

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

**Table of contents**

1. <a href="#">Background</a> .....	p.1
2. <a href="#">Changes coming into effect on May 2, 2022</a> .....	p.3
3. <a href="#">Federal procurement process</a> .....	p.3
4. <a href="#">Provisional security clearances</a> .....	p.4
5. <a href="#">Organization security screening process</a> .....	p.7
6. <a href="#">Organization security screening timelines</a> .....	p.8
7. <a href="#">Validity of organization clearances</a> .....	p.9
8. <a href="#">Organization clearance renewal process</a> .....	p.11
9. <a href="#">Physical and IT security inspection process</a> .....	p.11
10. <a href="#">Subcontracting process</a> .....	p.13

---

**1. [Background](#)**

**Q1. Why is PSPC’s Contract Security Program (CSP) changing the eligibility criteria to obtain, renew or upgrade an organization security clearance?**

A 5-year analysis of CSP security processing volumes revealed that close to 90 percent of organizations screened by the CSP have not been associated with a contract or subcontract with security requirements. Processing volumes for personnel security screening, on the other hand, revealed that less than 20 percent of individuals screened by the CSP worked on a contract or a subcontract with security requirements during that same 5-year period.

## **Questions and answers for industry**

### **Phase two of changes to the security screening process**

---

This significant effort to screen organizations who are not in need of a clearance puts needless pressure on the Government of Canada's security infrastructure. It creates unnecessary screening delays, weakens the security posture of Canadian industry and ultimately increases the risk that organizations pose to sensitive government information and assets.

#### **Q2. What are the benefits of this change to private sector organizations like mine?**

By refocussing organization security screening activities on active participants in a procurement process, the expected benefits are:

- Faster processing of organization security screenings
- Better support to industry in the delivery of important services and activities for the benefit of Canadians
- Reduced burden on industry, particularly on company security officers and alternates
- A streamlined subcontracting process with increased flexibilities to diversify supply chains and reduce costs
- Contribute to enhance the competitiveness and marketability of Canadian industry in foreign defence and security markets

#### **Q3. How does this approach compare with what other countries are doing?**

Universally, security clearances are granted on a need-to-know / need-to-access basis only. The security screening process is in fact only initiated upon confirmation of a demonstrated requirement, such as a valid contract or a demonstrated "need to know". Over 30 like-minded foreign partners conduct their clearances this way.

This approach enables other countries to have better service standards than the CSP. It also makes their industry more competitive on foreign markets. Aligning the CSP's rigorous security screening process with the approach of our international partners will provide for a better calibrated, focused, flexible and performant industrial security program.

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

**2. Changes coming into effect on May 2, 2022**

**Q4. Which changes are being implemented on May 2, 2022?**

Beginning May 2, 2022, the CSP will:

- Screen new organizations, and renew or upgrade the security clearance of existing organizations, who:
  - have responded to a government solicitation with security requirements;
  - will be awarded a contract with security requirements against a standing offer or supply arrangement;
  - will be awarded a sole source contract with security requirements;
  - will be awarded a subcontract with security requirements;
  - are underrepresented; or
  - are involved in a multinational program.
- Introduce a new provisional security clearance for organizations that require access to sensitive information or assets during the pre-solicitation stage of a procurement process.
- Introduce flexible options for contractors to simplify the subcontracting process.
- Reassess screened organizations for continued eligibility into the Program in accordance with existing policy requirements outlined in the [Contract Security Manual](#) and the Security Agreement.
- Review all organization security screening requests still in process and close those that do not meet the new eligibility criteria.

**3. Federal procurement process**

**Q5. Will all federal procurements be subject to these changes?**

Yes. These changes will apply to all federal procurements for goods, services and construction where the CSP's contract security services are used.

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

**Q6. How will these changes affect organizations bidding on solicitations with security requirements?**

Beginning on May 2, 2022, organizations bidding on government solicitations with security requirements will be required to complete and provide an Application for Registration form (PSPC 471) as part of their bid response (i.e. their proposal). This includes responses to requests for standing offer and requests for supply arrangement.

**Q7. If access to protected or classified information is only required to execute the contract, will my organization still be required to hold a security clearance at bid closing?**

No. As a result of these changes, organizations will only need to meet security requirements during the bid solicitation process if they are required to access protected or classified documents to prepare their bid submission. If access to protected or classified information is only required to execute the contract, government procurement officers must give bidders until the date of contract award to obtain their organization security clearance.

This will put all potential bidders on the same level playing field and provide a more competitive business environment by ensuring that organizations of all sizes are eligible to bid on government tenders with security requirements, regardless of whether or not they have a clearance with the CSP.

**4. Provisional security clearances**

**Q8. Will provisions be made for accessing protected or classified material in the course of a pre-solicitation and/or bid preparation?**

Yes. On May 2, 2022, the CSP will introduce a new provisional security clearance to provide a faster and less burdensome screening process for potential bidders requiring access to sensitive information prior to bidding (e.g. to access classified requests for proposal).

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

This new clearance will allow potential bidders to have a few individuals cleared prior to bid submission. Confirmed respondents to the associated solicitation will then be invited to complete the organization screening process to obtain a designated organization screening or facility security clearance with the CSP, in line with the new eligibility criteria.

**Q9. How can my organization request a provisional security clearance?**

To request a provisional security clearance, organizations must approach the procurement officer overseeing the solicitation to demonstrate their interest in participating, and to request a security screening if they do not already hold the appropriate level of clearance. Organizations must also provide the procurement officer with a complete Application for Registration form (PSPC 471). The procurement officer will then contact the CSP to request a provisional security clearance on the organization's behalf.

**Q10. What process must my organization follow to obtain a provisional security clearance?**

Once the CSP receives a valid request from a procurement officer, the CSP will conduct an organization assessment and request the following documentation from the organization:

- A company security officer appointment and acknowledgment and undertaking form to appoint a company security officer (CSO)
- Personnel security screening forms for the CSO and for the individuals that have been identified for the bidding team.
- Signed Security Agreement
- Personnel security screening forms for one key senior official (for classified level screenings only)

If the requirement is at the protected level, the CSO and individuals of the bidding team will be required to complete the [TBS/SCT 330-23](#) form, subject themselves to a mandatory fingerprint check and undergo a reliability status screening in accordance with the Treasury Board of Canada Secretariat (TBS) [Standard on Security Screening](#).

## Questions and answers for industry

### Phase two of changes to the security screening process

---

If the requirement is at the classified level, the CSO, the key senior official (KSO) and the individuals of the bidding team will be required to complete the [TBS/SCT 330-23](#) and [TBS/SCT 330-60](#) forms. They will also need to subject themselves to a mandatory fingerprint check, and, depending on the requirement, undergo a security screening at the secret or top secret level in accordance with the TBS Standard on Security Screening.

For all levels of provisional security clearances:

In section A of the TBS/SCT 330-23 form for the CSO, and if applicable, the KSO, the organization must reference scenario 3, from the list of [Scenarios that are accepted as justification to process personnel security screening requests](#).

In section A of the TBS/SCT 330-23 form for the individuals of the bidding team, the organization must reference scenarios 6, 7, 8, 9, 10 or 11, depending on the type of pre-solicitation they are participating in.

For more information on the reliability status and security clearance process for personnel, visit [Personnel security screening processes](#).

#### **Q11. How long will provisional security clearances be valid for?**

Provisional security clearances will be valid for the duration of the bid solicitation stage only. The reliability status or security clearances of the CSO, KSO (as applicable) and individuals of the bidding teams will also only be valid for the duration of the solicitation stage. However, if the organization submits a bid response, the CSP will allow the organization to retain the CSO's, and if applicable, the KSO's personnel screening. All other personnel screenings will be closed-out.

#### **Q12. Are foreign organizations also eligible for a provisional security clearance?**

No. Foreign organizations requiring access to Canadian classified information at the pre-solicitation and/or bid preparation phase(s) will continue to require a facility security clearance granted by their respective national Designated Security Authority and confirmed by the CSP with their foreign counterparts.

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

If a foreign organization requires access to Canadian protected information at the pre-solicitation and/or bid preparation phase(s), the CSP will continue to assess their eligibility for an alternative solution. If eligible, the CSP will request documentation (e.g. criminal record checks, credit checks) from the foreign organization in order to assess the risk associated to the handling, processing and safeguarding of the Canadian protected information.

**5. Organization security screening process**

**Q13. How will these changes affect the organization security screening process?**

Beginning May 2, 2022, all organizations bidding on a solicitation, request for standing offer or request for supply arrangement with security requirements posted on or after May 2, 2022 will be required to complete the CSP Application for Registration (AFR) form (PSPC 471) during the bid solicitation process and submit the completed form with their bids.

A complete AFR means that all mandatory blocks of information have been filled out and the form is signed and dated. Incomplete AFRs will not be processed by the CSP and may lead to the rejection of the organization's bid by the procurement officer responsible for the solicitation process.

Beginning May 2, 2022, organizations being awarded a sole source contract with security requirements will also be required to complete the AFR form and submit it to the procurement officer responsible for the contract.

Upon receipt of the AFR(s) and confirmation from the contracting department that the organization submitted a bid response or will be awarded a sole source contract, the CSP will initiate the organization security screening process and contact the organization directly to request additional screening documentation.

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

**Q14. What will happen to the organization security screening of unsuccessful bidders?**

As of May 2, 2022, bidders that are not awarded a contract or subcontract with security requirements will continue to be eligible for a security clearance and permitted to complete the organization security screening process, even if they are unsuccessful.

**Q15. If my organization recently obtained, renewed or upgraded its security clearance, will I be required to complete a new Application for Registration Form to bid on a new solicitation with security requirements?**

Yes. Organizations that are already screened by the CSP and that are bidding on a new solicitation, request for standing offer or request for supply arrangement with security requirements will need to complete the Application for Registration (AFR) form (PSPC 471) as part of their bid response.

To reduce the administrative burden, organizations bidding on a solicitation, request for standing offer or request for supply arrangement with security requirements should save the information from their previously completed AFR form. At the next solicitation, these organizations will only need to amend the form (if information has changed from their previous bid response), resign it and date it before submitting it with their bids.

**Q16. How will these changes affect organizations that were sponsored for registration in the CSP prior to May 2, 2022?**

Requests for private sector organization screening received prior to May 2, 2022 and that are still pending as of that date will be reassessed by the CSP to ensure they meet the new eligibility criteria. If a request is no longer eligible, the CSP will close it. Please refer to Q4, above, for the list of eligibility criteria for organization security screenings.

**6. Organization security screening timelines**

**Q17. How will these changes improve organization security screening timelines?**

By eliminating the broad security screening of suppliers and implementing a more targeted approach, the CSP expects the following improvement in processing times for **simple** organization security screening requests.



**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

- Designated organization screenings
  - Current: 50 business days (on average)
  - Target: 30 business days, 85 percent of the time
  
- Facility security clearances
  - Current: 124 business days (on average)
  - Target: 75 business days, 80 percent of the time

These shorter processing times are not new service standards; they are targets set by the CSP to measure its performance. As the CSP implements the changes, it will monitor service levels against these targets to assess the effectiveness of the change. If a decline in service levels is observed, the CSP will adjust its approach accordingly. If an improvement in service levels is observed and sustained, the CSP will review its service standards and update them to reflect the new reality.

**7. Validity of organization security clearances**

**Q18. How long will organization security clearances be valid for?**

Organization security clearances granted on or after May 2, 2022 will be valid for 2 years for designated organization screenings and 1 year for facility security clearances. At the end of this period, the CSP will terminate the organization's security clearance if the organization is not participating in another procurement process or executing a contract or subcontract with security requirements.

Organizations that actively bid on government solicitations with security requirements with a complete Application for Registration form (PSPC 471) should not worry about having their organization security clearance terminated, even if they do not have any active contracts or subcontracts. In this case, the organization's security clearance will remain active as long as it continues to bid on government solicitations with security requirements.

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

**Q19. How will these changes affect organizations that have already been screened by the CSP?**

These changes will not immediately impact organizations that have been granted a designated organization screening (DOS) or facility security clearance (FSC) prior to May 2, 2022. When the DOS or FSC is due for renewal, the CSP will assess if there is a need to maintain the clearance by confirming if the organization is involved in a solicitation process, or has been awarded a contract or subcontract with security requirements.

If the CSP is not able to validate that the organization has a requirement to renew their organization clearance, it will terminate the clearance in accordance with the [Contract Security Manual](#) and the organization's Security Agreement.

**Q20. Will it be possible to reactivate my organization's security clearance after the CSP has terminated it?**

Yes. Once terminated, an organization's security clearance will be eligible for reactivation if the organization is engaged in another solicitation process (and submits a complete Application for Registration form with their proposal) or is awarded a contract or subcontract with security requirements within:

- 2 years of the termination date for designated organization screenings and reliability status; or
- 1 year of the termination date for facility security clearances at the secret/top secret/NATO levels and equivalent personnel security clearances.

This reactivation window aligns with the Treasury Board of Canada Secretariat [Standard on Security Screening](#) and with Canada's international and NATO obligations.

**Q21. How can I reactivate my organization's security clearance with the CSP?**

If the CSP terminated an organization's security clearance because the organization did not submit a proposal against a solicitation with security requirements within the timeframe indicated in Q20, above, the organization can reactivate its clearance by bidding on a government solicitation with security requirements with a complete Application for Registration form.

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

To reactivate an organization security clearance, the procurement officer overseeing the solicitation must submit a security screening request to the CSP. Upon receipt, the CSP will validate the organization's information and request additional screening documentation from the organization as needed.

If there are no changes to the organization's key people, the CSP will also request the [TBS/SCT 330-23](#) form for the company security officer (CSO) and if applicable, for the key senior officials (KSO), to reactivate their reliability status or security clearance. Depending on the date their reliability status or security clearance was closed-out, the CSO and KSO may need to undergo a new fingerprint check.

For more information on personnel security screening reactivations and mandatory fingerprinting, visit [Reactivate a previously held security status of clearance](#) and [Mandatory electronic fingerprints](#).

#### **8. Organization clearance renewal process**

##### **Q22. How do I renew my organization clearance?**

When an organization bids on a government solicitation with security requirements, the CSP will automatically renew the organization's security clearance. If the organization is under a long term contract, the CSP will contact the company security officer, as required, to ensure the clearance remains valid.

#### **9. Physical and information technology security inspection process**

##### **Q23. How will these changes affect organizations that require a document safeguarding capability or the authority to process information technology (IT)?**

Organizations requiring one or more security safeguards (document safeguarding capability, production capability, and authority to process IT), will be invited to undergo a physical security inspection during the bid evaluation stage. This is referred to as a bid inspection.

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

During the bid inspection, bidders will be made aware of the recommendations and corrective measures they have to implement to obtain a document safeguarding capability (DSC). From there, it will be up to the bidders to decide if they want make the required changes to their facilities, either before contract award or once they have secured the contract. Once the successful bidder has been identified, the CSP will complete the inspection and grant them a DSC.

The authority to process IT is already contract-specific and triggered after contract award. The IT security inspections will continue to be conducted on the successful bidder only, once physical security requirements have been met and once all IT assets utilized by the supplier to create the contract deliverables have been installed and configured.

**Q24. What will happen if my organization does not implement the CSP's recommendations and corrective measures during the bid evaluation stage?**

Implementing the CSP's recommendations and corrective measures can represent a significant investment that bidders may not be willing or able to make before contract award. However, the CSP strongly encourages bidders to make the necessary changes to their facilities following their bid inspection. This will allow the CSP to complete the inspection process for successful bidders in a much timelier manner, and to initiate in parallel, the IT security inspection process (if applicable). It will also ensure the timely awarding of contracts with document safeguarding capability requirements and prevent delays in the delivery of goods and services.

**Q25. How will these changes affect an organization's document safeguarding capability?**

These changes will not immediately affect organizations that have been granted a document safeguarding capability (DSC), or that were sponsored for a DSC prior to May 2, 2022. However, if these organizations do not hold an active contract or subcontract with physical security requirements as of May 2, 2022, they will not be permitted to renew their DSC.

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

When the designated organization screening (DOS) or facility security clearance (FSC) of these organizations are due for renewal, the CSP will assess the need for the organization to maintain their security clearance. If the CSP is not able to validate the requirement for a DOS or FSC, it will terminate the organization's security clearance and their DSC, in accordance with the [Contract Security Manual](#) and the organization's Security Agreement.

**Q26. What will happen if my organization is required to retain protected or classified information/assets at my worksite(s) after the contract is completed?**

Organizations with a document safeguarding capability (DSC) that are contractually required to retain protected or classified information/assets at their worksite(s) after the contract is completed/expired, will be permitted to maintain their DSC and organization security clearance for the duration of the retention period. At the end of the retention period, once the protected or classified information has been returned to the client department, or destroyed at the CSP's request, the CSP will terminate the DSC, unless the organization has a new contractual requirement to safeguard protected or classified information/assets at their worksite(s).

**10. Subcontracting process**

**Q27. How will this change affect the subcontracting process?**

Organizations that have been awarded a contract or subcontract with security requirements can continue to sponsor their subcontractors for an organization clearance by completing the [Security Requirements Check List \(TBS/SCT 350-103\)](#) and [Request for private sector organization screening form](#).

Upon receipt of these forms, the CSP will continue to perform the necessary organization and personnel security screenings on legitimate subcontractors with a valid security requirement to assist the prime contractor in delivering its contractual obligations.

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

**Q28. What is the CSP doing to improve the subcontracting process for contractors?**

To reduce the burden on industry, the CSP reviewed its subcontracting process to explore ideas toward a simpler and more flexible process for contractors. Starting May 2, 2022, organizations can leverage two new options to request security screenings for their respective subcontractors. These new options replace the subcontractor compliance measure for independent contractors / individual business entities that was communicated to organizations on June 26, 2014.

Option one: Prime contractor requests and holds personnel security screenings for employees of their subcontractors (see Q31 and Q32 for more information).

Option two: Prime contractor collects the organization security screening forms from their subcontractors, reviews them for quality assurance and submits them to the CSP for processing (see Q33 to Q35 for more information).

**Q29. Is my organization obligated to leverage these options?**

No. Organizations can continue to follow the current subcontracting process if the new options do not suit their particular circumstances. These options were developed to improve security screening timelines for subcontractors, diversify supply chains and address challenges associated with short bid validity periods, seasonal workforces and labour shortages.

**Q30. Can my organization leverage both options for the same subcontracting organization?**

Yes, absolutely.

**Q31. When should my organization leverage the first subcontracting option?**

This option can be used by organizations (prime contractors and subcontractors) that subcontract work to sole proprietors or small organizations, where only a small number of individual resources, are required. Organizations are to use their judgement and refrain from using this option to screen a large number of subcontractor resources.

## Questions and answers for industry

### Phase two of changes to the security screening process

---

The resources must also reside in Canada. As such, requesting foreign security clearances is not allowed under this option. Other conditions apply:

- Protected or classified information and assets cannot be received or stored at the subcontracting organization's business location.
- Work on the subcontract can only be performed at the government worksite or at the prime contractor's business location if it is authorized for document safeguarding capability.

#### **Q32. How can my organization leverage the first subcontracting option?**

To leverage option one, company security officers (CSO) and alternate company security officers (ACSO) must follow the CSP's [personnel security screening processes](#) and request, as required, a reliability status or security clearance for individuals of the subcontracting organization.

In section A of the [TBS/SCT 330-23E](#), CSOs and ACSOs must justify the security requirement using the list of [scenarios that are accepted as justification to process personnel security screening requests](#). In this case, the CSO or ACSO would reference *Scenario 2: Work performed on an active contract or subcontract with security requirements*.

When using this option, CSOs and ACSOs are, per their duties, responsible for resources of the subcontracting organization, who they may not know as well as their own employees. The CSO or ACSO requesting the personnel screenings must assume the responsibility of conducting [background checks](#) on the individuals and performing [aftercare](#), just like they would for any other employee of their organization.

#### **Q33. When should my organization leverage the second subcontracting option?**

Prime contractors can use this option when:

- They do not accept the responsibility and liability of requesting and holding personnel security screenings for employees of their subcontractor(s);
- The requirements of their subcontract(s) do not meet the conditions of option one; and

**Questions and answers for industry**  
**Phase two of changes to the security screening process**

---

- They are willing and able to support their subcontractor(s) to complete organization screening forms.

Furthermore, the subcontractor(s) must:

- not already hold an organization security clearance with the CSP;
- be willing and able to invest time to obtain their own security clearance; and
- provide their agreement in writing to the prime contractor to allow the prime to collect and share their forms with the CSP.

**Q34. If leveraging the second subcontracting option, is my organization still required to request subcontract security clauses from the CSP?**

Yes. Before leveraging the second option, the prime contractor must continue to seek approval of their subcontract(s) by completing a [Security Requirements Check List](#) for each subcontract and submitting the form(s) to the CSP at [tpsgc.ssilvers-issrcl.pwgsc@tpsgc-pwgsc.gc.ca](mailto:tpsgc.ssilvers-issrcl.pwgsc@tpsgc-pwgsc.gc.ca).

Upon receipt, the CSP will issue security clauses to the prime contractor. Per the current subcontracting process, the prime contractor must insert the CSP's clauses into their subcontract(s) and to submit a copy of their awarded subcontract(s) to the CSP at [tpsgc.ssicontrats-isscontracts.pwgsc@tpsgc-pwgsc.gc.ca](mailto:tpsgc.ssicontrats-isscontracts.pwgsc@tpsgc-pwgsc.gc.ca).

**Q35. How can my organization leverage the second subcontracting option?**

To leverage the second option, the prime contractor's company security officer (CSO) or alternate company security officer (ACSO) must use their expertise in CSP requirements and processes to assist their subcontractors with the completion and submission of a full organization security screening package. This package contains the following forms:

- CSP Application for Registration (PSPC 471), with supporting documentation
- Company security officer appointment and acknowledgment and undertaking
- Alternate company security officer appointment and acknowledgment and undertaking (if applicable)



## Questions and answers for industry

### Phase two of changes to the security screening process

---

- [TBS/SCT 330-23E](#) used to request a reliability status for the CSO
- [TBS/SCT 330-60E](#) used to request secret and/or top secret clearances for the CSO and key senior officials (in addition to the TBS/SCT 330-23E)
- Security Agreement

The CSO or ACSO of the prime contractor is responsible for providing these forms to their subcontractors. Once the subcontractor has completed the forms, they must submit their package to the CSO or ACSO of the prime contractor. Upon receipt, the CSO or ACSO must review the forms to ensure they are complete and accompanied with the necessary supporting documentation, before submitting them to the CSP at [tpsgc.ssiinscription-issregistration.pwgsc@tpsgc-pwgsc.gc.ca](mailto:tpsgc.ssiinscription-issregistration.pwgsc@tpsgc-pwgsc.gc.ca).

Once the CSP receives the screening package from the prime contractor, it will work directly with the subcontracting organization to process their organization clearance. While the screening process is underway, the subcontracting organization will be responsible for keeping their prime contractor updated on the status of their request. To obtain status updates, the subcontracting organization can contact the [Contract Security Program's client service centre](#).

To obtain copies of the CSP forms, prime contractors can contact the [Contract Security Program's client service centre](#).