The Committee's questions will focus on the Terms of Reference and the issues raised in submissions to the inquiry. This may include asking your views on:

1. **How existing laws are failing to protect workers from excessive surveillance:**
    a. Legislation hasn't kept pace with technology
    b. Lack of clear legislative obligation imposed on employers
    c. Failure to appropriately disclose to employees how surveillance technologies are utilised (in the workplace) and the subsequent implications i.e. biometric surveillance, privacy breaches (for employee), professional risk
    d. Transparency related to workplace surveillance is variable across employers and workplaces because it is discretionary and relies on the employer/organisations view of surveillance and technology, subsequent policies on employee rights, privacy and patient rights/privacy
    e. Surveillance not limited to employer surveillance, related to family and patients – home care represents 32% of patient care with private CCTV/concealed devices now additional to formal employer surveillance. Not covered by legislation.
    f. Because of the nature of health, the legislation does not account for the variety of intimidate care settings that exist in health and aged care. While preventing surveillance in places like toilets and bathrooms, health and aged care personal care occurs in other areas not covered/addressed in the legislation
    g. There is currently no legislative requirement for an employer to obtain consent for the collection or utilisation of personal information, nor do they impose any notification requirements on employers. The employers are afforded considerable power and digression to monitor employees in Victoria and employees are often ignorant to the extent of the surveillance.

2. **Examples of workplace surveillance leading to function creep and work intensification and the impact of this on workers.**

    Function Creep:

    a. Nurses and midwives working in the community providing in home care are being tracked and questioned about their travel activities and timed in relation to trips and the time paten for the care provided to clients/patients and time between patients/clients. This is then utilised as productivity and performance measure.
    b. ANMF see workers forgoing breaks, extending their work and driving time risking their health and safety and increasing the psychological stress they are experiencing.
    c. Members are undertaking administrative and other work in their vehicles risking further OHS issues and workload stress. The impact of this stress is an

increased risk taking on the road while travelling between client/patient work sites.

d. Further we are witnessing members who are then subject to disciplinaries based on misinterpreted data that is misappropriated for punitive means.

Impact of workplace surveillance on members:

a. Employer surveillance of N&M is widespread and includes recorded video surveillance, computer key stroke monitoring, telephone monitoring, email and finger, have and facial recognition scanning.
b. CCTV/Video is often relied upon for disciplinaries and workplace incident investigation and may lead to mandatory reports to the health practitioner regulator without context. This can lead to lengthy investigations and inappropriate restrictions to the practitioner's registration and employment. The employer relies upon CCTV footage, however the employee is denied the ability to review the footage and provide context and explanation. The employer or an external private entity is often in control of the footage and so the nurse/midwife or carer has no rights to how that is used, stored or destroyed.

3. **Issues associated with the use of body-worn cameras (BWC) and the safeguards required to ensure that data obtained from these cameras is not used for purposes beyond safety.**

Most security staff at health and aged care facilities in Victoria are private contractors and many wear BWCs following the public sector OVA initiative to disincentivise violence against health workers

The Surveillance Devices Act (including its coverage of BWC) does not contemplate the footage captured within the healthcare setting, nor does it incorporate nurses, midwives or personal care workers in the 2021 amendment re: protected information obtained by body worn cameras. This means that they have no safeguards relating to their actions captured in the footage that may be included as evidence in a case and considered protected information.

ANMF is requesting that nurses, midwives and personal care workers are included within the surveillance devices act and protected from prosecution where private activities are inadvertently captured on BWCs used in the course of ordinary duties.

The template for BWC policy in the Department of Health, has not been updated since 2018 and would most likely not be fit for purpose for current practices in Victoria Health and Aged Care sector.

4. **The impacts of workplace surveillance by people other than employers (e.g. students or patients) and how the Victorian Government should deal with this type of surveillance.**

ANMF has numerous examples of patients/families/clients etc taking phone recordings of members within hospitals, homes, secure settings.

This results in surveillance being used by patients, visitors or family members to record interactions with staff during care provision, which causes significant psychological distress to the healthcare workers involved. Most care providers (acute, aged care and

community) have limited or no policies in place to manage or prevent healthcare workers being recorded by patients or their family members. Furthermore, healthcare workers are not educated on what action they can take to protect themselves or intervene in such a situation. ANMF (Vic Branch) members have been the subject of online harassment and scrutiny, after being filmed, photographed or identified on social media by patients and their families. Often with limited support from their employers, healthcare workers are left despondent and have little recourse to enable the removal of their personal information or image from social media or from the general public domain.

Example of footage of a patient being placed in the public domain associated with Code Grey without to patient's consent because footage is owned by outside organisations (security companies)

ANMF (Vic branch) member contacted seeking representation following receipt of formal disciplinary proceedings from her public health employer. The disciplinary allegations were in relation to misconduct and performance concerns. The member was a registered nurse and was working as the Nurse in Charge at a major metropolitan public health service.

The allegations related to the management of a patient on the acute medical ward. The patient was a 65-year-old male with a complex medical history admitted for management of acute behavioural deterioration and aggression secondary to dementia and delirium.

In summary:

1. Multiple Code Greys (behavioural aggression response) activated, on the related occasion two security guards attended wearing Body Worn cameras (BWC).

6. Our member undertook a preliminary clinical assessment, underpinned by her knowledge of the situation and patient vulnerabilities, and her obligations associated with the DMF.

7. Due to the multitude of risks including the significant patient agitation and ongoing threats of aggression to both patients and staff, the nurse advised staff to delay approaching the patient again, until the imminent arrival of the doctor to assess the patient and determine the safest care option.

8. The resultant disciplinary actions were based off excerpts of the audio-visual footage captured by the BWC. This did not protect the privacy of the patient or consider the risk to others. The excerpts from the footage were transcribed as evidence without the aforementioned context, and the footage was not provided to the nurse in the first instance.

9. This scenario demonstrates the risk of unregulated surveillance ANMF members are exposed to, in addition to the lack of privacy protections and patient dignity. The footage obtained by the BWC was captured by the security personal, who are contracted by external providers and are not employed by the health service. As such the footage is not privy to the health service privacy and process.

5. **Measures the Victorian Government should implement to protect workers' biometric data**.

    a. Improved employer obligations to consult with workers, their union representatives including in relation to proposed implementation of changes to policy and procedure.

    b. The introduction of an independent regulator of workplace surveillance.

    c. Department of Health to develop and make available consistent workplace surveillance and data privacy policies for Victorian public health services to ensure all employees are aware of their rights and responsibilities and can easily access this information.

6. **Why it is important for workers to have the right to access data collected about them through surveillance.**

    a. Improved employer obligations to consult with workers, their union representatives including in relation to proposed implementation of changes to policy and procedure.

    b. Strengthening worker protections in relation to the use of surveillance footage, preventing its routine use for individual disciplinary procedures.

    c. In relation to BWC, extend protections to surrounding employees who may be involved or implicated in relation to a workplace patient interaction.

    d. The introduction of an independent regulator of workplace surveillance. 5. Given the nature of audiovisual footage and the interactions recorded by workplace surveillance and body-worn cameras in healthcare settings, health services should anticipate the collection of health and personal information. Mandating employers undertake Privacy Impact Assessment to identify and mitigate any associated privacy risks. Where private companies own the audiovisual information that the requirements for storage and disposal of the footage are publicly available for employees of the health service and there are legislative obligations for the private entity to also consider the rights of the health service employees.

    e. Department of Health to develop and make available consistent workplace surveillance and data privacy policies for Victorian public health services to ensure all employees are aware of their rights and responsibilities and can easily access this information.

7. **The risks to workers when employers use workplace surveillance data to train AI models and any protections that should be put in place to protect workers.**

    a. The nature of the surveillance within the healthcare context is not only a risk to RN's, RM's and carers but also poses significant risk to the public.

    b. In late October 2024, the Office of the Australian Information Commissioner published *Guidance on privacy and developing and training generative AI Models*.

c. The 5 key takeaway points (inserted for context):

1.1.1. ***March 2025**, commensurate with the likely increased level of risk in an AI context, including through using high quality datasets and undertaking appropriate testing. The use of disclaimers to signal where AI models may require careful consideration and additional safeguards for certain high privacy risk uses may be appropriate.*

1.1.2. ***Just because data is publicly available or otherwise accessible does not mean it can legally be used to train or fine-tune generative AI models or systems**. Developers must consider whether data they intend to use or collect (including publicly available data) contains personal information and comply with their privacy obligations. Developers may need to take additional steps (e.g. deleting information) to ensure they are complying with their privacy obligations.*

1.1.3. ***Developers must take particular care with sensitive information, which generally requires consent to be collected.** Many photographs or recordings of individuals (including artificially generated ones) contain sensitive information and therefore may not be able to be scraped from the web or collected from a third-party dataset without establishing consent.*

1.1.4. ***Where developers are seeking to use personal information that they already hold for the purpose of training an AI model, and this was not a primary purpose of collection, they need to carefully consider their privacy obligations.** If they do not have consent for a secondary, AI-related purpose, they must be able to establish that this secondary use would be reasonably expected by the individual, taking particular account of their expectations at the time of collection, and that it is related (or directly related, for sensitive information) to the primary purpose or purposes (or another exception applies).*

1.1.5. ***Where a developer cannot clearly establish that a secondary use for an AI-related purpose was within reasonable expectations and related to a primary purpose, to avoid regulatory risk they should seek consent for that use and/or offer individuals a meaningful and informed ability to opt-out of such a use[1].***

d. Surveillance data captured within the healthcare and clinical setting does not necessarily consider the human context of health care and aged care and cognitive and clinical assessment and decision making. As detailed by the OAIC guidelines, the AI models are based on a theory of probability and do not comprehend the data processed or generated. In the healthcare and clinical setting, this is inherent with risks including
   - "data-driven nature of AI technologies, rely on large datasets including personal information, create new specific privacy risks, amplify existing risks and lead to serious harms"
   - Loss of control over personal and sensitive information
   - Bias/discrimination- data containing inherent bias (gender, race, age diagnosis) may be replicated and generate subsequent output containing these inferences leading to misinformation, reputational harm, unfair or inaccurate decisions.
   - Re-identification of personal information/ risk of disclosure of personal information re data breach

[1] Guidance on privacy and developing and training generative AI models | OAIC

- "**The impacts of generative AI may be particularly acute for children and people experiencing vulnerability.** For example, there are well-publicised examples of discrimination against individuals as a result of algorithmic bias in AI systems. Vulnerable groups, including First Nations people, will often not be properly represented in datasets which reflect historical biases or do not include sufficient data" [2]

e. The use of workplace surveillance obtained within the healthcare and clinical setting is of critical concern to ANMF members and the broader community when receiving healthcare. It would require significant safeguards, with specific and tailored rigorous processes and procedures to protect the misuse and dissemination of sensitive information.

8. Whether and why workplace surveillance should be considered a psychosocial hazard for work health and safety purposes.

There are significant impacts of workplace surveillance on nurses, midwives and personal carers, primarily on their psychological safety. These can be both positive and negative, depending upon the consultation, implementation and use of such surveillance.

a. one of the purposes for workplace surveillance is as a deterrent for occupational violence and aggression. Providing clear notification that a person's acts are being recorded appears to lessen the likelihood of escalation of a situation in many circumstances. When this is the purpose of surveillance, and the workers are advised of such, involved in the implementation and there is evidence of the surveillance being used for such purposes, this supports the psychological sense of safety that workers feel.

However, when such surveillance is implemented unilaterally by employers and without appropriate consultation with affected employees, ANMF (Vic Branch) members report that they feel apprehensive about the use of surveillance and whether it is intended to control rather than protect employees.

b. Additionally, where an unfortunate incident of occupational violence does occur, and the footage is used in a positive incident investigation (i.e. where the incident is looked at, and clear, proactive mechanisms are implemented to prevent future occurrences), this can be psychologically protective of the worker who has been involved.

This is contrary to where the footage is used only to identify potential mistakes the worker may have made, or in a culture of blame.

Where surveillance is used primarily as a tool for identifying disciplinary issues, staff become distrustful of workplace surveillance. This results in a lack of trust between workers and their employer leads to decreased employee performance, poor staff retention and increases in workplace psychological

[2] Guidance on privacy and developing and training generative AI models | OAIC

hazards and psychological injuries sustained by employees in the healthcare industry.

c. Surveillance is also used by patients, visitors or family members to record interactions with staff during care provision, which causes significant psychological distress to the healthcare workers involved.

   Healthcare workers are not educated on what action they can take to protect themselves or intervene in such a situation. ANMF (Vic Branch) members have been the subject of online harassment and scrutiny, after being filmed, photographed or identified on social media by patients and their families. Often with limited support from their employers, healthcare workers are left despondent and have little recourse to enable the removal of their personal information or image from social media or from the general public domain.

Overt workplace surveillance can provide employees with a sense of assurance and safety. However, the circumstances where family feel compelled to install audiovisual recording devices demonstrates the broader and critical issues experienced by ANMF members and the community within aged care.

Below are two case studies which demonstrate both the positive impacts regarding a sense of security and conversely, when surveillance is installed covertly, the negative impact of workers and resulting potential for resulting compromise to care delivery. In both instances, the lack of clear obligations and policies were apparent,

9. Case Study 1 –

   - *contacted by a member who has concerns about a resident's family member who installed CCTV in a resident's room.*
   - *The family member installed it without staff knowledge and staff were unknowingly recorded for 2 days before the facility was informed. The surveillance continues without staff agreement and therefore staff are now refusing to provide care for this resident because they are uncertain about the ramifications of the family member watching care delivery and potentially misinterpreting interactions with the resident.*
   - *The facility/employer does not appear to be taking staff's concerns seriously and is allowing the family member to continue using the devices without suitable policy or process to provide protection for staff and education to the family.*

10. Case Study 2 -

   - *This matter relates to residential aged care, and to a resident and her daughter, the resident is 96 and has significant and advanced dementia. The daughter is targeting anyone providing care to her mother 24/7. The resident requires assistant every 30 mins day and night and often 1:1 overnight due to her unpredictable*

behaviours. We now have an additional staff menders employed to help. There is a camera in the room, installed by the daughter, the staff are supportive of the cameras, not because they feel threatened, they view the surveillance as a way to objectively demonstrate the mother's behaviours and increase safety.

11. Your members' experience of the effectiveness of workplace surveillance laws in NSW and the ACT and any suggestions for improvement.

The Workplace Surveillance Act 2005 (NSW)
https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2005-047#pt.4
relevant excerpts below

PART 2 - NOTIFICATION OF WORKPLACE SURVEILLANCE OF EMPLOYEES

Note

9 Application of Part
10 Notice of surveillance required[3]

(1) Surveillance of an employee must not commence without prior notice in writing to the employee.

Note--: Subsection (6) provides for an exception to the notice requirement.

(2) The notice must be given at least 14 days before the surveillance commences. An employee may agree to a lesser period of notice.

(3) If surveillance of employees at work for an employer has already commenced when an employee is first employed, or is due to commence less than 14 days after an employee is first employed, the notice to that employee must be given before the employee starts work.

(4) The notice must indicate--

(a) the kind of surveillance to be carried out (camera, computer or tracking), and

(b) how the surveillance will be carried out, and

(c) when the surveillance will start, and
(d) whether the surveillance will be continuous or intermittent, and

(e) whether the surveillance will be for a specified limited period or ongoing.

(5) Notice by email constitutes notice in writing for the purposes of this section.

(6) Notice to an employee is not required under this section in the case of camera surveillance at a workplace of the employer that is not a usual workplace of the employee.

11 Additional requirements for camera surveillance
12 Additional requirements for computer surveillance
13 Additional requirements for tracking surveillance

[3] WORKPLACE SURVEILLANCE ACT 2005 - SECT 10 Notice of surveillance required

14 Exemption for certain surveillance by agreement

PART 3 - PROHIBITED SURVEILLANCE

15 Surveillance of change rooms and bathrooms prohibited
16 Prohibition on surveillance using work surveillance device while employee not at work
17 Restrictions on blocking emails or Internet access
18 Restrictions on use and disclosure of surveillance records--notified surveillance

PART 4 - COVERT SURVEILLANCE OF EMPLOYEES AT WORK

DIVISION 1 - RESTRICTIONS ON COVERT SURVEILLANCE

19 Covert surveillance prohibited without covert surveillance authority
An employer must not carry out, or cause to be carried out, covert surveillance of an employee while the employee is at work for the employer unless the surveillance is authorised by a covert surveillance authority.

20 What covert surveillance authority authorises
21 Exceptions--law enforcement, correctional centres, courts, casino
22 Defence--surveillance for security of the workplace

12. The measures that could be put in place to minimise unfair dismissals and performance management based on surveillance data.

a. Improved employer obligations to consult with workers, their union representatives including in relation to proposed implementation of changes to policy and procedure.
b. Strengthening worker protections in relation to the use of surveillance footage, preventing its routine use for individual disciplinary procedures.
c. In relation to BWC, extend protections prescribed by the Surveillance Devices Act (Vic) to recognise Nurses, Midwives and Carers who may be involved or implicated when performing ordinary duties within the healthcare and clinical context.
d. The introduction of an independent regulator of workplace surveillance.
e. Department of Health to develop and make available consistent workplace surveillance and data privacy policies for Victorian public health services to ensure all employees are aware of their rights and responsibilities and can easily access this information.

13. The pros and cons of regulating workplace surveillance and data protection through enterprise bargaining agreements and awards, or through dedicated laws.

a. Consistent with points above; and,
b. Incorporating workplace surveillance regulation and data protections within an EBA would assist in maintaining currency and contemporary protections for staff could be updated in negotiations, however, this requires underpinning legislation to ensure consistency and would concurrently raise the profile of the legislation and remove the risk of employers attempting to wind back protections.

c. While the regulatory framework provides the underpinning legislation, embedding the regulation in the EBA will in turn provide additional safeguards to reflect the nature of the specific work and workplace considerations associated with health and aged care.

ANMF (Vic Branch) acknowledges the importance of workplace surveillance in context for the protection of both health and aged care workers and the people and communities to whom they provide care. However, ANMF also posits that improving legislation and embedding a consistent approach to implementation, there will be better protections for health and aged care workers that will also positively affect patient care and patient privacy, as a direct result of the associated educational and structural improvements that will raise community awareness and health and aged care worker understanding of their rights and the rights of consumers. ANMF therefore recommends that Victorian workplace surveillance legislation considers:

1. **Improved employer obligations underpinned by robust legislation ensuring employers consult with workers, their union representatives including in relation to proposed implementation of changes to policy and procedure.**
   Strengthening worker protections through legislation, in relation to health and aged care consumers and their families surveilling health professionals while they deliver healthcare and perform " required duties". Further, obliging employers to embed positive reinforcement of those protections, for instance in HITH as part of the Home pre risk assessment policy and procedure and service orientation education of client and their families.
2. **Strengthening worker protections in relation to the use of surveillance footage, preventing the use of footage captured by workplace surveillance, being used out of clinical context risking delayed care** for instance, disciplinary procedures and increasing privacy protections for health consumers and workers alike
3. **In relation to workplace surveillance inclusive of BWC,** extend protections prescribed by the Surveillance Devices Act (Vic) to recognise Nurses, Midwives and Carers who may be involved or implicated when performing ordinary duties within the healthcare and where clinical context is not adequately considered.
4. The introduction of an independent regulator of workplace surveillance.
5. Given the nature of audiovisual footage and the interactions recorded by workplace surveillance and body-worn cameras in healthcare settings, health services should anticipate the collection of health and personal information. **Mandating employers undertake Privacy Impact Assessment to identify and mitigate any associated privacy risks**. Where private companies own the audiovisual information that the requirements for storage and disposal of the footage are publicly available for employees of the health service and there are legislative obligations for the private entity to also consider the rights of the health service employees.
6. Department of Health to develop and make available consistent workplace surveillance and data privacy policies for Victorian health services to ensure all employees are aware of their rights and responsibilities and can easily access this information.