should be more training on their end to understand the process of allowing branches to view. Also at the annual training, Public Works should tell us the “why” of what they are asking for. We could use this to help train our applicants.”

2.4 COSTS AND DRIVING FACTORS

A key objective of the interviews was to determine the cost of security screening management to the organization with each participant. It was anticipated, however, and borne out in the interviews that not everyone would have all of the information required to complete the task, and that there would be significant variation in the cost per organization and cost per application. Based on the results of the interviews it is virtually impossible to determine an “average” or representative cost to an organization or per application, but the interviews provided some key drivers in the variation.

a) Estimating Costs

The following table provides some breakdown and overall cost to an organization, and per application, for each of the 20 organizations in the study. Although results cannot be used to predict or extrapolate costs for others, it is helpful in understanding the key factors that drive differences in costs. Based on only these 20 interviews, and the information participants were able to provide, key drivers in cost can be:

- The level of seniority of the CSO (i.e., salary level);
- Whether or not the organization pays applicants for their time to complete the application and/or obtain finger prints;
- If the applicant is paid for their time, the salary level of the applicant;

- Whether or not the organization assumes the cost of the finger prints, or if this cost is assumed by applicants themselves; and,
- The volume of applications completed annually.

Two other elements in determining cost were fairly consistent across many of the interviews: participants tend to overestimate costs for the overall task, until it is broken down into smaller units of work; and many are unsure of the rate of company overhead.

The following table provides details of the costs to the extent that information was available from each of the 20 interviews.

Relatively few of the organizations interviewed said that they track the costs related to management of security screening. In spite of this, most were also not overly surprised by the cost and generally found it to be in line with the cost expectations of doing business. Only a few found the costs surprisingly high.

Costs									
Interview	Type	Resource	Hours	Wage /hr	Expenses	Cost/app	Volume	Annual Total	Note
1.	Reliability	CSO	1.5	\$ 24.04	--	--	--	--	--
-	Reliability	Applicant	2	\$ 40.00	\$60.00	\$ 176.06	180	\$ 31,690.80	Includes overhead
-	Secret	CSO	5	\$ 24.04	--	--	--	--	--
-	Secret	Applicant	3.5	\$ 40.00	\$60.00	\$ 320.20	200	\$ 64,040.00	--
-	Total		--	--	--	--	380	\$ 95,730.80	--
2.	Reliability	CSO	0.5	\$ 38.50	--	\$ 19.25	1200	\$ 23,100.00	Includes overhead
-	Reliability	Applicant	NA	--	NA	--	--	--	--
-	Secret	CSO	1.25	\$ 38.50	--	\$ 48.13	100	\$ 4,813.00	--
-	Secret	Applicant	NA	--	NA	--	--	--	--
-	Other Annual	CSO	72	\$ 38.50	--	--	--	\$ 2,772.00	--
-	Total		--	--	--	--	1300	\$ 30,685.00	--
3.	Secret	CSO	3	\$ 183.00	\$40.00	\$ 589.00	10	\$ 5,890.00	Includes overhead
-	Secret	Applicant	--	--	--	--	--	--	--
-	Total		--	--	--	--	--	\$ 5,890.00	--
4.	Both	--	--	--	\$75.00	\$ 400.00	50	\$ 20,000.00	No other specifics provided
5.	Both	CSO	10	\$ 22.00	--	--	--	--	--
-	Both	Applicant	1.5	\$ 26.67	\$60.00	\$ 320.01	3	\$ 960.02	--
-	Other annual	--	22	\$ 22.00	--	--	--	\$ 484.00	--
-	Total		56.5	--	--	--	--	\$ 1,444.02	--
6.	Reliability	CSO	4	\$ 112.50	--	--	--	--	Includes overhead
-	Reliability	Applicant	2	\$ 112.00	\$75.00	\$ 749.00	6	\$ 4,494.00	Applicant paid to get FPs only
-	Secret	CSO	8	\$ 112.50	--	--	--	--	--
-	Secret	Applicant	NA	\$ 112.00	NA	\$ 900.00	4	\$ 3,600.00	Applicant uses Reliability FPs
-	Other annual	CSO	32	\$ 112.50	--	--	--	\$ 3,600.00	--
-	Total		100	--	--	--	--	\$ 11,694.00	--

Costs									
Interview	Type	Resource	Hours	Wage /hr	Expenses	Cost/app	Volume	Annual Total	Note
7.	Both	CSO	2.5	\$ 475.00	--	--	--	--	--
-	Both	Applicant	5.5	\$ 500.00	\$50.00	\$ 3,987.50	3	\$ 11,962.50	--
-	Other annual	CSO	8	\$ 475.00	--	--	--	\$ 3,800.00	--
-	Total		32	--	--	--	--	\$ 15,762.50	--
8.	Both	CSO	2.5	\$ 67.31	--	\$ 168.28	300	\$ 50,484.38	Includes overhead. Estimated 15hrs/week in apps
-	Both	Applicant	NA	NA	NA	--	--	--	Do not pay for application time or FP costs
-	Other annual	--	400	\$ 67.31	--	--	--	\$ 26,925.00	--
-	Total		1150	--	--	--	--	\$ 77,409.38	--
9.	Reliability	CSO	5	\$ 24.00	--	--	--	--	--
-	Reliability	Applicant	NA	--	\$50.00	\$ 170.00	20	\$ 3,400.00	Do not pay for application time
-	Secret	CSO	6	\$ 24.00	--	--	--	--	--
-	Secret	Applicant	NA	--	\$50.00	\$ 194.00	50	\$ 9,700.00	Do not pay for application time
-	Other annual	--	400	\$ 24.00	--	--	--	\$ 9,600.00	--
-	Total		800	--	--	--	--	\$ 22,700.00	--
10.	Reliability	CSO	1.5	\$ 21.64	--	--	--	--	--
-	Reliability	Applicant	NA	--	\$50.00	\$ 82.46	552	\$ 45,517.92	Do not pay for application time
-	Other annual	--	25	\$ 21.64	--	--	--	\$ 541.00	--
-	Total		853	--	--	--	--	\$ 46,058.92	--
11.	Both	CSO	3	\$ 75.00	--	--	--	--	--
-	Both	Applicant	NA	--	\$93.88	\$318.89	49	\$15,625.12	Do not pay for application time
12.	Reliability	CSO	1	\$ 19.50	--	\$19.50	416	\$8,112.00	Do not pay for application time or FP costs
13.	Both	ACSOs	1	\$ 25.00	\$75.00	\$100.00	25	\$ 2,500.00	No details provided
-	Total	CSO	50	--	--	--	--	\$ 15,000.00	--

Costs									
Interview	Type	Resource	Hours	Wage /hr	Expenses	Cost/app	Volume	Annual Total	Note
-	Total		--	--	--	--	--	\$ 17,500.00	--
14.	Both	CSO	4	--	--	--	50	--	--
-	Other annual	--	40	--	--	--	--	--	No details provided
-	Total		240	--	--	--	--	\$10,000.60	--
15.	Both	CSO	--	--	--	--	--	\$42,250	Provided only as % of salary
-	Both	Applicant	NA	--	\$60.00	--	21	\$1,260	--
-	Total	--	--	--	--	--	--	\$43,510	--
16.	Both	CSO	1.5	--	--	--	--	--	--
-	Both	Applicant	.5-1.5	--	--	--	--	\$60,000.00	No details provided
17.	Reliability	CSO	.12	--	--	--	--	--	--
-	Reliability	Applicant	1	\$35.00	\$45.00	--	--	--	--
-	Secret	CSO	.4	--	--	--	--	--	--
-	Total		2	--	--	--	--	--	Missing information – cannot calculate
18.	Reliability	CSO& applicant	4	\$200.00	\$60.00	\$860.00	10	\$8,600	
19.	Both	CSO& applicant	8-10	--	--	--	2000	\$1,000,000.00	No details. Assumes \$500/application (about \$46.00/hr)
20.	Both	ACSO	.3	\$100	--	\$30	5	\$150	Do not pay for application time or FP costs

2.5 CHANGES WITH AN IMPACT ON EFFICIENCY/COST

When asked about key suggestions, improvements and changes that would increase efficiency and reduce costs, most referred back to primary sources of frustration described earlier. Suggestions include:

- A single contact at CSP to go back to about all issue areas related to an application (i.e., a single reviewer assigned and identified);

“Please identify a real person at the end (of a request) rather than an anonymous black box.”

“I think actually having a call center that could help you a bit better through the process or even having them be able to review it thoroughly prior to rejecting it or sending it back to you. I think those are two efficiencies that could definitely help.”

“I think it’s actually mostly having them be able to see what’s on your screen so you can talk to them directly about what the issue is.”
- A service level agreement/predictable estimated time for turnaround unless there are specific flags that make the cases complex, in which case, there is a predictable, estimated time to receive notification of this;

“I should be able to ask and receive a clear / accurate status check on any clearance application. It should be available through an online dashboard.”

“They should have a service level agreement that says unless there’s an indicator of some problem any clearance request should be settled within 5 days because this is just a computer check.”
- Better information, transparency on issues as they are flagged, with detail of status (with update notification sent as status changes);
- Address the perceived dichotomy that an applicant must be working on a project to apply for a clearance but can not work on the project without a clearance.
- Keep everything (update status, notifications of issues, submissions, etc) entirely within OLISS;
- Provide updated forms and added instructions to make it easier for applicants to complete the forms on paper;
- Provide detailed check lists for organizations, with comprehensive explanations, about what to do and in what order to do it. Also provide a review checklist prior to submission;

- OLISS automated check for gaps in timeline, use of copies instead of originals, missing documents/information;

“I think cutting out the fax and doing more electronic notification would make a big difference to me personally.”

“If they could have an update that also anticipated completion time that would be super helpful.”
- Better access to the call centre and shorter response time, along with more knowledgeable staff;
- Streamlined information requirement through linking to other Government of Canada systems (e.g., birth certificates, passports CRA tax data etc), along with possibly linkages to provincial data (e.g., drivers license) to streamline identification. This is particularly applicable to renewals and transfers where the information already exists.

“It kind of seems like wasted effort to me you know? If you’re cleared you’re cleared so why do I have to have an application to have it moved over? And I understand the whole reason for it is because you’re tied to another organization but on a certain level it just kind of seems like rubber stamping.”

“To me you can simply request a passport. If you’ve got through the passport process you’ve gone through all that security and it has your birth date on it, where you were born, so just ask for the passport.”
- Charge a fee per security clearance application to recover some costs and avoid putting background check responsibility onto organizations. This may also result in a reduced volume of applications because many organizations indiscriminately apply for all new hires because of unpredictable wait time.
- Enable OLISS reports to be exported to Excel, with room for one or two customizable fields.
- Revamp webinars to make them more relevant to certain industries and useful for answering FAQs.

APPENDIX A
RECRUITMENT REGISTRATION

APPENDIX A: Recruitment Registration

ENG (Email)

Research on Managing the Security Screening Process - EKOS | Recherche sur la gestion du processus de vérification de sécurité - EKOS

(La version française du message suit)

Dear _____,

The Contract Security Program (CSP) within Public Services and Procurement Canada has commissioned EKOS Research Associates, a national Public Opinion research provider, to conduct research on its behalf. Last year you completed a survey for us about your experiences in accessing the Online Industrial Security Services (OLISS) Portal for individual security screening (e.g., in managing applications for reliability, secret or top secret screening). At the end of the survey, you agreed to being contacted in the future to possibly participate in a follow-up interview.

We are contacting you now to ask for your participation in an interview to be conducted by telephone with a researcher from EKOS, in the next few weeks. It will take between 30 and 60 minutes, and you will be asked to expand on your experiences with managing the security screening process in your organization. Recognizing that your time is valuable, we will send you a cheque for \$150 to thank you for participating.

Your participation in the interview is confidential. We will not share any information that could identify you or your business with CSP or any other third party at any point during or after the research is completed.

Please click on the link below to select the best time and day to complete an interview. We will follow up with a phone call to confirm the appointment.

<CLICK HERE>

If you have any issue with the link above please copy the following link into your browser:

<https://surveys.ekos.com/ekos/cwx.cgi?EN:07119:{ID}>

If you have any questions about how to answer the survey, please contact <.....> at the following address: <.....>. If you feel that you have received this email in error, or have other questions about the survey, please contact <.....> at the following address: <.....>

Please note that EKOS adheres to the requirements of the *Privacy Act*. The report that results from this research will be made publicly available in approximately six months' time on the Library and Archives Website. For more information, or to learn about your rights under the *Access to Information Act*, contact Salim Barghouth at Salim.Barghouth@tpsgc-pwgsc.gc.ca.

Sincerely,

Susan Galley
Vice President
EKOS Research Associates Inc.

Privacy Notice

Provision of the personal information is collected on a voluntary basis pursuant to the *Financial Administration Act*. Personal information is anonymized by the system. As part of its examination of the contract security screening process to help improve its practices, the Industrial Security Sector of Public Services and Procurement Canada (PSPC) will use the anonymous data to assess the efficiency and effectiveness of contract security services, and cost to companies, in order to offer a valid basis of comparison later on. The information collected is described under the Standard Personal Information Bank [Public Communication PSU 914](#). Your personal information is protected, used, and disclosed in accordance with the *Privacy Act*. Please do not disclose unnecessary confidential information about yourself or other individual. If you require clarification about this notice, you can contact the PSPC Privacy Director by email at AIPRP.ATIP@tpsgc-pwgsc.gc.ca; by phone at 873-469-3721, or by regular mail at the following address: Privacy Director, Place du Portage, Phase III, 5C1, 11 Laurier St, Gatineau, Quebec, K1A 0S5. If you are not satisfied with our response to your privacy concern, you may wish to contact the Office of the Privacy Commissioner of Canada.

Introduction

Thank you for your interest in completing an interview.

The interview will be conducted by telephone and should take between 30 and 60 minutes to complete.

We will ask you to tell us more about how the process of managing the security application works in your organization and what is working well and what is not, as well as what additional information or communications would help you with the process.

Using the drop-down boxes below, please provide the time and date most convenient for you to complete an interview. If possible, please provide a second-choice alternative in case your preferred time is unavailable. Someone will call you to confirm an exact time.

Q1A

Select Preferred time - First Choice/Second choice/Third Choice:

PQ2

Please provide your name, telephone number and email address below to allow us to reach you if you are selected to participate.

QFNAME

First name

1

QLNAME

Last name

1

QEMAIL

E-mail address

1

QTELEPHONE

Telephone

2

THNK

Thank you for your interest. We will be in touch by email and telephone if you are selected to participate in a discussion.

APPENDIX B
INTERVIEW GUIDE

APPENDIX B: Interview Guide

Public Services and Procurement Canada (PSPC) operates the Contract Security Program (CSP), which provides contract security screening of organizations and their personnel doing business with the Government of Canada. The CSP has commissioned EKOS Research Associates (EKOS) to conduct research to gather information and help inform program decisions and process improvements.

As part of this study, EKOS is conducting a number of interviews among organizations currently registered with the Program. The interviews are intended to expand the Program's understanding of:

- what is involved for businesses to manage the security screening process within their organization;
- the cost to businesses for this activity; and,
- what the Program can do to help make this process as effective and efficient as possible for businesses.

Recognizing that your time is valuable, we will send you \$150 to thank you for participating. The interview is expected to last between 40 and 60 minutes. Participation is voluntary and your confidentiality will be respected. No information that might directly or indirectly reveal your identity will be released or published without your specific consent to the disclosure. Further, the program will not be informed of the respondent names or organizations of those participating. However, the interview will be recorded to allow the interviewer to prepare summary notes from the interview. The recording will be destroyed once the notes have been finalized.

Introduction

1. To start off, what is your role within your organization?
2. What is your involvement with the Contract Security Program?
 - a. How familiar would you say you are with the overall process and with OLISS?

Application Process

3. What does the process of applying to the CSP look like for your organization?
 - a. Who does this activity? Does it occur within the organization or do you contract this out to someone else?
 - b. Is it one person or many within your organization? Are they dedicated to this activity or do they also have other areas of responsibility? Is it consistently the same person/people doing this work?
 - c. Are applications started and finished at one time, or worked on a little bit at a time, while juggling other activities?

- d. Who trains someone new to manage this activity, if needed?
4. When you think about the process involved in managing contract screening, what do you consider to be the beginning of the process?
 - a. Is it the start of an application or is there something before this that signals the “start”?
5. When is the process “complete”?
 - a. Is it when the application is successfully filed or when the approval is received? A different point in time?
6. How long is this process (in weeks) typically for a Reliability clearance? For Secret/Top Secret?
 - a. Does this seem like an appropriate length of time?
7. What is the failure rate of applications? What is the most common reason(s) why this occurs?
 - a. What does this mean for delays and overall length of time to complete?
 - b. What does this mean for added time to work on the application?
8. Do you find you need assistance at anytime to navigate the application process? Is it always at the same place in the process? What kind of assistance (e.g., training, advice)?
 - a. How well is this assistance working for your business?
 - b. Is there anything that you feel needs to be changed or emphasized to make this part of the process work better, or be more helpful to you?
9. Are there areas generally where you feel the application process is cumbersome or ineffective? What would be needed to address any issues you have had with managing contract screening? Can you provide some specific examples?

Cost

The main objective of this interview is to try and understand better what the cost implications are for managing contract screening for your business. For this reason, I'd like us to try and break down what is involved in the process and what it means in cost to your organization.

10. **(If contract out)** What is your best estimate of how many applications are processed for you each year?
 - a. How much does your organization pay for this service each year, on average?
 - b. What we really want to get at is, how much do you think you pay for each application for Reliability? How about for Secret/Top Secret? What else do you pay for and how much does that cost?

11. **(If kept in-house)** Has your organization ever tried to break down the cost for activities involved in managing the security screening application process? If so, what have you estimated that it costs to your organization to comply with the CSP requirements?
12. Whether you have or haven't tried to pinpoint the cost associated with managing the security screening application process, let's go through some of the basic elements in calculating this.
 - a. How many hours (in a week/month/year) are dedicated to actively managing the security screening process? Would you be able to estimate an "average" number of hours to complete the process for 1 application for a Reliability clearance? How about for a Secret/Top Secret clearance?
 - b. Other than the actual application, is there a broader "effort" involved in managing the process (e.g., training, record keeping, communications with CSP, other)? How many hours would this include (in a week/month/year)?
 - c. At what personnel level is this function typically done? What is the salary for this level? Let's break down the amount of salary directly dedicated to the security screening process?
 - i. Probe: Is this a person who is dedicated to this task alone or are they juggling this with other tasks? Does this become the main priority?
 - d. Are there any other direct financial costs (e.g., cost for training)? What more would need to be added, if anything to calculate a complete figure including any overhead?
13. Now that we have calculated a cost per application for a Reliability clearance and for a Secret/Top Secret clearance, or an overall cost per year to your organization, does this seem to be about what you were thinking it was?
14. Going back to what we talked about earlier, is there anything that CSP could be doing to help your business to reduce the time or the costs associated with managing the security screening process?
 - a. What could be changed to assist you?
 - b. In what way would this help and how would it translate into reduced costs for you?
 - c. Is there any impediment that in your opinion could be removed that would streamline the process for you?
15. If CSP were to concentrate its efforts to improve one area of the security screening process, what would make the biggest difference to your organization?
 - a. If you were in charge of the Program, what one change or idea would you implement?

Conclusion

16. Do you have anything else you would like to add?

Thank you for your participation!