Australian Government
Department of Finance

Guidance for the management of Notifications of Significant Events and breaches of the Commonwealth Supplier Code of Conduct

The purpose of this document is to provide guidance and encourage consistent assessment and action for any Notification of Significant Events (NoSE) and breaches of the Commonwealth Supplier Code of Conduct (the Code) in relation to Commonwealth procurement contracts. In this guidance, use of the word notification covers both notifications under the NoSE clauses and Code.

Under the Commonwealth procurement framework each entity is responsible for its own procurement and contract management processes and decisions to meet its business needs, in line with the Commonwealth Procurement Rules. This includes monitoring compliance, managing contract performance, identifying misconduct by suppliers (and undertaking necessary action) and managing any notifications.

This guidance provides high level advice on a process for responding to notifications. Depending on the nature of the goods or services being procured, whether a notification is classified as a significant event and/or breach of the Code will be at the discretion of the official/entity. Similarly, the severity of any significant event or breach will require the judgement of the official/entity and will be dependent upon a range of factors related to the specific contract.

Use of this guidance is optional, and the ultimate decision-making authority lies with each entity.

Introduction

The NoSE clause was introduced into the Commonwealth Contracting Suite and ClauseBank on 19 May 2023. The Code came into effect on 1 July 2024, mandated by the Commonwealth Procurement Rules for all Commonwealth forms of contract. Supporting clauses were published alongside the Code in the Commonwealth Contracting Suite and ClauseBank. For contracts that were entered into prior to the introduction of the NoSE clauses and Code, officials should strongly consider updating those contracts to include those clauses.

Receiving a notification

For those contracts that include the NoSE and/or Code clauses, officials may receive notifications from the supplier, another Commonwealth entity, or a third party. When handling a notification, it is important to consider the specific terms and conditions of the contract. Where the notification is not received from the supplier, the contract manager will need to approach the supplier to progress its consideration.

If multiple entities are notified by a supplier of the same significant event or breach, they may consider either coordinating a cooperative response, or an entity may

choose to respond on behalf of all notified entities, for example where a notification relates to a range of contracts entered into under a panel arrangement.

When receiving a notification, contract managers should engage with their legal and procurement teams for any additional processes and considerations that an entity has put in place.

Process for responding to a Notification of a Significant Event or a breach of the Commonwealth Supplier Code of Conduct

Phase 1 Identify and assess	• **Request** notification (if required) • **Receive** notification • **Assess** severity

Phase 2
Initial action
	• Undertake one, or a combination of the following actions:
	  ○ Request additional information
	  ○ **Watch and monitor**, reassess if necessary
	  ○ Issue a **warning**
	  ○ Request a **remediation** plan (proceed to phase 3) and consider **restricting** or **suspending** the supplier thoughout the remediation process
	  ○ If applicable, **contact** other entities that may have active contracts with the supplier
	  ○ Upfront **termination** for particularly severe incidents

Phase 3
Remediation
	• **Review** remediation plan
	• **Determine** next course of action:
	  ○ Accept remediation plan in its current state (proceed to phase 4)
	  ○ Request revised remediation plan
	  ○ Termination, if deemed necessary

Ongoing Communicate and monitor	• **Ongoing communication** with the supplier on the implementation of the agreed course of action • **Report** as required • **Ongoing monitoring** of the supplier's actions through regular communication and media monitoring • **Follow up** to ensure adherence and compliance to agreed remediation plan

Phase 1 – Identification and assessment

Step 0 – Request notification (if required)

- A potential significant event (event) under the NoSE clauses or a breach of the Code may be brought to the attention of a contract manager by a supplier, a third party such as the media, or may be noticed by the contracting Commonwealth entity itself. If a potential event/breach was identified without a *notice* by the supplier, contract managers may request the supplier provide a *notice* within 3 business days unless a different timeframe is agreed.
- Consider whether the potential event/breach should reasonably have been identified by the supplier and promptly communicated. If the supplier considers that an event/breach has not occurred, they may provide information to support that claim.

Step 1 – Receive notification

- A supplier must immediately notify contract managers on becoming aware of a potential event/breach. The *notice* should include a summary of the potential event/breach, the date it occurred, and details of the personnel involved.
- If the potential event/breach involves a contract under a panel arrangement, notify the manager of the panel. The panel manager may, at that time, seek to manage this process and provide guidance to the contracting entity on what further steps the entity should take.

Step 2 – Assess severity

- Gather all facts and evidence regarding the potential event/breach.
- Consider whether the notification consitutes a significant event under the NoSE clause and/or a breach of the Code. Consider escalating this determination to an appropriate delegate providing all relevent information for informed decision-making. If an event is not considered significant, you may notify the supplier that no further action is required.
- Media coverage can be useful in the initial identification of a potential event/breach but it may not be appropriate to solely rely on when determing whether it is an event/breach and assessing severity. Consider whether additional information is required.
- The supplier may provide information and context about the potential event/breach to assist in evaluating the severity. The entity may request this information from a supplier, and the response and transparency of the supplier can factor into the evaluation and remediation process.
- Consider contacting other stakeholders involved or affected by the event/breach, including other Australian Government entities who have active work orders with the supplier, to assess wider impact and gain perspective. Should you do so, be mindful of your privacy and confidentiality obligations and seek legal advice where necessary.

- Consider engaging other Australian Government entities who have active work orders with the supplier to discuss the severity.
- Evaluate the event/breach against each relevant criteria in the sliding scale of severity (refer Attachment A). Consider how the notification came to your attention; an event/breach proactively notified by a supplier may demonstrate capable monitoring and reporting procedures, while discovering an event/breach through the media may indicate a lack of transparency. Consider what existing controls are in place to manage the event/breach. Consider whether the event/breach was an isolated incident or if it may be part of a broader pattern or trend. Note that the circumstances of each event/breach is unique and should be assessed as such.

Phase 2 – Initial action

Step 3 – Determine initial course of action

Once the severity of the event/breach is determined, follow one, or a combination of the following actions and document the decision:

- **Note event/breach, watch and monitor for now, reassess if necessary**
  - If an event/breach was considered sufficiently minor that remediation was not considered necessary, the entity may choose to take no further action and monitor the situation to ensure that the event/breach does not increase in severity or frequency.
  - Alternatively, on receiving *notice* of an event/breach, there may be insufficient information to determine a course of action due to pending outcomes from examinations, inquiries, investigations or legal proceedings. If no initial action is considered appropriate, the entity may choose to monitor the situation and consider options until there is sufficient information to make an assessment.
  - Further information on monitoring is in Ongoing Phase, Step 7.
- **Issue a warning**
  - In minor instances, it may be considered appropriate to issue a warning to the supplier without taking further action. Ensure warnings outline potential consequences for any further similar events/breaches.
    - A warning will not always be a required action.
- **Request remediation plan**
  - In minor to moderate instances, a remediation plan may be requested by the contract manager. The remediation process should be proportional to the event/breach. It may be determined that delivery of goods and services can continue as usual throughout the remediation process.
  - A *notice* of an event/breach may be considered severe enough that it may be considered appropriate to restrict services or suspend business from occuring under the contract during the remediation process, in line with any

existing dispute resolution clauses. The impact to the Commonwealth should be considered when making this assessment, including potential effects on the delivery of policy objectives, service continuity, and whether alternative suppliers are available to mitigate disruption. Seek legal advice to ensure any restriction or suspension is managed appropriately. Consultation with key impacted entities may be considered appropriate prior to the suspension of a supplier.

- **Termination**
  - A breach of Code or NoSE clauses may be considered so severe that no amount of remediation will suffice and that termination is immediately warranted. If termination is to be considered, the contract manager must ensure this decision aligns with termination clauses of the relevent contract or arrangment, and all options to remediate have been considered. The decision to terminate is intended to be the final step, noting dispute resolution clauses may be available to the supplier with regards to this step.
  - When considering the option of termination, seek legal advice to ensure it is managed appropriately. Assess the impact to the Commonwealth. The contract deliverables may be something that can be picked up and resumed by another supplier, or all or a substantial proportion of the work done to date may be compromised which could impact key Commonwealth objectives, or the supplier may be the sole provider of the goods/services required.
  - Consultation with key impacted entities may be considered appropriate prior to any recommendation to terminate a supplier.
  - All decisions regarding termination should be made in accordance with the entity's Accountable Authority Instructions and any internal processes and policies.

Phase 3 - Remediation

Step 4 – Request remediation plan

- At the entity's discretion, the preferred format, content and complexity of the remediation plan can vary depending on the nature and severity of the event/breach. For minor incidents, concise email correspondence may be considered sufficient detail to constitute a remediation plan. More severe incidents may necessitate a thorough and comprehensive remediation plan that may seek changes to company policies or procedures. If requesting a remediation plan from a supplier, clearly communicate expectations of what success looks like while avoiding being unnecessarily prescriptive. The type of details requested in a remediation plan should be informed by the nature and circumstances of the incident, considering any information already provided or available.
- Consider which of the following factors are relevant when requesting a remediation plan in line with the relevant clause(s):

- how the event will be addressed in the context of the goods/services, including confirmation that the implementation of the remediation plan will not in any way impact on the delivery of the goods/services or compliance with other obligations under the contract
- how the supplier will ensure similar events do not reoccur
- any other matter reasonably requested.

- Additional information requested may include, but is not limited to:
  - the reasons the incident(s) occurred
  - the failings of current processes that led to the incident
  - disciplinary consequences of the incident
  - measures taken to minimise any further impact of the incident
  - monitoring and compliance mechanisms to identify and manage potential future events/breaches.

Step 5 – Review and assess remediation plan

- Assess the draft remediation plan. Consider whether the outlined remediation sufficiently addresses concerns regarding the severity of the incident. If the remediation plan is approved, determine whether the incident is entirely resolved or if further implementation actions are required by the supplier to embed business changes. The contract manager should ensure ongoing communication and monitoring activities support the supplier to implement changes (refer Ongoing Phase).
  - If the proposed draft remediation plan is considered insufficient in its current state, determine what adjustments would need to be made for the plan to be accepted.
  - If the proposed remediation plan can be approved incorporating some improvements then request a revised remediation plan and clearly outline what changes need to be made.
    - For the NoSE clause, suppliers must resubmit revised draft remediation plans for approval within 3 business days of the request unless a different timeframe is agreed.
- If a remediation plan fails to adequately account for the severity of an incident or if there are multiple failed attempts to agree on a sufficient remediation plan, suspension, restriction or termination may be considered appropriate actions for your entity to take.
  - When considering the option of termination, assess the impact to the Commonwealth. The contract deliverables may be something that can be resumed by another supplier, or a substantial proportion of the work done to date may be compromised which could impact key Commonwealth objectives, or the supplier may be the sole provider of the goods/services required.
- Consultation with key impact entities may be considered appropriate prior to any recommendation to terminate a supplier.

- Seek legal advice to ensure termination is appropriate and managed appropriately.
- Maintain appropriate documentation for all decisions, and the basis for those decisions.
- All decisions regarding suspension or termination should be made in accordance with the entity's Accountable Authority Instructions and any internal processes and policies.

Ongoing – Monitoring and follow-up

Step 6 – Communicate

- Communication between customers and suppliers is a key mechanism to ensure best practice is maintained and reduce the likelihood of events/breaches occurring in the first instance, or recurring following a notification.
- Communication with the supplier throughout remediation activities is critical to ensure the supplier understands the severity of the event, your entity's (and more broadly, the Commonwealth's) expectations of required actions, evidence of implementation, and future monitoring requirements.
- If the event/breach was in relation to a contract under a panel arrangement and the panel manager is not managing the process, keep the manager of the panel informed throughout the process.
- For panel managers, if a supplier was removed, restricted or suspended from a panel arrangement, communicate this update to users of the panel and provide guidance on engagements with the supplier. Consider any other stakeholders that may be worth informing, such as managers of other panel arrangements that the supplier contracts through.
- Consider your reporting obligations, including any internal protocols. For consultancy contracts above $2 million, notifications against the Code are required to be reported biannually for the Senate Order for Consulting Services.

Step 7 – Monitor

- There is an ongoing need throughout the term of any contract to monitor the ethical behaviour of suppliers, commensurate with the scale, scope and risk of the contract.
    - This requirement is especially pertinent in the aftermath of a notification of an event/breach.
- The contract manager should monitor the supplier's approach to the initial notification process, and initial actions required.
- Throughout remediation activities, the contract manager should monitor the reported outcomes of implemented actions, and ensure compliance with the agreed remediation plan. Depending on the nature and severity of the incident,

this may involve a simple acknowledgement of no further incidents to report, or it may require a more comprehensive monitoring and reporting arrangement.

- It may be appropriate to regularly check in with suppliers regarding resolved events/breaches to gain confidence in the supplier's ability to deliver contracted services, or to inform future procurement processes.
- The contract manager should consider establishing a system of continued monitoring.
    - Ensure situations being monitored are resolved or a final update is provided prior to concluding an arrangement with a supplier.
- Remain cognisant of the quantity and frequency of monitored situations and stay vigilant to identify any potential trends or patterns of concerning events or behaviour.

Step 8 – Post-remediation

- If a suspension or restrictions had been imposed under the contract as a result of an event/breach, consideration may be given to removing those limitations and returning to business as normal.
- Suspensions or restrictions may be accompanied by a timeframe or threshold to trigger evaluation to determine if it is still appropriate or necessary to continue restricting or suspending the business.
    - If a specific timeframe has been established, as the end date is approaching consider whether the supplier has demonstrated adequate remediation or evidence of compliance for the suspension or restriction to be lifted in full.
        - Should it be determined that the suspension or restriction should not be lifted in full, consider whether the suspension or restriction should be extended or removed in part.
- If a suspension or restriction is indefinite or determined by a key performance indicator or threshold, establish a schedule or reminder system to ensure reevaluation occurs.
- Following remediation, entities should consider whether ongoing engagement with the supplier is required to ensure sustained compliance. This may include updating contract key performance indicators to reflect remediation outcomes, adjusting the frequency of contract management meetings, or establishing periodic check-ins to monitor long-term behavioural change.

Attachment A – Sliding Scale of Severity

The following scale provides a high-level overview of factors that may influence the assessment of severity and potential options for remediation. It is intended as a guide only and should not be interpreted as prescriptive. Each event/breach must be evaluated in context, considering the nature of the incident, its impact, and the specific contractual arrangement.

	Minor	Moderate	Severe
Factors of severity	• Nil to minimal business impact	• Potential of substantial business impact	• Significant to severe business impact
	• Nil to minimal damage to reputation of business or Commonwealth	• Potential of some damage to reputation of business or Commonwealth	• Damage to the reputation of business or Commonwealth
	• No confidentiality concerns	• Some concerns around confidentiality practices	• Violation of confidentiality agreement
	• Any potential or actual conflicts of interest were declared and managed appropriately	• Potential or perceived conflicts of interest could have been more proactively declared but did not impact contract deliverables	• Conflict(s) of interest were mismanaged, not declared, or impacted the deliverables of the contract
	• Isolated or infrequent incidents	• Regularly occurring incidents	• Frequently or consistently occurring incidents
	• Anticipated or common occurrence in relevant industry	• Atypical in normal industry business practices	• Poor or prohibited practice in relevant industry
	• Incident identified and managed by existing processes	• Incident identified by existing processes	• Incident identified by the Commonwealth or a third party
	• Supplier was upfront, honest and prompt in notifying the contract manager	• Supplier was aware of the event/issue and failed to proactively notify the contract manager but was prompt to respond with comprehensive information when requested by the contract manager	• Supplier attempted to conceal the incident, failed to proactively notify the contract manager of the incident, and/or failed to provide information when requested.
Potential supplier remediation actions and/or consequences	Note and take no further action, or request formal correspondence from the supplier (e.g. email/letter) providing a brief description of: • how/why the incident occurred • how the incident was/will be managed by existing policies and procedures • additional information as requested, including proposed actions to avoid future recurrence, e.g. updates to internal processes / policies / procedures Communicate and monitor as required.	Request a remediation plan detailing: • the reasons the incident(s) occurred • the failings of the current processes that led to the incident • any disciplinary consequences of the incident • all measures taken to minimise the further impact of the incident • any planned changes to policies and procedures to prevent future re-occurrence The contract manager can deem the remediation plan insufficient and request further details. Communicate, monitor and follow up to ensure implementation of remediation.	Consider suspension or termination of contract. For arrangements not terminated, request a comprehensive remediation plan detailing: • the reasons the incident(s) occurred • the failing of the current processes that led to the incident • any disciplinary consequences of the incident • all measures taken to minimise the further impact of the incident • any planned changes to policies and procedures to prevent future re-occurrence • the establishment of a continued monitoring arrangement