Purpose

1. This is the first annual report from the Government Chief Information Officer (GCIO), the Government Chief Privacy Officer (GCPO), and the NZ Intelligence Community (NZIC) on system-wide capability and maturity in privacy and protective security.

2. This report sets the new baseline for privacy and protective security across government. All agencies within the different Protective Security and GCPO mandates completed privacy and protective security self-assessments. The self-assessments are based on the Privacy Maturity and Protective Security Frameworks established by the GCPO and for the Protective Security Requirements (PSR).

Executive summary

3. Good practice in privacy and protective security underpins government's ability to safely and appropriately use, reuse, and share information to deliver citizen-centred services. It also means government security practice can keep pace with a constantly evolving threat environment. Trust and confidence in the government informs the extent to which information can be used to achieve outcomes. The safe and appropriate use of information is a key element in delivering better public services.

4. We have found that:

   - Material progress has been made in both protective security and privacy maturity, building off the Information Privacy and Security (IPS) Programme, led by the GCIO following the Review of Publicly Accessible Information Systems.
   - Agencies have increased protective security and privacy governance maturity. Strong governance is driving improvement in protective security and privacy cultures.
   - Agencies have undertaken realistic assessments of their current protective security and privacy maturity, and have clear aspirations for improvement, *[withheld under section 9(2)(g)(i) of the Official Information Act]*.
   - Chief Executives and Chairs have defined both their short term (12 month) and long term (three to five years) targets for capability in privacy and protective security. We are satisfied that these aspirations are appropriate.
   - It is not yet possible to determine whether current investment is at optimum levels to achieve agencies aspirations. Over time, the self-assessments will show whether an agency's level of investment is commensurate to their long term ambitions.
   - The maturity baseline set by core agencies and District Health Boards (DHBs) suggests that, to maximise the safe use and reuse of personal and non-personal information, a strong focus is needed on information management, information security, and business processes.
   - The threat environment is constantly evolving, and expectations on agencies to safely share information for better public services are increasing.

- Agencies need to continue to build resilient protective security and privacy cultures to ensure they are able to safely respond to the changing threat environment.
- The maturity frameworks established by the GCPO and PSR team, and their ongoing support to agencies, are designed to help build those resilient protective security and privacy cultures.
- Privacy and protective security risks will never be completely eliminated, so an ongoing focus is needed.

5. The diagrams at **Appendix A** show the current state, the 12 month state, and the future state of privacy and protective security in key areas, as assessed by agencies.

Background

6. In 2013, the State Services Commissioner and Cabinet directed the GCIO to lead a plan of action to improve privacy and security capability across the State services (Cab Min (13) 6/2D) and report to the Minister of State Services annually on progress. The GCIO established the IPS Programme. The IPS Programme resulted in system-wide improvement in operational practice. The Programme closed in June 2015, and the GCPO and the NZIC were tasked with continued focus on system-wide capability and maturity in privacy, protective security and the effective use of data and information (SEC-15-MIN-0005). This report follows on from the final report to Cabinet on the IPS Programme.
7. While good progress has been made, privacy and protective security risks will never be completely eliminated. Agencies' privacy and protective security programmes need to be regularly reviewed and updated to reflect rapidly changing security environment and evolving technology.
8. The GCPO was appointed in July 2014 (Cab Min 13 39/9) to ensure a long-term focus on privacy management and building privacy capability across the State services.
9. The PSR was agreed in December 2014 (Cab Min 14 39/38) and brings together personnel, physical and information security guidance together under one overarching risk-based framework. The PSR is administered by the New Zealand Security Intelligence Service on behalf of the NZIC.
10. The GCPO and PSR teams support Chief Executives to embed and refine improvements in privacy and protective security respectively. The GCPO and PSR teams work closely together and with agencies to lift system-wide capability and maturity in privacy and protective security. The work is subject to oversight and co-ordination through the Information Group, under the GCIO's ICT Partnership Framework. The Security Intelligence Board of the Officials' Domestic and External Security Committee provides ongoing oversight for the capability and maturity of protective security across State services.
11. The different mandates for the GCPO and PSR are set out in **Appendix B**.

Lifting operational practice within agencies

12. The GCPO established core expectations of Chief Executives, representing good practice for privacy management. The PSR Team established core requirements of agencies to enhance performance in personnel, physical and information security practices. Capability and maturity models have been established to support these expectations, along with outreach teams. These mechanisms are designed to encourage system-wide progress in practice and capability. The approach reinforces the accountability of Chief Executives, and the need for agencies to tailor their improvement programmes to their level of privacy and protective security risk.

13. While the GCPO and PSR frameworks build off the IPS programme, the GCPO and PSR self-assessments are more detailed than what was required under the IPS programme, and therefore the data is not directly comparable.

14. This report sets the new baseline for privacy and protective security across government, based on the first self-assessments from agencies.

15. The DHBs joined the GCPO mandate in July 2015. The GCPO is developing a work programme to raise Chief Executive and Board awareness of the importance of good privacy practice, focussing on governance and executive oversight. The DHBs are outside the PSR mandate.

16. The majority of New Zealanders are positive or neutral about how government agencies protect personal information. In 2015, for the first time in the Kiwis Count survey, New Zealanders were asked whether they were satisfied that the personal information they provide to government was properly protected[1]. The initial result shows that, for those that gave an opinion, nearly half (48%) are satisfied that their information is properly protected, 31% are neutral and 21% are dissatisfied. In a recent survey by the Privacy Commissioner[2], New Zealanders expressed a decreased level of concern about the way government (59% concerned) and health organisations (47% concerned) are sharing information. This represents a decrease of 8% percent and 6% percent from 2014 respectively.

17. These statistics show that, while New Zealanders' trust and confidence in government information-handling may be improving, there is a clear need for further improvement.

[1] These questions were included in the State Services Commission's Kiwis Count survey from January 2015, see *www.ssc.govt.nz/kiwis-count* .

[2] www.privacy.org.nz/news-and-publications/surveys/privacy-survey-2016/.

Analysis of the self-assessments

18. The self-assessments are agencies own views on the risks they face. It is therefore not possible to determine whether the overall investment in capability and development is at optimum levels. Over time, the self-assessments will show whether an agency's level of capability investment is commensurate to their long term ambitions. The PSR and GCPO teams are working closely with agencies who, through the self-assessments, indicated they may be struggling with aspects of their privacy or protective security programmes. We will continue to review agency progress and target support as necessary.

19. Having reviewed the 12 month plans of agencies, we are confident that more focus and effort is being brought to bear on protective security and privacy programmes. Protective security and privacy are mutually supporting, and agencies are resourcing both programmes. Agencies are making specific and overt judgements about their effort and expenditure against other risks and pressures they are facing. Agencies have indicated that the success and speed with which their privacy and protective security programmes can be developed and implemented is greatly influenced by prioritisation decisions made by the agency.

20. We have tested our analysis of the self-assessments with Deloitte, who support these findings.

Maturity in governance, leadership and accountability has increased

21. The GCPO and PSR teams' focus on governance and executive oversight has led to an increase in governance maturity. All core agencies with large personal information holdings have executive accountability, and a clear line of sight between privacy officers, and the executive. The Chief Security Officer is a member of senior management in all agencies. This line of sight has led to significant progress in privacy and protective security programmes. Governance, leadership and accountability continue to be areas of focus for agencies, and for the GCPO and PSR teams.

22. Not all DHBs have executive oversight of their privacy functions[3]. The GCPO is focussing on establishing and embedding executive oversight within the DHBs over the next year.

Improving protective security and privacy maturity is a three to five year programme

23. All agencies have committed to programmes of work to improve their protective security and privacy capability and maturity. It is expected to take agencies three to five years to reach and embed their targeted maturity levels, and to build resilient protective security and privacy practices and cultures.

[3] DHBs became subject to the GCPO mandate in the last year. A focus for the GCPO in 2016/17 is raising awareness of GCPO core expectations building off programmes used for core public sector agencies over the last two years.

24. Programmes are leveraged off existing frameworks, for example risk management, health and safety, and business continuity. Protective security and privacy requirements are presented in language and through channels already familiar to staff. This reinforces that privacy and protective security are not isolated areas for specialists, but are the responsibility of all employees of an agency.

25. We strongly support agencies taking a considered approach to developing and embedding strong protective security and privacy cultures. Agencies have achieved a level of cultural change with a deliberate focus over the last year. Embedding resilient cultural change is crucial to overall maturity, and this takes time.

26. Effective personnel security practices across State services are essential to building sustainable privacy and protective security cultures. Agencies need to satisfy themselves that they have an appropriate level of assurance regarding any person with access to agency systems or for the role they are undertaking.

27. The PSR team will work with the NZIC to support agencies in building effective personnel security capability, in support of strong protective security culture.

Use of information and information security

28. Privacy and protective security are the foundations for unlocking the value in, and the safe use and reuse of, information to assist in delivering better public services. They are also part of a complex data and information ecosystem that needs to work in combination to be effective. This ecosystem is reflected by the large number of cross-government initiatives currently underway that are likely to influence information management[4].

29. The baseline maturity scores set by core agencies and DHBs suggests that to maximise the safe use and reuse of personal and non-personal information, a strong focus is needed on information management, information security, and business processes.

30. Information security relies on the understanding and implementation of the *New Zealand Government Security Classification System.* The capability analysis suggests that most agencies are two to three steps away from their target information security maturity. Agency self-assessments commonly discuss educating personnel and enhancing records management as the next steps in improving information security.

31. 9(2)(f)(iv) confidentiality of advice

[4] By information management we mean the collection of information from one or more sources, the stewardship, use and disclosure of that information to those who need it, and its ultimate disposal.

32. The work underway is consistent with and complementary to Archives New Zealand's new Records and Information Management Standard, the Data Futures Partnership, and Land Information New Zealand's Open Government Information and Data Programme.

33. The programmes of work outlined above will influence strategic information management. Together with the work already planned by agencies, we expect an increase in information management maturity in the next 12 months.

34. We believe messages from you to Chief Executives and Chairs on the importance of good information management practices may assist agencies to focus on this area.

What does this tell us?

35. The analysis set out above tells us that:

- Agencies are progressing in developing robust and resilient protective security and privacy cultures.
- Chief Executives and Chairs have set long term protective security and privacy maturity targets, and have developed three to five year programmes to meet these targets.
- A focus on personnel security will support building sustainable privacy and protective security cultures.
- A focus on information management, information security, and business processes will help maximise the safe use and reuse of personal and non-personal information.
- Ongoing support is needed from the GCPO and PSR teams, to assist agencies to meet their targets, and respond to Ministers' expectations and the constantly evolving threat environment.

Next steps

36. The GCPO and PSR teams will continue to work with agencies to ensure ongoing increases in system-wide capability and maturity in privacy and protective security. We will refine our work programmes based on analysis of the self-assessments. Another self-assessment in March 2017 will help determine annual progress.

37. The GCIO, and the GCPO and PSR teams will consider how best to encourage an increased focus on information management and information security, particularly in agencies with large and varied data sets, and in the DHBs.

38. The PSR team will focus on building effective personnel security capability, in support of strong privacy and protective security cultures.

39. As good privacy and protective security practices are essential to building and maintaining public trust and confidence in the government, we recommend that you share this report with your Ministerial colleagues, and release this report publicly on the State Services and GCIO websites.

Recommendations

40. The Government Chief Information Officer and the Director of Security recommend that you:

    1. **Note** that the GCIO, GCPO and NZ Intelligence Community were directed by Cabinet to report to the Minister of State Services annually on system-wide capability and maturity in privacy, security and the effective use of data and information.
    2. **Note** that the GCPO and PSR programmes have resulted in system-wide improvement in protective security and privacy maturity.
    3. **Note** that reaching target capability across State services in protective security and privacy are three to five year programmes.
    4. **Note** that enhanced focus on good information management and information security practices is necessary if agencies are to be able to use, reuse and unlock the value in government held information.
    5. **Note** that the PSR and GCPO teams will work with the NZIC to support agencies in building effective personnel security capability, in support of strong privacy and protective security cultures.
    6. **Note** that the GCPO and PSR teams are focussing on assisting agencies to build resilient protective security and privacy practices and cultures over the next three to five years.
    7. **Agree** to forward this paper to your Ministerial colleagues.
    8. **Agree** that this report can be publicly released.

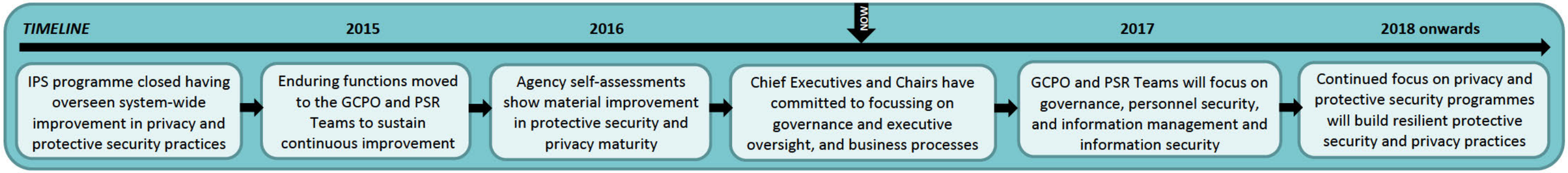
Colin MacDonald
Government Chief Information Officer

Rebecca Kitteridge
Director of Security

Hon Paula Bennett
Minister of State Services

_____/_____/_____

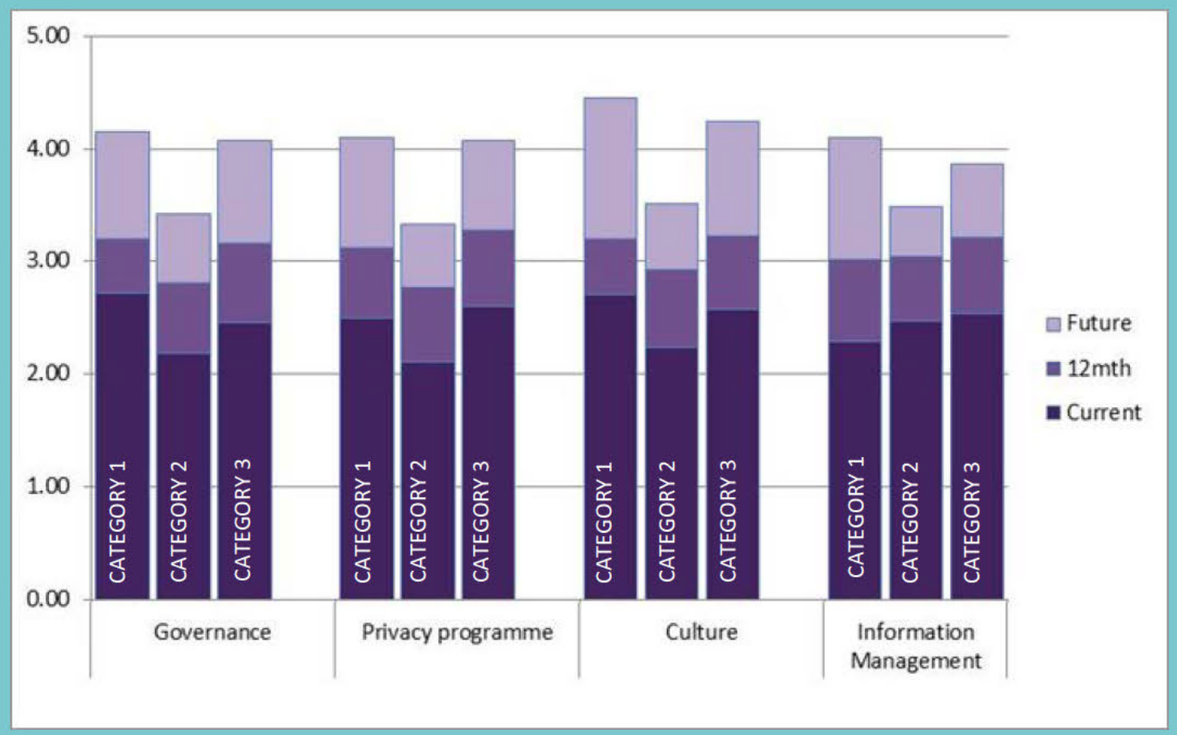
Appendix A: Current, 12 month, and future states of privacy and protective security across government

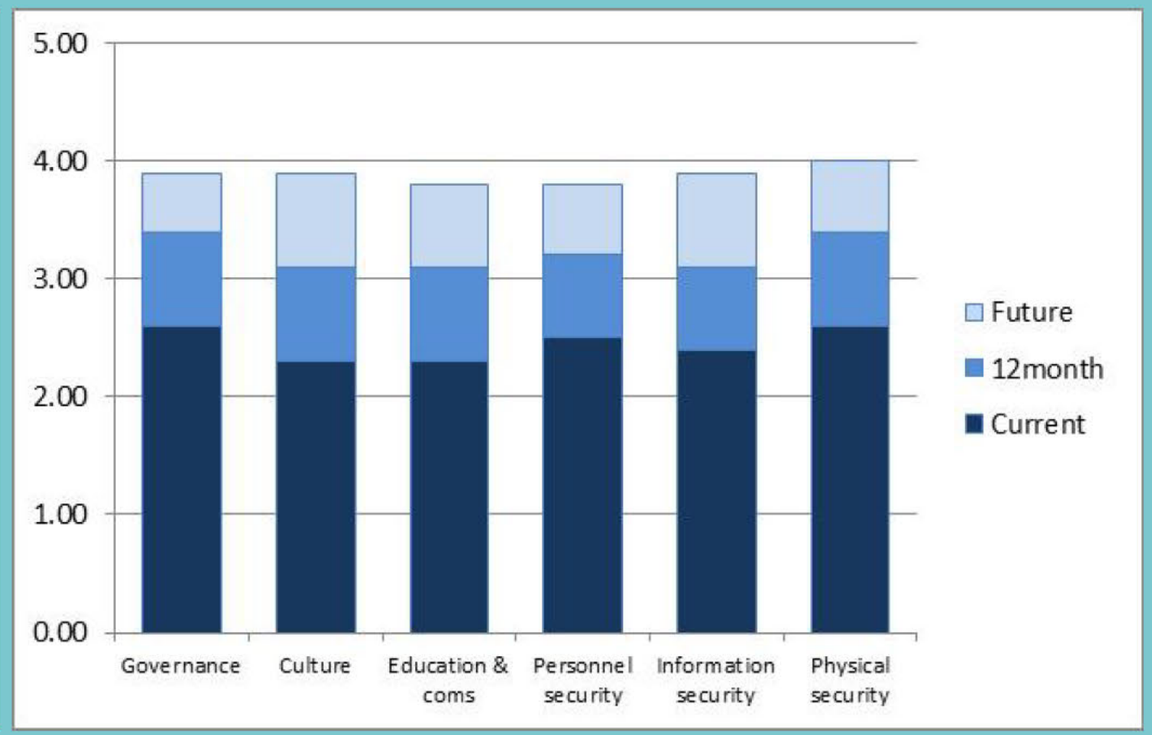


AGENCY PRIVACY MATURITY IN KEY INDICATORS

AGENCY PROTECTIVE SECURITY MATURITY IN KEY INDICATORS

These diagrams depict agency-defined current, short term (12 month) and long term (three to five years) targets for capability in privacy and protective security. We are satisfied that these aspirations are appropriate. Over time, the self-assessments will show whether investment is commensurate to long term ambitions.





Category 1: Agencies with a large and/or complex amount of personal information that may be held for different functions and purposes.
Category 2: Agencies with a small amount of personal information, or information collected for single purpose.
Category 3: District Health Boards.

The PSR mandate includes Public Sector Departments, Non-Public Service Departments in the State Services and non-State services, and one standalone agency.

LONGER TERM OUTCOMES

Government agencies effectively manage their privacy and protective security

Government agencies have safe and effective practices in information use, reuse, and information sharing

Government has the protective security capability to respond effectively to an evolving threat environment; and safely share data and information to enable better public services

→ Trust in Government
Public safety
Citizen-centred service delivery

Appendix B: Mandates of the GCPO and the PSR

The following agencies are in the Government Chief Privacy Officer's mandate

Public Service Departments

- Business, Innovation, and Employment, Ministry of
- Canterbury Earthquake Rebuild Authority
- Conservation, Department of
- Corrections, Department of
- Crown Law Office
- Culture and Heritage, Ministry for
- Defence, Ministry of
- Education, Ministry of
- Education Review Office
- Environment, Ministry for the
- Foreign Affairs and Trade, Ministry of
- Government Communications Security Bureau
- Health, Ministry of
- Inland Revenue Department
- Internal Affairs, Department of
- Justice, Ministry of
- Land Information New Zealand
- Māori Development, Ministry of
- New Zealand Customs Service
- Pacific Peoples, Ministry for
- Primary Industries, Ministry for
- Prime Minister and Cabinet, Department of the
- Serious Fraud Office
- Social Development, Ministry of
- State Services Commission
- Statistics New Zealand
- Transport, Ministry of
- Treasury, The
- Women, Ministry for

Non-Public Service Departments in the State Services

- New Zealand Defence Force
- New Zealand Police
- New Zealand Security Intelligence Service
- Parliamentary Counsel Office

Non-Public Service Departments in the wider State sector

- Office of the Clerk of the House of Representatives (voluntary)
- Parliamentary Service (voluntary)

Crown entities in the State Services

- Accident Compensation Corporation
- District Health Boards:
  - Auckland
  - Bay of Plenty
  - Canterbury
  - Capital and Coast
  - Counties-Manukau
  - Hawke's Bay
  - Hutt
  - Lakes
  - MidCentral
  - Nelson Marlborough
  - Northland
  - South Canterbury
  - Southern
  - Tairāwhiti
  - Taranaki
  - Waikato
  - Wairarapa
  - Waitematā
  - West Coast
  - Whanganui
- Earthquake Commission
- Housing New Zealand Corporation
- New Zealand Qualifications Authority
- New Zealand Trade and Enterprise
- New Zealand Transport Agency
- Tertiary Education Commission

The following agencies are in the Protective Security Requirements mandate

Public Service Departments

- Business, Innovation, and Employment, Ministry of
- Canterbury Earthquake Rebuild Authority
- Conservation, Department of
- Corrections, Department of
- Crown Law Office
- Culture and Heritage, Ministry for
- Defence, Ministry of
- Education, Ministry of
- Education Review Office
- Environment, Ministry for the
- Foreign Affairs and Trade, Ministry of
- Government Communications Security Bureau
- Health, Ministry of
- Inland Revenue Department
- Internal Affairs, Department of
- Justice, Ministry of
- Land Information New Zealand
- Māori Development, Ministry of
- New Zealand Customs Service
- Pacific Peoples, Ministry for
- Primary Industries, Ministry for
- Prime Minister and Cabinet, Department of the
- Serious Fraud Office
- Social Development, Ministry of
- State Services Commission
- Statistics New Zealand
- Transport, Ministry of
- Treasury, The
- Women, Ministry for

Non-Public Service Departments in the State Services

- New Zealand Defence Force
- New Zealand Police
- New Zealand Security Intelligence Service
- Parliamentary Counsel Office

Non-Public Service Departments in the wider State sector

- Office of the Clerk of the House of Representatives
- Parliamentary Service

Standalone agencies

- Reserve Bank of New Zealand