Overview of 1st two months of the Labor Government (2025-2028)

❖

Ministry of Home Affairs, Immigration & Citizenship, and Cybersecurity

---

This report provides an objective account of actions, policy changes, and operational measures undertaken within the Home Affairs, Immigration & Citizenship, and Cybersecurity portfolio during its first sixty days. It outlines key initiatives implemented across national security, migration management, and cyber threat preparedness, identifies major challenges and how they were addressed, highlights gaps where further work is needed, and assesses the practical impact of these developments on Australia's security, immigration policy, and cyber resilience.

Key actions undertaken

i. National security and counter-terrorism

One significant action during the period was the formal listing of "Terrorgram," a neo-Nazi online extremist network, as a terrorist organization under the Criminal Code. This measure criminalizes membership, material support, and promotion of the group's ideology, directly addressing the growing threat of online radicalization and extremist violence. The listing was prompted by evidence that the network had influenced attempted attacks in Australia, filling a legal gap in counter-terrorism powers.

In parallel, plans were outlined to expand an early intervention program piloted in New South Wales to a national level, providing parents and communities with tools to identify and respond to signs of youth radicalization. The reunification of key security agencies, including ASIO, the AFP, and Border Force which are aimed to resolve past coordination failures and strengthen intelligence sharing. Active enforcement efforts also continued, as shown by the prosecution of a suspect for an attempted firebombing of a Melbourne synagogue, demonstrating the portfolio's commitment to countering hate-motivated violence.

ii. Immigration and Citizenship

In the subject of immigration and citizenship, the issue was marked by the operational consequences of the High Court's NZYQ ruling, which invalidated indefinite detention for non-citizens who cannot be removed. The period was marked by the fallout from the High Court's NZYQ decision, which ended indefinite detention for non-removable non-citizens. The existing preventative detention powers proved unworkable, with no individuals meeting the legal threshold for re-detention. In response, alternative steps included third-country resettlement arrangements, such as transfers to Nauru, and new offences for failing to cooperate with removal efforts. Supervision and monitoring orders were applied where deportation was not immediately possible, but the legal gap remains unresolved.

More broadly, the portfolio maintained the Government's Migration Strategy, with measures like higher salary thresholds for employer-sponsored visas and the trial of the subclass 408 Workplace Justice Visa for exploited workers continuing. The approach rejected sharp cuts to migration intake, instead emphasizing the importance of skilled migration for sectors such as aged care, construction, and tourism. Regional engagement advanced through talks with Indonesia to disrupt people-smuggling networks and discussions with Bangladesh to support regular migration and diaspora links.

iii. Cybersecurity and critical infrastructure protection

Substantial progress was made in cybersecurity governance through the implementation of the Cyber Security Act 2024. The Act introduced mandatory reporting for significant cyber incidents and ransomware payments, minimum security standards for smart devices, and a Cyber Incident Review Board to assess major breaches. The number of designated Systems of National Significance under the Security of Critical Infrastructure framework also rose to over 220 assets across sectors such as energy, transport, communications, and finance. These assets now carry stricter obligations for incident response planning, cyber exercises, and real-time threat sharing with the Australian Signals Directorate.

The practical impact of these reforms was tested by a major airline data breach that exposed millions of customer records; prompt disclosure and government coordination demonstrated the benefits of the new rules while underscoring ongoing cyber risks. Public awareness work continued with the relaunch of the "Act Now. Stay Secure." campaign, promoting basic cyber hygiene such as multi-factor authentication and software updates, with resources tailored for culturally diverse and First Nations communities.

Major challenges and responses

Key challenges emerged across all parts of the portfolio. The High Court's ruling on indefinite detention left very limited tools for managing high-risk non-citizens who cannot be deported. While supervision orders and third-country resettlement have provided partial solutions, the lack of a workable, long-term legal framework remains a clear gap. In cybersecurity, the Qantas data breach highlighted that even well-prepared organizations remain vulnerable to sophisticated attacks. The incident demonstrated that the new mandatory reporting rules have practical value, but it also reinforced the need for continued vigilance and stronger enforcement.

Managing such a broad portfolio, spanning domestic security, migration integrity, and critical infrastructure protection required balancing immediate operational threats with longer-term policy development and stakeholder engagement. Public debate over migration levels intensified during this period, with proposals for drastic cuts firmly rejected in favor of maintaining skilled migration to support workforce capacity and economic stability.

Gaps and areas for improvement

Several policies and operational gaps were evident during the reporting period:

- **Preventative detention regime**: The lack of a viable legal alternative to indefinite detention leaves a gap in managing individuals assessed as high-risk but non-removable. Legislative options that balance community safety with constitutional compliance remain underdeveloped.
- **Structural migration reform**: While continuity in the migration strategy has supported stability, deeper structural reforms recommended in the 2023 review, such as simplification of visa streams and improvements to the points system have yet to be advanced.
- **Cybersecurity outreach and support**: Legislative and regulatory measures have strengthened protections for critical infrastructure and large enterprises. However, targeted support for small businesses and broader public engagement have not yet matched this uplift
- **Governance and oversight**: The reunification of core security and enforcement agencies under a single administrative structure has improved coordination but has also raised questions regarding external oversight and operational capacity. Measures to reinforce independent review and ensure sufficient resourcing would strengthen accountability.

Overall impact

The actions undertaken have contributed to a demonstrable strengthening of Australia's security posture, immigration integrity, and national cybersecurity readiness. The proscription of a newly emergent online extremist network and the planned expansion of youth anti-radicalization initiatives represent material steps in closing security gaps and preventing future threats. The reunification of intelligence and law enforcement functions is already delivering improved operational coordination, though sustained vigilance and oversight will be essential.

The following summarize recommendations dated May 29, 2025, sent by IPAG Asia Pacific, Melbourne to Hon Tony Burke, Minister for the Ministry of Home Affairs, Immigration & Citizenship, and Cybersecurity for implementing in the 1st 100 days of the 2nd term of the Labor Government. It provides status of implementation and what needs to be done is to be on track for timely completion of the initiatives.

IPAG Recommendations	Progress Made	Implementation Status (✓/✗)	Remarks
Activate Cyber Security Act & launch incident review board	Cyber Security Act implementation underway; mandatory reporting commenced; Cyber Incident Review Board announced but not yet convened for full retrospective review.	✓	Cyber Incident Review Board hasn't convened yet; ransomware regime needs expansion to better cover small businesses and the wider public.
Strengthening government cyber defenses & audit essential eight compliance	No specific agency audit results have been published yet; National Office for Cyber Security coordinating baseline uplift. No reported data on training benchmarks yet.	✓ (In progress)	Baseline uplifts underway but agencies need clear audit timelines and transparent reporting.
Expand critical infrastructure protection & response capabilities	SoNS expanded to 220+ assets; Qantas breach response tested coordination. No major new national exercise or reserve team announced yet.	✓	SoNS expansion positive but readiness needs large-scale national exercise or dedicated response teams.
Enhance Threat Intelligence sharing with new taskforce	Emphasis on real-time intel-sharing with operators. Limited detail on new taskforce or anonymized portal.	! (Limited progress)	
Develop National Cyber Workforce & pilot Federal Cyber Academy	No new national workforce target or Federal Cyber Academy announced; focus has remained on operational legislation. The focus has stayed on legislative side.	✗	Workforce pipeline remains weak; industry skills gap could widen without clear targets and funding.
Boost national anti-scam & public awareness campaigns	"Act Now. Stay Secure." campaign relaunched with tailored resources for multicultural and First Nations communities. Limited new events or community outreach; schools and local activities underdeveloped.	✓	Needs sustained funding and better outreach into high-risk groups.
Counter Foreign Interference through ASIO Operations & outreach	First-ever public threat assessment on foreign interference released; expanded outreach flagged; ASIO briefings cited. No significant gaps reported in this area.	✓	Ongoing efforts are strong; regular updates are needed to adapt to evolving threats.
Update & reboot national counter-terrorism strategy	"Terrorgram" proscribed; early intervention program announced for national expansion. No full strategy update has been released yet.	✓ (Partially)	Partial update is helpful; full strategy refresh still overdue.

IPAG Recommendations	Progress Made	Implementation Status (✓/X)	Remarks
Deliver improved migrant system reforms & Skills in Demand visa	Migration Strategy continued. No new visa pathways rolled out; points test, and visa simplification are still pending.	! (Limited progress)	Delays create uncertainty for employers and skilled migrants.
Crackdown on migrant worker exploitation & strengthen enforcement	Existing Workplace Justice Visa continues. No new measures on job mobility or joint taskforce announced.	! (Limited progress)	Compliance weak spots remain; stronger joint taskforce and proactive audits needed.

Moving forward……

The first sixty days of the consolidated portfolio have delivered significant progress across security, immigration, and cybersecurity priorities. Substantive operational actions, structural reforms, and early policy measures have strengthened national capacity to detect and disrupt extremist threats, manage complex immigration challenges within legal constraints, and address increasingly sophisticated cyber risks.

Nonetheless, several areas require sustained policy focus. Among these are the development of a legally robust framework for managing high-risk non-citizens, the implementation of structural migration reforms, expanded outreach to improve baseline cyber resilience, and continued attention to oversight mechanisms. Addressing these gaps will be critical to ensuring that initial gains translate into lasting improvements in safety, integrity, and national cyber resilience.