Annual report to Minister of State Services on privacy and protective security

Purpose

1. This is the second 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. All mandated agencies completed privacy and protective security self-assessments based on maturity frameworks established for the Protective Security Requirements (PSR) and the GCPO.
3. This second report:
    - discusses the findings from the privacy and protective security self-assessments as well as the experience of the GCPO and PSR teams in their direct engagement with agencies,
    - confirms the baseline set last year for privacy and protective security capability across the State services,
    - outlines the progress made in the previous 12 months,
    - recommends a path forward in the medium term to support continued privacy and protective security maturity, and
    - recommends a path forward in the long term to support government initiatives.

Executive summary

Positive progress

4. There has been collective improvement overall in both privacy and protective security capability since the 2016 reporting round. Several agencies have applied a degree of recalibration to their self-assessment scores, suggesting that they now have a better understanding of the requirements of privacy or protective security in regard to their own agencies. The culture of the agency together with other competing priorities has also been a factor. At a system level, capability has matured across all privacy and protective security components.
5. Agencies need to embed further capability in effective and sustainable privacy and protective security cultures as they approach their desired capability levels. Embedding a culture of privacy and protective security throughout an organisation is neither a quick nor an easy task.

Medium term deliverables

6. Agencies are responding positively to the 'critical trusted friend' role of the PSR and GCPO teams. Assistance by the GCPO and NZIC in the past 12 months on governance and personnel security has resulted in an increased capability by agencies in those two domains.

7. In our view, an ongoing focus on governance as well as effective assurance processes to support executives will add further value. This will be a central enabler in the development of effective privacy and protective security cultures.

8. The GCPO, GCIO and NZIC can further support agencies in meeting their medium term goals by providing aligned privacy and security services, de-conflicting guidance such as the New Zealand Information Security Manual (NZISM) and the PSR, and improving access to security providers through effective procurement services.

9. A focus on governance and assurance, and incremental improvements to the support provided by the GCPO and NZIC will add to the forward momentum. This will provide confidence that agencies will continue to make good progress and achieve their capability goals in the medium term. However the initial three to five year timeframe may need to be revised for privacy following the third year of reporting.

Opportunities for acceleration

10. While agencies are making steady progress in building privacy and protective security capability, cross-government initiatives such as the use of big data and digital services provide additional expectations for a secure and efficient State sector.

11. Government priorities suggest that accelerated progress is needed to support the planned delivery of better public services. Leadership of the privacy and protective security programmes at the strategic level will provide the added momentum for accelerated system-wide improvement.

12. The GCPO and NZIC will support government priorities and accelerated progress with continued support from the centre. This will need to continue once agencies have met desired capability targets as the constantly evolving threat environment, the increased focus on use and re-use of information, and the central need for the public to have trust and confidence when interacting with government means that agencies will need a sustained focus on privacy and protective security.

13. Appropriate privacy and protective security capability at the system level and sustainable privacy and protective security cultures will continue to support the successful delivery of customer centric services and the social licence.

Recommendations

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

    1. **Note** that the GCIO, GCPO and NZIC are required 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. **Agree** that the GCPO and PSR programmes have already resulted in positive progress, with system-wide improvement in privacy and protective security capability across mandated agencies.

    3. **Agree** that embedding effective privacy and protective security culture across New Zealand government will require a sustained focus.

    4. **Agree** that the GCPO and NZIC work to further provide aligned privacy and security services, de-conflict guidance such as the New Zealand Information Security Manual (NZISM) and the PSR, and improve access to security providers through effective procurement services.

    5. **Note** that government initiatives provide an opportunity to accelerate the progress agencies are making in improving their privacy and protective security capability.

    6. **Agree** that given government initiatives, privacy and protective security functional leads will support the development of programmes to accelerate progress at the system level.

    7. **Direct** the GCIO, GCPO and NZIC to continue to work together to deliver coordinated support to agencies and support above recommendation.

    8. **Agree** to forward this paper to your Ministerial colleagues.

    9. **Agree** that this report can be publicly released.

Background

15. Following the closure of the Information Privacy and Security Programme in June 2015, the GCPO and the PSR were tasked to continue to focus on system-wide capability and maturity in privacy, protective security and the effective use of data and information.

    - ***GCPO*** was established 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.
    - ***PSR*** was implemented in December 2014 (Cab Min 14 39/38) and brings together personnel, physical and information security guidance under one overarching risk-based framework. The PSR is administered by the New Zealand Security Intelligence Service (NZSIS) on behalf of the NZIC.
    - Both the GCPO and the PSR frameworks are designed to clarify core privacy and protective security requirements for agencies. Implementation is supported by engagement teams and tools (such as the privacy and protective security capability maturity models).

    The different mandates for the GCPO and PSR are set out in **Appendix 1**.

16. This report follows the first annual report on system-wide capability and maturity in privacy and protective security in 2016. The first report identified that awareness and capability were improving [*withheld under section 9(2)(g)(i) of the Official Information Act*]

17. In the first year agencies focused on effective governance as an essential foundation for lifting privacy and protective security capability. Where appropriate, agencies were starting to leverage existing frameworks such as risk management, health and safety and information management to enhance protective security and privacy processes.

18. Information management and information security emerged as areas that needed an increased focus. Mature information management practices are necessary for agencies to view information as an asset, to ensure information is appropriately protected, and to get the most out of technology, systems, and processes.

19. The previous report found a need for a sustained, medium term lift in privacy and protective security to be embedded in effective privacy and protective security culture. Robust personnel security practices and an interrelated view of protective security are essential in building strong protective security and privacy culture. Based on agencies protective security and privacy baselines in 2016, this was expected to be a three to five year programme.

Findings from the 2016/2017 year of assurance reporting

Confirmation of the baseline

20. There has been overall progress in both privacy and protective security since the 2016 reporting round. Agencies have lifted average capability across all nine privacy components and all 12 protective security components. The gaps between current

and target capability levels are shrinking and agencies have programmes in place for further capability improvements. [*withheld under section 9(2)(g)(i) of the Official Information Act*]

21. In 2016/2017 larger agencies in the privacy mandate have given greater attention to information management and business processes, smaller agencies to breach and incident management, and privacy programmes, while DHBs focused on their privacy programmes, and privacy risk management.

22. [W*ithheld under section 9(2)(g)(i) of the Official Information Act*]. The commentary provided from agencies on the implementation of the PSR suggests that agencies are looking past strict compliance to holistic security solutions that meet protective security needs and enable business.

23. Agencies are continuing to leverage existing frameworks such as risk management, health and safety and information management to enhance their protective security and privacy processes.

Evidence of a Deepening Understanding

24. Agencies are demonstrating an increased level of understanding of the privacy and protective security frameworks by applying a degree of 'recalibration'. Where an agency reported a lower level of privacy or protective security capability than last year, they commonly pointed out an improved understanding of privacy or protective security and their own positions. Additionally for some, the need to grow the agency's culture has slowed implementation of certain policies and procedures. Competing priorities have also been a factor.

25. The openness on the part of agencies, together with their willingness to collaborate to identify and address capability gaps, is a positive outcome and has been encouraged by the PSR and GCPO teams. This may reflect the teams both being regarded as a "trusted critical friend" to the system.

Progressing privacy and protective security programmes

26. Despite the recalibration in some areas, system level improvements have been made across the board. Agencies have also clearly demonstrated their ongoing commitment to improve their privacy and protective security postures. Enough momentum is evident to provide confidence that agencies will continue to make good progress towards achieving their capability targets in the medium term.

27. Capability improvements in privacy and protective security are a long term process and progress needs to continue. Agencies are progressing well to meet their capability targets; however the initial three to five year timeframe may need to be revised for privacy following the third year of reporting. As a sector, DHBs commenced their maturity journey later than other agencies but we expect them to follow a similar path to that of the other agencies. DHBs will be a particular focus for GCPO support in the coming year. They are not currently part of the PSR mandate.

Effective protective security and privacy culture requires sustained focus

28. Both the PSR and GCPO teams have focused on encouraging agencies to build appropriate privacy and protective security governance structures and to increase awareness with practitioners. As an indication that the system is responding positively to signals from the PSR and GCPO teams, agency reporting shows that executive and practitioner knowledge has improved and agencies are embedding privacy and protective security into their governance structures.

29. In our view, an ongoing focus on governance as well as effective assurance processes to support executives will add further value. This will be a central enabler in the development of effective privacy and protective security cultures.

30. Permeating good privacy and protective security awareness and practice throughout agencies is fundamental to good privacy and protective security practices. This requires agencies to have resilient and effective privacy and protective security cultures and will be central to agencies achieving their capability targets. We recognise that embedding a culture of privacy and protective security throughout an organisation is neither a quick nor an easy task.

31. The GCPO and NZIC can further support agencies in meeting their medium term goals by providing aligned privacy and security services, de-conflicting guidance such as the New Zealand Information Security Manual (NZISM) and the PSR, and improving access to security providers through effective procurement services.

32. Once an agency has reached their target privacy and protective security capability, the safeguarding of that capability will require sustained focus. The constantly evolving threat environment, the increased focus on use and re-use of information, and the central need for the public to have trust and confidence when interacting with government means that agencies will need to continue to prioritise privacy and protective security with a view to the future.

33. A sustained focus on privacy and protective security will benefit from continued support from the centre. Agencies are responding positively to the support and guidance provided by the PSR and GCPO teams, and this is being reflected in the steady improvements being made at a system level. While our approach has not been one of strict compliance, we do have robust escalation paths that can be followed when necessary.

34. Both teams are also facilitating and encouraging communities of practice and the sharing of knowledge among agencies to support a sustainable lift of system-wide capability.

Government imperatives provide incentive for accelerated progress

35. While agencies are making steady progress in building privacy and protective security capability, cross-government imperatives provide additional expectations for a secure and efficient State sector.

36. Big data and digital service transformation are government priorities to deliver better public services. Removing barriers to data sharing allows government to steward data as a system asset and achieve better outcomes for New Zealanders. However it must

be done while ensuring agencies are safeguarding the privacy and security of information. Similarly, a common standard and platform to provide single points of access for customers requires individual agencies to achieve a common baseline of privacy and protective security capability.

37. Privacy and protective security are foundations to unlocking the value in the safe use and reuse of information. The current level of privacy and protective security governance, leadership and accountability capability supports government imperatives. This focus needs to be sustained in order to support the safe use, reuse, and sharing of information to assist in delivering better public services.

38. To support this objective, the GCPO will work with the State Services Commission and the Office of the Privacy Commissioner to develop a program of targeted activities to lift and embed privacy considerations into agency practice. The GCPO and PSR teams will continue to directly engage with agencies to ensure access to privacy and protective security support and advice. This also provides the GCPO and PSR teams with insights into the ability of agencies to operate with the appropriate level of privacy and protective security capability.

39. Agencies need to deliver to New Zealand's diverse communities and people and create an inclusive culture across the public service while managing the risks presented by people. The Personnel Security Review, a Security Intelligence Board approved programme of work aimed at lifting personnel security practice across State service, is being driven by a multi-agency steering group. The Review uses a cross government reference group to identify best practice and drive change across the system.

40. The recent Ministry of Social Development sentencing has put an increased focus on physical security for agencies. The PSR team is working with WorkSafe New Zealand, State Services Commission, and the Government Property Group to ensure guidance is aligned and not duplicated. Agency implementation of the privacy and protective security frameworks should enable agencies to meet business outcomes in a safe and secure manner and reflect their risk profiles.

Strategic and functional leadership and support at the system level will enable accelerated progress

41. Agencies have programmes of work to build effective privacy and protective security capability culture. [*Withheld under section 9(2)(g)(i) of the Official Information Act*]. Government priorities suggest that accelerated progress is needed to support the planned delivery of better public services.

42. Currently, while there is an increased focus on sharing information between agencies, privacy and protective security are sometimes considered as an afterthought. Agencies are responding to government initiatives to share information; however this is not yet supported by consistent capability and effective privacy and protective security culture at the system level. Good practice does exist but it is often within teams in core agencies that regularly hold and use personal information rather than being widespread and uniform practice

43. Leadership of the privacy and protective security programmes at the strategic level would provide the added momentum for accelerated system-wide improvement. The functional leads for big data and digital service transformation have a strategic role in delivering better public services. These roles, along with the GCPO and a functional lead for protective security, are in the best position to advocate the essential and foundational role of privacy and protective security in enabling better public services at a system level.

This leadership will support trust and confidence in the system to deliver customer centric services

44. The past 12 months shows that agencies are responding positively to the 'critical trusted friend' role of the PSR and GCPO teams. A concerted effort on governance and personnel security has resulted in increased capability in those two areas.

45. Privacy and protective security direction from the leads would allow the two teams to signal the need to build proportionate capability in information management and security to better support government initiatives.

46. Public trust and confidence in transacting with the government is a fundamental pillar of customer centricity and the social licence contract. Appropriate privacy and protective security capability at the system level and sustainable privacy and protective security cultures will continue to support the successful delivery of customer centric services.

Recommendations

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

1. **Note** that the GCIO, GCPO and NZIC are required 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. **Agree** that the GCPO and PSR programmes have already resulted in positive progress, with system-wide improvement in privacy and protective security capability across mandated agencies.
3. **Agree** that embedding effective privacy and protective security culture across New Zealand government will require a sustained focus.
4. **Agree** that the GCPO and NZIC work to further provide aligned privacy and security services, de-conflict guidance such as the New Zealand Information Security Manual (NZISM) and the PSR, and improve access to security providers through effective procurement services.
5. **Note** that government initiatives provide an opportunity to accelerate the progress agencies are making in improving their privacy and protective security capability.
6. **Agree** that given government initiatives, privacy and protective security functional leads will support the development of programmes to accelerate progress at the system level.
7. **Direct** the GCIO, GCPO and NZIC to continue to work together to deliver coordinated support to agencies and support above recommendation.
8. **Agree** to forward this paper to your Ministerial colleagues.
9. **Agree** that this report can be publicly released.

[*Withheld under section 9(2)(g)(i) of the Official Information Act*]

Appendix 1: 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