

Implementing Gene Synthesis Screening in Australia

October 2026

AI is making it easier to create a biological weapon. AI systems can now [provide expert-level guidance](#) relevant to biological weapons development, and [generate genomes of viruses](#) (bacteriophages) not previously seen in nature. We cannot rely on safeguards placed on AI models. Most biological AI tools—[over 95%](#)—have no safeguards at all, and where they do exist, [jailbreaks are common](#). Rapidly advancing open-weight models with easily removable safeguards will further increase risks and undercut developer-side mitigations.

Gene synthesis screening is a key mitigation against the misuse of biotechnology to create pathogens. A bad actor with AI guidance still needs physical genetic materials, like synthetic nucleic acids, to act. Gene synthesis screening involves providers checking orders for dangerous sequences and verifying customers before shipping. Most synthetic nucleic acids used in Australia are imported, making import conditions a practical way to implement screening. Under the *Biosecurity Act 2015*, the Director of Biosecurity has the power to impose screening conditions on all such imports immediately and without new legislation.

In September 2026, California became the [first jurisdiction in the world to mandate gene synthesis screening](#). Australian experts have already [called on the Australian Government](#) to do the same.

This report details how Australia could follow California's lead by mandating gene synthesis screening. The proposal draws on the [US Framework for Nucleic Acid Synthesis Screening](#)—which California mandates—and international standards and guidance from organisations such as International Biosecurity and Biosafety Initiative for Science (IBBIS) and the International Gene Synthesis Consortium (IGSC).

Acting now would reinforce Australia's role as a world leader in biosecurity.

We recommend Government:

- **Publish an Australian Framework for Gene Synthesis Screening.** This would be provider-facing and set out requirements providers must meet, including sequence screening, customer verification, and record keeping. This framework could be modelled on the US Framework for Nucleic Acid Synthesis Screening.
- **Impose an import condition on synthetic nucleic acids,** requiring providers to declare they have screened orders in line with Australia's Framework for Gene Synthesis Screening. This uses existing powers under the *Biosecurity Act 2015* and requires no new legislation.

Proposed details for Australia's Framework for Gene Synthesis Screening

Australia's Framework for Gene Synthesis Screening should cover:

1. Screening orders to identify sequences of concern
2. Verifying customer identity, legitimacy, and use
3. Refusing and reporting unresolved flagged orders
4. Retaining records relating to purchase and screening
5. Ensuring cybersecurity and information security

1. Screening orders to identify sequences of concern

The framework should outline how providers are expected to screen orders for sequences of concern (SoCs). This should include a clear, adaptable definition of SoCs,¹ and what providers must screen for.

Providers should screen for sequences from pathogens and toxins on recognised control lists, like the Australia Group Common Control Lists and other national export-control lists. Similar to the US framework, providers should also “make efforts to implement a mechanism to screen additional SoCs known to contribute to pathogenicity or toxicity, even when not derived from or encoding regulated biological agents”. Screening should detect when scattered mutations mean a sequence is not an exact match but likely functions similarly.

Government should compile a SoC database that providers screen against, updated over time as new SoCs are identified. The database allows for consistent screening across providers, and provides a place to add newly identified sequences. The database should include:

- Sequences from pathogens and toxins on recognised control lists (e.g., the Australia Group Common Control Lists and other national export-control lists);
- Additional sequences known to contribute to pathogenicity or toxicity, even where not from a listed agent;
- Sequences from curated databases maintained by expert organisations.

To prevent misuse, the database should have appropriate cybersecurity and access controls.

Government should partner with expert organisations to compile and maintain the database. Independent organisations like [IBBIS](#) develop and maintain SoC databases, produce free screening tools, and contribute to international screening standards. Government should consult with such organisations, alongside the Australian Centre for Disease Control, to determine how Australia operationalises SoCs.

A compiled, government-maintained database is recommended by independent organisations such as [Americans for Responsible Innovation](#) and the UK’s [Centre for Long-Term Resilience](#), and is required by a [US federal bill](#). It would take Australia beyond the US framework that California has adopted, which leaves providers and manufacturers to develop or source their own SoC database.

A database creates a common baseline for screening, but may not capture every SoC. Providers should therefore also make efforts to screen for SoCs the database does not yet contain, including variants or novel sequences.

The framework should also:

- Set a minimum sequence length for screening. The US framework requires screening sequences of 50 nucleotides or more.
- Account for split orders. Providers should detect where shorter sequences could be assembled into a SoC, whether ordered from the same provider in a single batch or across multiple orders over time. These should be flagged just as a direct SoC order would be. Over time, Australia should also work toward cross-provider screening to detect SoC orders deliberately split across providers.²
- Outline what screening methods providers can use. The US framework lets providers determine which tools or software systems to use. Providers should evaluate the effectiveness of their screening, and improve their methods over time.

¹ The US framework sets out three criteria for designating a SoC: evidence it contributes to pathogenicity or toxicity in humans and animals; how widely its function is known (and so how likely it is to be recognised as a candidate for misuse); and how easily it could be misused.

² The proposed United States *Biosecurity Modernization and Innovation Act* includes a “privacy-preserving ... mechanism” to “facilitat[e] effective split order detection across covered providers”.

2. Verifying customer identity, legitimacy, and use

The framework should specify that providers verify customer identity for all orders (such as name, institution, address, contact information). For orders containing SoCs, providers should also verify customer legitimacy and 'legitimate use'.³ These checks help establish whether SoCs are being ordered for legitimate research or to cause harm.

Verifying customer legitimacy means confirming the legitimacy of the individual placing the order and their institution.

- Individual legitimacy can be supported by checking a customer's research history (e.g., ORCID profile or publications), project documentation (e.g., grant documentation), or relevant government-issued approvals (e.g., a relevant Gene Technology Regulator licence or registration under the Security Sensitive Biological Agents scheme).
- Institutional legitimacy can be checked in several ways, including verifying the institution is an established legal entity, has a life sciences mission, provides biosafety oversight, or holds relevant regulatory approvals.

Verifying legitimate use means confirming the customer has a legitimate use for the SoC ordered. This could include a written description of the intended use, or institutional approval from someone responsible for overseeing biorisk (e.g., a biosafety officer or biorisk manager).

Providers should also ascertain whether customers are the end users of the SoC, or whether the order will be passed along to a third party. If customers pass the order to a third party, providers should also assess the legitimacy of that third party.

3. Refusing and reporting unresolved flagged orders

The framework should specify that providers refuse orders with unresolved concerns, and report the customer to the relevant authorities. Reporting matters because the *prospect* of being reported can deter bad actors from trying to order SoCs in the first place. Reporting also alerts authorities to potential threats they can investigate.

Under the US framework, reports go to an FBI field office or, where a customer may be violating export control laws, the Department of Commerce's Bureau of Industry and Security.

Government should specify how reports should be made in Australia. This could sit with the Department of Agriculture, Fisheries and Forestry or the Australian Federal Police.

4. Retaining records relating to purchase and screening

The framework should specify that providers retain records of orders and screening results so authorities can trace and investigate a concerning transaction later.

The US framework requires retaining records for three years, while the IGSC Harmonized Screening Protocol recommends eight to align with the statute of limitations for weapons offences.

We recommend, at minimum, retaining records for five years. This aligns with the five-year retention period required of importers under the *Customs Act 1901*.

³ IBBIS has outlined [emerging customer screening standards](#) that these recommendations draw on.

5. Ensuring cybersecurity and information security

A SoC database that compiles sequences from unregulated agents poses an information hazard if it can be accessed and used by bad actors. Government, and any provider holding a copy of the database, should implement cybersecurity and access controls to protect that information.

The framework could also specify that providers report any suspected cyber attack to the relevant authority and protect their customers' identities and proprietary information.

Treatment of benchtop DNA synthesisers in the framework

The framework should cover benchtop DNA synthesisers, which let users synthesise nucleic acids themselves rather than ordering them from a provider. Benchtop DNA synthesisers are a growing part of the synthesis landscape and carry particular risks. Users who can synthesise their own sequences can bypass provider screening and are subject to less oversight than commercial orders.

Australia's framework should set clear expectations for benchtop DNA synthesisers, drawing from the US framework:

- Manufacturers should integrate SoC screening into the devices so users cannot synthesise sequences without those sequences being screened.
- Screening should be on par with what is required of providers in the framework, including screening against SoC databases that are updated as new sequences are identified. This screening should be verifiable.
- Manufacturers should verify the legitimacy of customers buying the devices, and track legitimate use across the device's lifecycle, including when it is transferred to a new user.
- The devices should flag SoCs in real time and detect attempts to tamper with screening or the equipment.

These expectations could not be enforced through an import condition under the *Biosecurity Act 2015*, given benchtop DNA synthesisers are laboratory devices that do not themselves carry a disease or pest risk. In the immediate term, Government could:

- Amend the *Customs (Prohibited Imports) Regulations 1956* so that benchtop DNA synthesisers without inbuilt screening cannot be imported. This is a promising near-term intervention, given there are currently no manufacturers of benchtop DNA synthesisers in Australia.
- Use the Gene Technology Regulator's certification conditions under the *Gene Technology Act 2000* so that certified labs can only use benchtop DNA synthesisers with inbuilt screening.

In the longer term, if these devices are made in Australia, legislative amendments might be required. One option is amending the *National Health Security Act 2007*, which is intended to "establish controls for the security of certain biological agents that could be used as weapons". The Act could be expanded to cover manufacturers and suppliers of equipment capable of synthesising dangerous biological agents, like benchtop DNA synthesisers. This would involve adding a new regulated category alongside the existing agent-handling regime.

Reviewing and updating the framework

The framework should be reviewed and updated regularly. Similar to the US framework, we recommend a comprehensive assessment every two years, alongside a standing mechanism to update screening details between those cycles. This could include updating the SoC database, minimum sequence lengths for screening, and assessment methods.

Updates should be informed by new evidence on pathogenicity, better methods to identify functional equivalents, predictive modelling for novel sequences, and changes in the threat landscape.

Over time, Australia's approach should move from provider self-attestation toward rigorous compliance assessments. This could be done through a "whitelist" process, where Government authorises providers after assessing their compliance with the framework, similar to the [AusTreat scheme](#). Alternatively, it could be done through independent auditing, where providers are certified against the framework by an accredited third party.

Roles and responsibilities

Government should determine who owns and maintains the framework and SoC database. This could be the Department of Health, which already maintains the List of Security Sensitive Biological Agents and regulates who may handle them. The Department of Health should collaborate with the Department of Agriculture, Fisheries and Forestry and the Australian Centre for Disease Control.

A broader group should be involved in reviewing and updating the framework. One option is for this to sit with the existing Multiagency Group on Synthetic Biology and AI. Participants should include:

- The Department of Home Affairs, as the lead on AI-enabled biological risk;
- The Department of Agriculture, Fisheries and Forestry, which administers import permit conditions under the *Biosecurity Act 2015*;
- The Australian Centre for Disease Control, for pathogen and surveillance expertise;
- The Australian AI Safety Institute, for insights into how AI is impacting biosecurity risks;
- The National Intelligence Community, for proliferation and threat considerations;
- Other experts, including from organisations such as IBBIS that specialise in screening tools and databases.

What other jurisdictions are doing

This report draws from the US Framework for Nucleic Acid Synthesis Screening. Similar measures have been proposed at the US federal level, and in the European Union, New Zealand, and United Kingdom—all covering sequence screening, customer verification, and safeguards for benchtop synthesisers.⁴

	Instrument	Status	Who it applies to
California	AB 1864	Enacted	Providers and benchtop manufacturers selling into California
United States	Biosecurity Modernization and Innovation Act (S.3741)	Proposed	Providers and benchtop manufacturers selling to US persons
European Union	EU Biotech Act	Proposed	Providers and benchtop manufacturers placing products on the EU market
New Zealand	Gene Technology Bill	Proposed	Domestic (NZ-based) providers and benchtop manufacturers
United Kingdom	DSIT Screening Guidance on Synthetic Nucleic Acids	Published guidance	UK providers and users

Biosecurity risks from AI are not currently catastrophic, but will escalate quickly. Australia must act now to stay ahead.

⁴Jurisdictions differ on whether they require a government-maintained SoC database. The US federal bill requires one, while California's law and the UK guidance do not. The EU Biotech Act would define SoC categories in legislation but not mandate a central database. Australia doing so would set a new standard.