Australian Government

Inspector-General of Biosecurity

Review Work Plan

Use of technology for biosecurity risk management

Contents

1. Background

Technology is now embedded in routine biosecurity work at airports, seaports, mail centres and associated compliance and laboratory functions. Alongside major digital programs, officers increasingly rely on everyday digital tools to capture information, verify documentation, support referrals and record decisions in real time. The operational value of these tools depends not only on capability, but also on reliability, connectivity, usability, training and how well workflows and record-keeping expectations align with what happens on the ground.

Technology-enabled interventions include day-to-day use of mobile devices (for example, iPhones used by officers at airports for scanning and capturing information) and trials of new passenger-facing digital processes (for example, electronic passenger declaration initiatives). These routine use cases matter because they shape data quality, timeliness of decision records and how consistently officers can apply risk-based processes under real operating pressures.

Operational cases of technological use for biosecurity operations (illustrative examples)

- **Frontline workflow tools (day-to-day):** Technologies and workflows that support frontline capture, verification, referrals, record-keeping and escalation, including traveller and mail operations enabled through the Traveller and Mail System (TAMS).
- **Screening, targeting and decision support:** Enhanced screening/imaging and algorithm-supported triage, including 3D X-ray for passenger baggage pre-screening and in mail centres, and 3D algorithms to automatically detect biosecurity risks (including meat, fruit, vegetables and seafood). Technology that supports cargo surveillance and operational decisioning includes the Biosecurity Automated Threat Detection System (BATDS) for container surveillance, as well as ongoing work on analytics-enabled risk targeting, workflow tools to support officers, and phased replacement of legacy components.
- **Digital trade and client interfaces:** Digital trade and certification processes through eCert/ePhyto for Full Import Declarations and Long Form Self-Assessed Clearance lodgements for selected grain and horticulture pathways (including trade from the USA and Korea). Client-facing visibility and interaction tools include the Biosecurity Cargo Status Tracker (BCST) to provide customs brokers and self-reporting importers with on-demand visibility of referred entries.
- **Surveillance, diagnostics and science-enabled decisioning:** Operational and scientific applications of analytics and diagnostics, including MALDI-TOF mass spectrometry and MinION to accelerate diagnostics and surveillance, eDNA/genomics analytics, and smart trapping and AI imaging approaches for fruit fly surveillance (including collaborations with research and industry partners).
- **Emerging and pilot technologies:** Proof-of-concept and pilot initiatives intended to strengthen pathway processing, including low-energy X-ray (to improve detection of smaller seeds in mail), the Hades-5Z inspection robot fitted with thermal and high-definition cameras (to support underbody inspection of vehicles and machinery for biosecurity risk material) and RingIR (for real-time vapour detection of fumigants such as methyl bromide, sulfuryl fluoride and phosphine).

Technology changes can alter roles, escalation pathways, decision evidence and how industry and partner agencies interact with the department. As operational reliance increases, weaknesses in use-design, data, configuration, monitoring or assurance arrangements can have greater consequences—making reliability, supportability and benefits realisation critical considerations.

2. Rationale

Australia's biosecurity increasingly depends on well integrated policy, operations, data and the capability of digital systems to manage risk in a complex and dynamic environment. The National Biosecurity Strategy (2022–32), its 2024 Action Plan and the Biosecurity 2030 Roadmap all point to stronger end-to-end integration, enabled by technology, research and better use of data. In that context, the review will consider whether the department's technology posture and use is genuinely enabling integrated operations or whether issues such as fragmented systems, inconsistent data capture and quality, unclear accountabilities, variable support arrangements or uneven capability across regional centres are undermining delivery.

An independent assessment is particularly important as operational reliance on technology increases and tools mature from "pilot" to "business as usual". Technologies such as imaging, algorithm-supported detection and paperless certification exchange have the potential to lift detection performance, reduce processing times and support more consistent decision-making. However, how they are used and how officers are supported to use them, as well as potential over-reliance on them can lead to increased risk. A review can also consider potential new technologies and the way that they could be effectively utilised to improve risk management within the biosecurity system. It is important that the department understands the problems that are to be solved by technology and the interface with the people who use it, rather than focusing on technological solutions that are "looking for problems."

3. Review purpose

To provide independent assurance on how effectively the department is using technologies across biosecurity operations to manage risk and deliver intended outcomes.

4. Review objectives

The objectives of this review are to:

- assess whether technology-enabled changes translate into consistent practice, measurable improvements and confidence in risk-based decision-making supported by appropriate governance, data quality controls and performance monitoring
- identify where new technologies could be used effectively to strengthen the system.

Line of inquiry

The review will seek answers to the following key evaluation questions:

1. Are adopted technologies helping officers make right decisions quickly?
2. Before officers rely on system outputs (for example, a flag, an alert, a scan result), what assurance exists that the system is usually correct and stays correct over time?
3. Do systems and processes capture the right records (what happened and why) without staff needing workarounds?
4. Is the technology actually improving results (for example, finding more risks, clearing work faster, improving compliance)?
5. Are governance and accountability clear for design changes, configuration, support and sustainment?
6. Do staff and users have what they need to use the technology properly (that is, training, guidance and support)?
7. Do connected systems (for example, Integrated Cargo System) fit well with the departmental processes or do they create gaps and confusion?
8. What important problems (or biosecurity issues) could technology help solve next, and what is the department doing (or what does it need to do) to achieve that?

5. Review scope

The scope of this review includes assessing the following:

- *Technology portfolio across operations:* Current tools and capabilities in use to minimise biosecurity risks and improve operational delivery (for example, digital lodgement, advanced diagnostics, AI assisted screening and decision-making).
- *Risk alignment and outcomes:* Where technology is risk-based and demonstrably improves detection, targeting, clearance times and compliance outcomes; gaps and improvement opportunities.
- *Governance and accountability:* Roles, decision rights and assurance mechanisms for technology adoption and change (including oversight of reforms).

- *Adoption and capability:* Staff and industry readiness, training and support (including local support models, usability and connectivity constraints, and contingency/fallback arrangements); consistency of use across operations.
- *Performance and benefits realisation:* Metrics, monitoring and evaluation frameworks that evidence intended outcomes and inform investment decisions.
- *Partner and industry leverage:* How the department identifies, assesses and adopts relevant approaches used by industry, government and research partners, including interoperability, data sharing arrangements and assurance.

In summary, the review would test whether the technology is solving the *right* problems—that is, whether investment is being driven by clearly evidenced operational constraints and priority biosecurity risks rather than primarily by platform refresh cycles, isolated ideas or the availability of new features. Furthermore, the review would also examine how effectively technology is being operationalised in practice, including whether frontline officers and industry users are supported through fit-for-purpose guidance, training, change management, sustainment and practical troubleshooting.

In addition to assessing how current technologies are performing, the review will take a forward-looking view of where technology could make the biggest difference over the years. This will focus on practical operational problems that are ongoing, such as reducing manual re-entry and double handling, improving end-to-end visibility across pathways, strengthening risk targeting and prioritisation, improving frontline connectivity and offline capability and making decision records easier to capture in real time.

Criteria for selection of case studies

Given the breadth of technologies across operations, the review will adopt a case study approach, selecting a small number of representative operational settings and technologies (including both mature and recently introduced tools) to test governance, assurance, operational use, support arrangements and outcomes in practice. Case study selection approach will use the following criteria:

- mix of mature and recently introduced technological tools
- mix of pathways (cargo, airports, seaports, mail centres)
- high volume vs regional/low volume conditions
- tools that affect decisions (screening/triage) versus tools that affect records/workflow (capture and referrals).

Out of scope

This review will not examine:

- detailed technical certification of models/algorithms (for example, source-code-level review, full AI/ML model redevelopment or testing), beyond checking that validation and assurance arrangements are fit-for-purpose
- Whole-of-government interoperability reform outside the department's control (only assessing interfaces but not redesign partner agency systems)
- individual incident investigations (unless used as a case study to test governance/assurance)
- procurement audit activity, including contract pricing, vendor selection decisions or commercial negotiations
- policy merits review (that is, whether policy settings are "right"), except where policy clarity/enablement affects lawful use of data/technology.
- funding except to the extent of decision-making about areas of reform.
- scientific efficacy review of research programs (such as, whether a specific diagnostic method is "best available science"), except insofar as the department's assurance/rollout governance is sound
- policies and activities of external stakeholders, including other Commonwealth agencies, state/territory governments and individuals.

6. Methodology

The review will largely be completed in the following parts:

1. *Planning and scoping*—the Inspector-General will hold an entry meeting with the departmental executives to confirm the review's purpose, objectives and scope to provide an opportunity for all parties to discuss the proposed review process.
2. *Preliminary data and information request*—seeking a dossier of relevant documents and records.
3. *Desktop review*—analysing information provided by the department.
4. *Operational technology workshop*—bringing together a cross-section of operational staff, enabling functions (including ICT/digital), and where appropriate industry-facing roles, to identify high-friction problems in current workflows and prioritise where technology, process redesign or better support arrangements could improve outcomes.
5. *Staff interviews*—interviewing relevant staff to elicit readiness and usefulness of technologies in delivering biosecurity regulatory functions under varied operating environments.
6. *Site visits (fieldwork)*—visiting targeted sites across regions to observe use of technology by frontline officers.
7. *Secondary data and information request*—another request of relevant documents and records may be made where gaps are identified.
8. *Draft review report and fact-checking*—drafting a review report and seeking feedback from the Director of Biosecurity.
9. *Report finalisation*—considering Director of Biosecurity's feedback to finalise draft report.
10. *Report publication*—transmission of final report to the Minister and publication on the Inspector-General's website.

7. Risks and treatments

Table 1 lists potential risks and treatment measures for timely completion of the review.

Table 1 Assessment and treatment of potential risks to review project

Description	Impact if unmitigated	Treatment	Mitigated risk level
Availability of sufficiently skilled staff within the Inspector-General team to deliver reviews.	• Delays to fieldwork, analysis and reporting • Reduced depth and quality of evidence and findings.	Lock in a resourcing plan early; sequence work into clear workstreams; use surge support if capacity drops; manage handovers and knowledge capture if staff move.	Low
Timely availability and access to relevant departmental managers and frontline staff for interviews and engagement.	• Slower evidence collection • Incomplete perspectives • Late-stage rework if key voices are missed.	Hold early introductory meetings to confirm scope and access pathways; issue a structured information request; establish nominated contact officers; maintain a rolling interview schedule; escalate access issues through formal channels where needed.	Low–Medium
Overall resourcing constraints impacting pace and coverage.	• Narrowed coverage or longer timeline • Reduced assurance confidence.	Prioritise "must-have" questions and evidence; phase deliverables; adopt a risk-based sampling plan; track effort weekly against plan and trigger resourcing decisions early.	Low

Moving target risk (concurrent change): major programs and releases may continue during fieldwork, shifting processes, system configurations and roles mid review.	• Findings become time-sensitive • Difficult to generalise.	Set evidence cut-off dates; capture process maps and configuration snapshots; treat changes as distinct "before" and "after" periods; confirm current-state vs future-state explicitly in findings.	Medium
Data quality and measurement risk: inconsistent performance metrics across pathways/gateways or not comparable over time (changes in definitions, baselines or collection methods).	• Lower confidence in conclusions about benefits realisation • Disputes during fact-checking • Weaker recommendations.	Develop a metric data dictionary (definitions, baselines, collection method); triangulate with operational logs and qualitative evidence; run validation checks; state limitations transparently where comparability is not achievable.	Medium
Evidence fragmentation across systems: information spread across legacy platforms, local workarounds and multiple repositories; records not standardised.	• Slow and incomplete end-to-end evidence trail • Gaps that delay drafting and clearance.	Agree early on authoritative sources; create an evidence map (what, where, owner); keep an evidence register; apply standard naming and secure storage protocols.	Low–Medium
Variation in training uptake, local procedures and informal workarounds make it harder to distinguish tool limitations from adoption issues.	Risk of misattributing root causes and targeting recommendations at the wrong problem.	Compare sites by training completion and role expectations; review training materials and local procedures; conduct task walkthroughs.	Medium
Decision accountability for technology changes spans multiple divisions and programs, delaying authoritative answers or sign-offs.	• Slower evidence confirmation • Contested findings • Delays in management response and clearance.	Map governance early (who decides and who owns controls); hold joint sessions with relevant decision-makers to resolve inconsistencies quickly.	Low–Medium
Time compression around reporting and clearance, for example: fact-checking, clearance and management response processes can take longer than planned, especially where findings touch multiple divisions.	• Schedule risk late in the timetable • Publication delays • Reputational risk if rushed.	Build clearance buffers; provide early emerging-themes briefings; run progressive fact-checking; maintain an issues log; keep evidence trails audit-ready to speed clearance.	Medium

8. Administrative contacts

Inspector-General of Biosecurity

Name	Position
Dr Melissa McEwen	Inspector-General of Biosecurity (IGB)
Dr Naveen Bhatia	Assistant Director, Project Lead, IGB Support

9. Proposed timetable

Indicative timeframes for the completion of major tasks are in Table 2.

Table 2 Indicative timeframe for completion of review tasks

Activity	Month
1. Initial planning and background research	Mar 2026

2. Review work plan	Mar 2026
3. Entry meeting	Apr 2026
4. Preliminary data and information request	May 2026
5. Desktop review of documentation and data analysis	May 2026
6. Fieldwork and staff interviews	May-Jun 2026
7. Supplementary data and information request	Jun–Jul 2026
8. Drafting of report	Aug–Oct 2026
9. Draft report to the department for fact-check	Nov 2026
10. Final review report to the Secretary to seek formal management response	Nov 2026
11. Transmission of final report to the Minister and publication on IGB website	Dec 2026

10. Conflict of interest declaration

The Inspector-General and her support staff do not have any personal conflicts of interest to declare in undertaking this review.