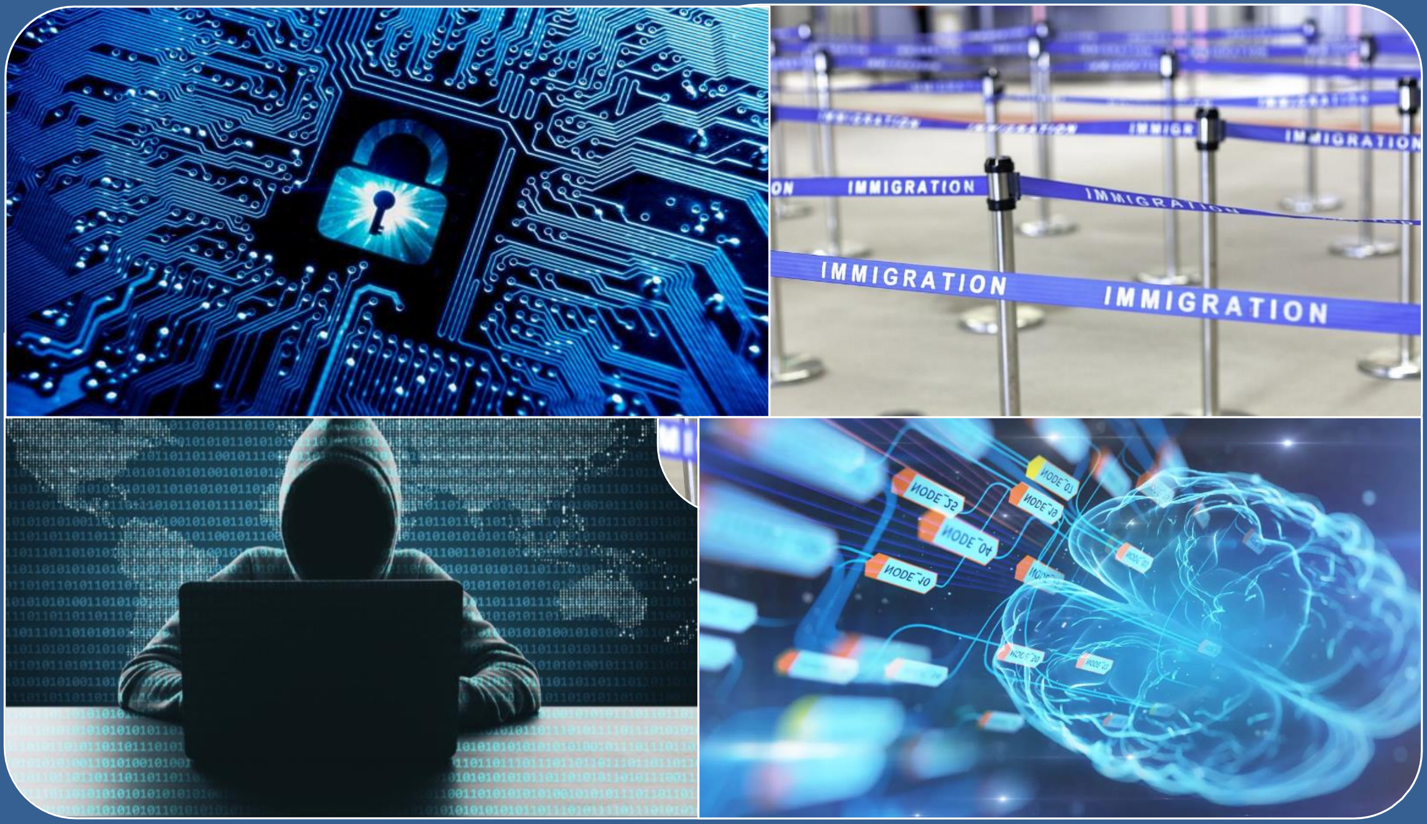
100 days strategic agenda: 10 focus areas for cybersecurity, home affairs and immigration



Department of Home Affairs

◆

Government of Australia

IPAG Asia Pacific

IPAG Asia Pacific

Level 2, Suite 201/217,
Two Melbourne Quarter,
697 Collins Street, Docklands,
Melbourne, VIC 3008

100 days strategic agenda

❖

Top 10 focus areas for cybersecurity, home affairs and immigration

The beginning of Labor Government’s second term, alongside a recalibrated Cabinet, presents a window of opportunity to advance key national priorities across Cybersecurity, Home Affairs, Immigration & Citizenship. This document sets out a targeted, time-bound agenda for the first 100 days. The suggestions respond to the surge in cyber incidents targeting Australia's infrastructure, businesses, and citizens and in parallel outline a number of interventions across Home Affairs, Immigration and Citizenship. Each recommendation is policy-anchored, stakeholder-calibrated, and structured around concrete actions, ensuring measurable progress and ministerial authority from the outset.

Section I: Top 6 priority actions on cybersecurity

Australia faces a heightened cyber threat environment, with over *1,100 cyber incidents* handled by the Australian Cyber Security Centre (ACSC) in the past year, alongside a surge in ransomware and attacks on critical infrastructure. While the overall threat landscape is broad, many recent breaches have exploited basic vulnerabilities, with credential stuffing, in particular, accounting for a large share. The following six cybersecurity priorities are ranked by priority, each with defined context and deliverables.

1. Implement landmark cybersecurity legislation and standards.

The Cyber Security Act 2024 grants authority to the ministry to mandate critical security standards and requires mandatory reporting of ransomware payments to the Australian Signals Directorate (ASD). It also establishes a Cyber Incident Review Board to investigate major breaches. These reforms address rising cyber threats following several high-profile cyber-attacks and aim to enhance national resilience.

Proposed actions:

- Convene the Cyber Incident Review Board to hold inaugural meetings and scrutinize a major incident of the past.
- ASD/ACSC to publish ransomware-reporting templates and launch a reporting portal.
- Measure success by formal activation of the Cyber Incident Review Board, completion of its first incident analysis, and documented compliance with new ransomware reporting requirements.

2. Strengthen government cyber defenses and baseline controls.

Only 15% of federal agencies met the Essential Eight Maturity Level 2 in FY2023–24, down from 25%, due to stricter ASD benchmarks (e.g., faster patching, phishing-resistant MFA). ASD issued 930 alerts for malicious activity, signifying vulnerabilities in patching, access controls, and backups. Strengthening cyber posture is essential not only for protecting sensitive public data and intergovernmental services, but also for mid-to-large enterprises where the impact of cyber breaches can be especially severe.

Proposed actions:

- All agencies audit compliance with the Essential Eight and submit remediation plans. Non-compliant agencies may be subjected to parliamentary scrutiny or temporary sanctions.
- Assign the National Cyber Security Coordinator and Home Affairs Cyber Office to oversee and assist.
- Prioritize critical patching and phishing-resistant MFA rollout and ensure 90% of users complete cyber training.

3. Defend critical infrastructure and strengthen cyber incident response.

In FY2023–24, 11% of cyber incidents handled by ASD targeted critical infrastructure. The Security of Critical Infrastructure Act 2018 (SOCI) amendment, passed in late 2024, expanded the definition of critical assets to include business-critical data and granted the Minister enhanced intervention powers during "all-hazard" incidents. Operators in 11 designated sectors, must now strengthen both operational and data systems. Government agencies must coordinate emergency preparedness, especially the Critical Infrastructure Centre and Cyber and Infrastructure Security Centre.

Proposed actions:

- Launch a Critical Infrastructure Cyber Review and Exercise Program.
- Convene CEO/CISO roundtable to outline SOCI duties and promote joint preparedness.
- Publicize and bolster the ACSC's Cyber Security Hotline (1300 CYBER1); establish deployable cyber incident response teams.
- Finalise the National Cyber Incident Coordination Plan and strengthen surge response capacity.
- Establish a cyber incident reserve, an on-call, government-backed team of elite industry experts to support major government or critical infrastructure responses.
- Demonstrate measurable improvements in response time and interagency readiness.

4. Enhance threat intelligence sharing and early-warning systems.

Timely threat intelligence sharing is critical to stopping cyberattacks before they escalate. Despite ACSC initiatives like the Cyber Threat Intelligence Sharing (CTIS) platform and Protective DNS service, gaps remain in coordination across sectors. KPMG recommends establishing an independent, anonymized, non-profit hub to collate threat data across industries, enhancing national situational awareness.

Proposed actions:

- Launch a Cyber Threat Information Sharing Taskforce including industry, government, and cybersecurity experts.
- Expand participation in the ACSC's CTIS platform and enhance real-time alert capabilities.
- Launch a pilot portal to facilitate secure, anonymized threat indicator exchange.

- Begin addressing legal and policy settings to support broader information sharing.
- Develop initial governance and funding options for a long-term public–private sharing model.

5. Accelerate cyber workforce development and skills pipeline.

Australia faces a significant shortfall in cybersecurity professionals, which threatens the delivery of national cyber initiatives. The 2023–2030 Cyber Security Strategy and 2023 Migration Strategy emphasize building a "sovereign cyber workforce.", Expanding domestic training, diversifying talent pathways, and easing skilled migration are critical to closing capability gaps and securing long-term resilience.

Proposed actions:

- Announce a national cyber workforce growth target and launch a Federal Cyber Academy pilot in partnership with ASD and academia.
- Subsidize university cyber programs and certifications, with optional service placements in government or critical sectors.
- Funds targeted Cyber Skills Scholarships in priority areas (e.g., cloud, OT security).
- Launch a global recruitment drive to attract top-tier international cyber talent, with partnered funding and academic appointments.
- Track impact through enrolments, certifications, sector hires, and international expert intake.

6. Launch a National Anti-Scam & public cyber awareness campaign.

In 2024, Australians reported over 494,000 scam incidents with $2 billion in losses, compared to 601,803 in 2023, a 25.9% drop, aided by joint efforts from the government, banks, and the National Anti-Scam Centre (NASC). Scammers now use sophisticated tactics, including phone spoofing and crypto fraud. Public education is essential to build a "human firewall." Raising digital awareness improves resilience, reduces losses, and eases pressure on support systems.

Proposed actions:

- Launch multilingual scam awareness campaigns.
- Distribute cyber safety resources to schools; ACSC to host free business-focused scam prevention webinars.
- Run Cyber Safety Days in community centers with device check-ups and multilingual support.
- Expand NASC operations; establish a new fusion cell targeting priority scam types.

Section II: Home affairs, immigration & citizenship - 4 immediate policy priorities

Beyond cybersecurity, immediate action is essential to address significant national challenges and effectively start implementing reform initiatives within the first 100 days.

7. Counter foreign interference and espionage campaigns.

Australia faces an unprecedented threat from foreign espionage and interference, now ranked by ASIO as more serious than terrorism. The initiative "Foreign Interference Rapid Response" could be undertaken, prioritizing strengthened countermeasures:

Proposed actions:

- **Boost ASIO's Counter-Interference Operations:** Allocate short-term resources to ASIO and law enforcement to intensify investigations. Track progress via ASIO's briefings and publicize outcomes where appropriate to deter further activity and demonstrate government resolve.

- **Community Outreach and Resilience:** Home Affairs engaging diaspora and student leaders through community liaison officers, establish confidential reporting mechanisms, and coordinate public awareness initiatives with ASIO.

8. Reboot counter-terrorism strategy to address emerging extremist threats.

Australia's terrorism threat level was lowered to "Possible" in 2022, yet evolving risks persist. ASIO highlights rising ideologically motivated violent extremism (IMVE), including nationalist and racist threats. The government's Counter-Terrorism Strategy needs update. Convening the ANZ Counter-Terrorism Committee would provide the appropriate intergovernmental coordination to inform and guide a comprehensive strategy refresh.

Proposed actions:

- **Update Counter-Terrorism Strategy (2025–2030):** Revise the national strategy to focus explicitly on emerging threats, including IMVE and online radicalization, incorporating insights from recent incidents and international trends.

- **Enhanced Early Intervention Programs:** Strengthen the "Prevent" pillar by expanding programs like 'Living Safe Together' into at least five new communities. Partner with local organizations for youth mentoring and pilot educational modules addressing online radicalization.

9. Deliver migration system reforms and reduce visa backlogs

Australia's migration system has undergone major reform following the release of the Migration Strategy under a comprehensive system review. Among others, the strategy discusses streamlined visa pathways, "Skills in Demand" visa with faster processing and a reformed points test to attract high-contributing migrants.

Proposed actions:

- **Roll Out New Skilled Visa Pathways:** Finalize the Skills in Demand Visa Framework. Clarify occupational criteria, streamline specialized high-earning streams, and publish clear employer/applicant guidelines. Attract top international students and skilled migrants by offering a stable, rules-based migration system and clearer post-study or long-term residency pathways amid tightening immigration settings in other advanced economies.

- **Integrity and Service Improvements:** Activate specialized units to combat student visa fraud, introduce upgraded customer service benchmarks, and enhance transparency and fairness via improved digital application-tracking tools.

10. Crackdown on migrant worker exploitation and improve visa holder protections

Protecting migrant workers from exploitation is essential to uphold Australia's labor standards and public confidence in migration. Persistent reports of wage theft, unsafe conditions, and forced labor highlight the need for urgent action. The Migration Strategy 2023 prioritizes fair treatment, proposing reforms like greater job mobility for sponsored workers. To Initiate an "Honest Work, Fair Pay" package for migrant worker protection, the following actions are to be undertaken:

Proposed actions:

- **Improve Mobility for Sponsored Workers:** Extend the employment grace period for sponsored workers seeking new jobs from the current 60-90 days up to 180 days, reducing power imbalances and exploitation risks.

- **Joint Enforcement Taskforce:** Establish a Home Affairs-Fair Work taskforce focused on high-risk industries. The task force will conduct rigorous inspections and audits and publicize enforcement outcomes to deter violations.

- **Outreach and Support**: Establish a multilingual exploitation-reporting hotline and educational outreach, prominently integrated into international student orientations and seasonal worker induction programs.

This 100-day agenda presents a focused, cross-portfolio strategy to reinforce Australia's cyber resilience, national security, and migration integrity. Each initiative is grounded in recent reforms and designed to deliver measurable outcomes through coordinated action. By aligning operational readiness with strategic direction, the agenda is designed to build early momentum and lay the groundwork for long-term capability across government and the broader community. Its success will depend on execution, coherence, and a sustained commitment to national resilience.