New Zealand Intelligence Community
*Te Rōpū Pārongo Tārehu o Aotearoa*
nzic.govt.nz

| | |
|---|---|
| **Meeting Date:** | October 2020 |
| **Responsible Agency:** | New Zealand Security and Intelligence Service (NZSIS) |
| **Title of item:** | Review of the New Zealand Government Classification System (the System) |

## Background

1 The purpose of the System is to define how government information is classified to ensure it is appropriately protected and meets relevant requirements. Each classification indicates the sensitivity of the information and provides a base set of security measures that protect information against common threats and minimise the risk of compromise.

2 The System applies to all New Zealand government state sector organisations and its information used to conduct business including any information exchanged with external partners and personal information collected from the public.

3 The System is not mandated or required by any statute. It is an administrative act, done within a legal framework that provides public rights of access to official information and emphasises the democratic value of open government. The foundational statute in this framework is the Official Information Act 1982 (OIA).

4 In December 2018, a review was initiated under direction from SIB (the Review) on the back of a report[1] written by the Inspector-General of Intelligence and Security (IGIS) having undertaken a voluntary review of the System. The IGIS found that the System was not well understood, consistently applied, or well supported by effective systems or processes across wider government. It further found:

- Classifiers need to make inherently difficult judgements about degrees of harm to national interests.
- The distinction between policy/privacy and national security classifications is not widely understood and serves little purpose generally.

[1] A review of the New Zealand Security Classification System Report, Inspector-General of Intelligence and Security, August 2018

- IN CONFIDENCE and CONFIDENTIAL are very often confused; often notionally assumed to mean the same thing. CONFIDENTIAL has been removed by other the UK and Australia in their recent classification system reform projects. U.S.A. has asked organisations to refrain from its use.

- There is little difference between the handling measures and protections between SENSITIVE and RESTRICTED.

- There is need for a declassification regime and practices to be introduced. This finding was reinforced by observations by the Operation Burnham Inquiry that classified material complicated and delayed their work and although information was eventually obtained and approved for release to the public, it remained classified at the source.

5 The System has been unchanged since 2000. The System is nominally owned by Department of Prime Minister and Cabinet (DPMC); however the Director General of NZSIS has taken the lead on the review of the System. As part of this process, it is proposed to have Cabinet approve the proposed change in the System's ownership to the Director, NZSIS as part of the Government Protective Security Lead (GPSL) role.

## The System Review

6 The purpose of the Review was to understand the appetite for change of the System across government, design a more fit-for-purpose System, and to assess the impacts of changing the System on government.

7 Following the IGIS review, a Discussion Document was sent to 107 agencies in December 2018. Its purpose was to assess the appetite for change of the System, seek feedback on the IGIS' findings and recommendations, and understand the implications and issues a change to the system would bring. 26 agencies responded with unanimous support for changing the System and confirmation of the IGIS findings. However, there was no consensus on what a simplified System should look like.

8 A Reference Group of 17 agencies was formed and met over the course of 2019 to consider options to simplify the System. Refer to Appendix B: Fit for Purpose Classification System (Draft) for details on the recommended System.

9 In December 2019, a Change Proposal was socialised with the 36 PSR mandated agencies outlining the proposed System and outlined two options for change - Option A: Focus Guidance and Education and Option B: Change to the Fit-For Purpose System). It also requested volunteers to participate in the impact assessment process.

10 During the first half of 2020, 21 agencies participated in the impact assessment process to assess the preferences, costs, and benefits of each option.

## Key review findings

11 The key findings of the Review were:

- There was unanimous support for changing the System and confirmation of the IGIS findings by all agencies engaged during the Review.
- The System is not being applied correctly or consistently within a significant portion of the agencies interviewed and many did not use it at all.
- Evidence was found that poor application of the System leads to increased security risks and costs, which are both increasing (globally and in NZ).
- Barriers exist that prevent successful security education within agencies. These need to be addressed whether a change is made to the System or not.
- Respondents indicated that some of the security guidance is not fit for purpose (i.e. low-side agencies) and some security measures are costly to implement.
- The System underpins all protective security activity and changing it is only part of the answer – it cannot be changed in isolation of other aspects of protective security (e.g. PSR, NZISM).

## Investment objectives

12 Any investment in change of the System must achieve the following objectives and benefits:

- Make it easier for government, staff, and suppliers to understand the System and correctly classify information
- Reduce over-classification and make information easier to share
- Improve guidance and education on protecting official government information in all its forms
- Make it easier to understand and apply appropriate security measures to protect information and reduce security risks and incidents
- Reduce costs that results from System complexity, misclassification, and management of security incidents and breaches
- Support the Government's drive towards openness and transparency through regular declassification
- Improve alignment with international partners
- Make it easier and less costly for Government and suppliers to do business securely.

13 A change based on the previous objectives should achieve the following benefits for each organisation and the Government as a whole:

- Reduced risks, costs, and impacts from information security compromises

- Improved information security effectiveness and efficiency including improved capability maturity, compliance rates with requirements and standards, more secure information sharing, and clarity on methods required for secure use of technology and cloud providers

- Higher confidence and trust in New Zealand's capability to protect information appropriately including more information transparency and openness and greater compliance with regulatory, legislative, and contractual requirements (e.g. OIA, Privacy).

## Options analysis

14 The two options (Option A: Focus Guidance and Education; Option B: Change to the Fit-For Purpose System) were reviewed with agencies, analysed and the indicative costs and benefits were estimated. Refer to Appendix C: Option A and B Overview for more information.

15 Before assessment of the overall costs, Option B was the preferred option by 20 of 21 agencies interviewed. 1 agency had no preference.

16 The cost benefit analysis undertaken is indicative in nature with a moderate confidence level of 50%. To achieve a greater confidence level, Phase 1 of the proposed work programme will need to be undertaken to fully plan and confirm the business case for the change.

17 The cost benefit analysis assumes implementation across the 37 PSR mandated agencies plus 2 voluntary agencies and models the costs and benefits of doing so over a 21-year investment period.

### Option A – Focus, standardise, and centralise Education

18 Option A does not change the System but looks to improve guidance and standardise and centralise security education.

- Although Option A does not change the System, it would simplify the System through the phase out and retirement of some classification levels over time and would deemphasise the distinction between Policy and Privacy versus National Security separation. The education would focus on the remaining core classification levels and provide guidance on how to phase out and handle information still classified at retired levels.

- No agency preferred this option as the final solution. Most agencies interviewed felt that the benefits could not be realised through education without simplifying the System and underlying security measures.

- The analysis assumes that Option A could achieve 0 to 5% reduction in risk of compromise and a 0 to 5% improvement in protective security effectiveness and efficiency. This translates into 20-year benefits ranging from $59.8M (best case) to nil (worst case).

- Option A analysis indicates an investment required of $12.6M: $0.5M upfront for 6 month detailed design phase, $3.7M transition over 2 years, and $0.4M per annum ongoing over 20 years.
- At best, Option A has a return on investment within 3 years, or never in the worst case.
- The outcomes from Option A would include:

  a Achieve economies of scale through a single source of education resources

  b Overcome security education barriers and constraints

  c Make protective security more relevant, relatable and easy to use for all staff (including suppliers) – not just security practitioners

  d Improve adoption, understanding, and correct usage of the System, information handling and secure behaviours (including security risk assessment capability).

## Option B – Change to the Fit for Purpose System

19 Option B transitions to the proposed future state System. Refer to Appendix B: Fit for Purpose Classification System (Draft) for details. It also includes revisions to PSR, NZISM, and underlying guidance to align to the changed System and to make the guidance easier to use and adopt. In addition, standardised and centralised education as defined in Option A is also a key component within this option.

- The goals of this option are to address the issues identified by IGIS, improve protective security effectiveness and efficiency and lower the cost of security, reduce information security risks and breaches and their resulting impacts and costs, and would better align the System with international partners such as the UK and Australia.
- Based on agencies assessment, the analysis assumes that Option B could achieve 10 to 20% (15% midpoint) reduction in risk of compromise and a 10 to 20% (15% midpoint) improvement in protective security effectiveness and efficiency. This translates into 20-year benefits ranging from $352M (best case) to $58M (worst case) and $179M (most likely case).
- Option B analysis indicates the greatest overall investment ranging from $28M (best case) to $44.9M (worst case), with $35.4M (most likely case): $2.3M upfront for a 13 month detailed design phase, $24.8M transition phase over 3 years, and $0.4M per annum ongoing over 20 years.
- Option B provides a most likely case return on investment within 6 years and a 20-year NPV of $55M.

- The outcomes of Option B would include:

  a Act as a catalyst for increased focus on protective security

  b Improve adoption, understanding, and correct usage of the System, information handling and secure behaviours (including security risk assessment capability).

  c Introduce mechanisms to address over-classification and ensure that declassification regimes are in place.

  d Improve protective security effectiveness and efficiency and lower costs of maintaining security measures at fewer classification levels

  e Greater alignment with the revised classification systems of Australia and the UK

  f Reduce information security risks and breaches and the resulting impacts and costs

  g Support government's mandates (e.g. openness and transparency, use of cloud) in a more secure way.

## Late introduction of Option C- A phased approach

20 While the Review was underway, COVID19 hit and changed the world we live in. Given that many people do not fully understand how to handle information securely under normal circumstances and working practices have changed, there are greater risks of information compromise:

- Increased insecure information usage and storage while working from home, video conferencing, and conversations in insecure environments
- Greater international tension
- Increased commercial and IP theft
- Greater cyber exploitation of changed and potentially insecure working practices.

21 In addition, New Zealand's economic climate and government funding priorities have changed.

22 With COVID19, government agencies attention, focus, and priorities have shifted highlighting the need for a slower more phased approach.

23 In the long term, the preferred option by most agencies is to move to the fit-for-purpose System (Option B) but the estimated cost of undertaking this option is high and may not be a priority in the current economic climate.

24 Option C would implement the proposed System gradually over the next eight to ten years that will:

- Signal the desired future state to all stakeholders
- Enable effective action planning with stakeholders
- Leverage implementation of the System as part of other priority security work programmes including technology initiatives
- Flatten and reduce the investment burden over time.

## Preferred Option

25 Given the current issues and growing risks, the PSR Governance Group recommends going forward with Option C:

- The fit-for-purpose System (Option B) is the long game outcome with Option A being used as a stepping-stone to get there.
- The path forward needs to cater for the current economic climate and provide a slow but phased, focused, and managed work programme.
- The work programme delivery will require a partnership between Government Protective Security Lead (GPSL), Government Chief Information Security Officer (GCISO), Government Chief Privacy Officer (GCPO), and Government Chief Digital Officer (GCDO).
- Criteria will be developed at the outset to define and measure the success of the work to be undertaken and to assess the readiness to move forward through future phases.

26 The work programme involves three multi-year phases (Refer to Appendix A: Classification System Review Phased Roadmap for an the visual A3 view):

- Phase 1: Plan and Engage (1 to 2 years)

  a Create greater security awareness and engagement, especially for agencies who operate in the RESTRICTED and lower classification levels.

  b Develop and deliver a government wide stakeholder engagement and communication campaign (agencies, industry, and suppliers) that will be run across all phases of the programme.

  c Identify and create change champions (up to 6) and help leaders to understand the value of their information and the cost of information compromise.

d Develop and deliver guidance and education quick wins that support delivery of priority security work programmes.

e Define the requirements for the Phase 2 education programme (e.g. success measures, strategy, approach, modules, roles and responsibilities, mechanisms).

f Engage with agencies to develop an informed action plan for how to phase out of some classification levels.

g Assess readiness for future phases and develop plan and budget to undertake the next phase.

h Develop and approve the business case and roadmap for the rest of the work programme.

- Phase 2: Educate (Option A) (2 to 4 years)

  a Simplify the System through the phase out of some classification levels and to address underlying issues and education barriers.

  b Build standardised security education programme and guidance and implement mechanisms for delivery and measuring success.

  c Roll out the education programme across the 37 PSR mandated agencies. However, the material would be made available and communicated such that non-mandated agencies and private sector organisations could take advantage of it to improve their own security education and overall capability.

  d Assess and measure the effectiveness and success of education programme.

  e Review and refine the fit-for-purpose System design to confirm and ensure that it still meets requirements.

  f Define the requirements for the transition to the fit-for-purpose System (e.g. finalise changes to the System, policies, controls, ICT, processes, and guidance).

  g Identify and leverage future ICT and other work programmes to deliver on Phase 3 requirements and thus reduce the overall cost and impact of implementing Phase 3.

  h Engage widely to define the action plan to move to the revised System and confirm the business case for change. Assess readiness and obtain approvals and funding.

- Phase 3: Invest (Option B: Transition to fit-for-purpose System) (3 to 4 years)

a Transition the System to the proposed fit-for-purpose System and align security policy, requirements, technology, and controls to the revised System. This includes making necessary changes to PSR, NZISM, and underpinning processes, guidance, and systems.

b Refresh the education to reflect the changes to the System.

c The aim is to make it easier for agencies and act as a catalyst for increased adoption and compliance with the System and consistent application of appropriate security measures across Government.

d The revised System would be rolled out across the 37 PSR mandated agencies. However, the material would be made available and communicated such that non-mandated agencies and private sector organisations could also take advantage of it to improve their own security education and overall capability.

27 The initial investment required to undertake Phase 1 would be $0.5M and would require the following resources. We are requesting approval to proceed into Phase 1.

| Role | Responsibilities | (FTE) |
|---|---|---|
| Project Manager (NEW) | Overall liaison and responsibility for the delivery of outcomes, the plan for the next phase, gauging existing work programmes from leads, and handling the decision-making process | 1 |
| Business Analyst / Consultant 1 (NEW) | A focus on modelling, analysis and requirements | 1 |
| Business Analyst / Consultant 2 (NEW) | A focus on engagement and awareness with agencies, including monitoring and testing in-agency | 1 |
| Resources from up to 6 champion agencies | Analysis, liaison, consultation, testing | 6 x 0.25 = 1.5 |
| Resources from lead agencies | Governance and policy support from the System Leads: GPSL, GCISO, GCPO (possibly with GCDO) | 3 x 0.5 = 1.5 |
| External expertise | Instructional design, education delivery solution exploration, and general consultancy | - |

28 Phase 2 and 3 investment requirements will be estimated and planned during Phase 1 as part of the business case and roadmap development.

## Proposed next steps

29 GPSL to brief the Minister

- Draft and socialise a briefing paper for the incoming Minister.
- Meet with the incoming Minister to determine appetite and preferences for moving forward including the time frame for engaging with Cabinet.

30 Prepare and submit a paper to Cabinet, outlining all options and highlighting SIB's recommended option, along with the proposed change of ownership of the System.

31 If approved to proceed, wide consultation will occur during Phase 1 across all of government and government suppliers.

## Recommendations

It is recommended that SIB:

32 ***Note*** SIB initiated this Review based on the IGIS review findings YES/NO

33 ***Agree*** Ownership of the System change to GPSL YES/NO

34 ***Discuss*** The following options in the paper, noting that the PSR Governance Group has recommended Option C:

A) Option A: Focus education and improve guidance on current System but simplify it through the phase out and retirement of some existing classification levels *OR*

B) Option B: Change to the Fit for Purpose System *OR*

C) Option C: Undertake a phased approach, moving to the fit-for-purpose System over a longer period of time using Option A as a stepping stone to get there (Recommended Option) *OR*

D) Status quo – no change A/B/C/D

35 ***Note*** GPSL will socialise all options with the incoming Minister, and in doing so will convey SIB's preferences. YES/NO

## Appendix A: Classification System Review Phased Roadmap



# Fit for Purpose Classification System
# Phased Roadmap

**Desired benefits of change**

- Reduced risks and impacts of compromises
- Improved security efficiency and effectiveness
- Higher confidence & trust in New Zealand's ability to protect information appropriately

**CLASSIFICATION SYSTEM REVIEW**

The purpose of the New Zealand Government Security Classification System (the System) is to define how government information is classified to ensure it is appropriately protected and meets relevant requirements.

A classification indicates the sensitivity of the information and the special handling and management required to protect it.

**Current state findings**

- The System is overly complex, not well understood, and difficult to use. Many agencies do not classify at all.
- Inherently difficult to make judgements about degrees of harm to national interests.
- IN CONFIDENCE and CONFIDENTIAL are often confused.
- There is little difference between SENSITIVE and RESTRICTED.
- CONFIDENTIAL has been removed by both the UK and Australia; USA has asked organisations to cease using it.
- Occurrences and costs of security breaches are increasing. Cost is estimated at $1.15m average per major breach.
- Security education is identified as a gap within agencies.
- Some security guidance is considered not fit-for-purpose and some requirements too costly to implement.

## Now to 2022

**PHASE 1 — PLAN & ENGAGE**

ACTIVITY

*Focus on awareness & support*
*Focus on privacy, policy and commercial risk*

- Define readiness and success criteria and priorities for change
- Engage with stakeholders to increase awareness and identify change champions
- Plan HOW to phase out classifications with agencies
- Develop education & guidance quick wins in support of priority security work programmes
- Model and test changes with change champions
- Assess success measures and readiness for continuation
- Plan, budget, and approve next phase.

OUTCOMES

- Create champions for security education & change (up to 6)
- Create greater engagement and security awareness
- Develop an informed plan for the next phase
- Help leaders to understand the monetary value of their information and risks / costs of information compromise
- Define requirements for the education programme

## 2023 to 2027

**PHASE 2 — EDUCATE**

ACTIVITY

*Focus on standardisation of education*

- No change to the System
- Improve guidance with standardised and centralised security education and training programme and tools
- More support for organisations to implement security education, induction and culture improvement
- Improve guidance to help organisations understand, assess, and address their specific security risks
- Simplify use by phasing out of some classifications and focusing guidance in line with desired future state
- Plan, budget, and approve next phase.
- Identify and leverage future ICT and other work programmes to deliver on Phase 3 requirements (e.g. SEEMAIL, Cloud, data tagging, etc.)

OUTCOMES

- Achieve economies of scale through a single source of education resources
- Overcome security education barriers and constraints
- Reduce cost and impact of Phase 3
- Make protective security more relevant, relatable, and easy to use for all staff (including suppliers)– not just security practitioners
- Improve adoption, understanding, and correct usage of the System, information handling and secure behaviours (including security risk assessment capability)

## 2028 TBC onwards

**PHASE 3 — INVEST (IN A FIT-FOR-PURPOSE SYSTEM)**

ACTIVITY

*Focus on transitioning to the fit-for-purpose System*

- Continue Phase 2 improved guidance, support, and standardised education
- Change to a simplified and fit-for-purpose System
- Align security policy, requirements and controls to the revised System and improve guidance to be more fit for purpose, easier to adopt and comply with
- Stand up a centralised programme to facilitate and support organisations to implement the fit-for-purpose system over a multi-year transition period.

OUTCOMES

- Act as a catalyst for increased focus on protective security
- Improve protective security effectiveness and efficiency and lower costs of maintaining security measures at fewer classification levels
- Greater alignment with the revised classification system of Australia and the UK
- Reduce information security risks and breaches and the resulting impacts and costs
- Support government's mandates (e.g. openness and transparency, use of cloud) in a more secure way

## ASSESS

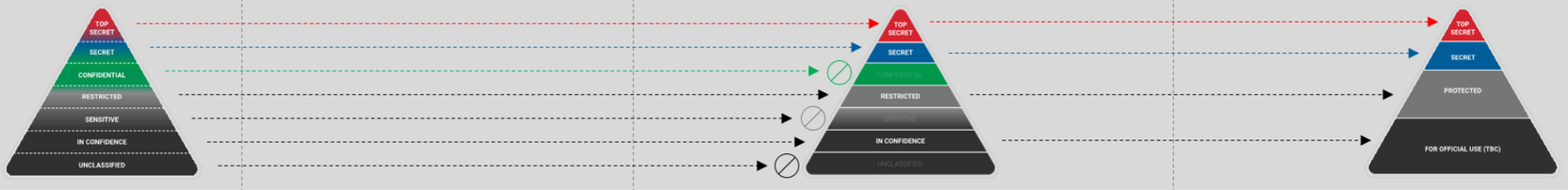
**Decision-making**
Proceed to Phase 1
Status Quo
SIB APPROVAL

**Assess against success & readiness criteria**
Decision-making
Proceed to Phase 2 (or Phase 3 if ready)
Continue in current phase
SIB APPROVAL
CABINET APPROVAL
FUNDING APPROVAL

**Assess against success & readiness criteria**
Decision-making
Proceed to Phase 3
Continue in current phase
SIB APPROVAL
CABINET APPROVAL
FUNDING APPROVAL

**Assess against success & readiness criteria**
TRANSITION YEAR 1
TRANSITION YEAR 2
TRANSITION YEAR 3
Decision-making and gateways
CONTINUED FUNDING
Keep transitioning
Final transition & ongoing BAU improvements

**System Leads: GPSL, GCISO, GCPO, GCDO & agencies acting as change champions**



## Appendix B: Fit for Purpose Classification System (Draft)

# New Zealand Government Information Classification System

| | FOR OFFICIAL USE[1] (ŌKAWA) | PROTECTED (MANAAKI) | SECRET (MUNA) | TOP SECRET (MUNA NUI) |
|---|---|---|---|---|
| **DEFINITION** | Most of the information that is created or handled by the state sector during routine business operations and services is FOR OFFICIAL USE information.<br><br>If FOR OFFICIAL USE information was compromised, the likely impact on individuals, organisations, or the national interest[2] would be **limited**.<br><br>For example, if FOR OFFICIAL USE information was compromised, it could:<br>- cause limited impact to<br>  o individuals<br>  o organisations operations or reputation<br>  o New Zealand's national interest.<br><br>FOR OFFICIAL USE includes the majority of routine and day-to-day business operations. If authorised for public release, information at this level may be published publicly. | Valuable, important and sensitive information that could damage New Zealand if it was inappropriately used, lost, stolen, or released without authorisation (for example, by being published in the media).<br><br>If the information was compromised, the likely impact on individuals, organisations, or the national interest would be **moderate**.<br><br>For example, if PROTECTED information was compromised, it could:<br>- Cause harm, significant harm or ongoing impact to individuals<br>- impede or degrade an organisation's primary function<br>- damage New Zealand's national interest. | Information that could seriously damage New Zealand's national interests if it was compromised.<br><br>The likely impact on individuals, organisations, or the national interest would be **major**.<br><br>For example, if SECRET information was compromised, it could:<br>- lead to loss of life<br>- raise international tension or cause serious damage to relationships with friendly governments<br>- cause **serious damage** to the<br>  o New Zealand economy<br>  o security or operations of New Zealand or allied forces<br>  o operations of valuable intelligence, security, or counter-terrorism activity<br>  o ability to detect, investigate, or prosecute serious organised crime<br>  o New Zealand Government operations or significant national infrastructure. | Information that could threaten the political stability or national security of New Zealand or friendly nations if it were compromised.<br><br>The likely impact on individuals, organisations, or the national interest would be **catastrophic**.<br><br>For example, if TOP SECRET information was compromised, it could:<br>- lead to widespread severe harm to the public or widespread loss of life<br>- provoke catastrophic or long-term conflict with friendly governments<br>- have a **catastrophic or long-term damage** to the<br>  o New Zealand economy<br>  o damage to the operational effectiveness of New Zealand or allied forces<br>  o effectiveness of valuable intelligence, security, or counter-terrorism operations<br>  o New Zealand Government operations or significant national infrastructure. |
| **APPLIES TO** | All state sector organisations create or handle FOR OFFICIAL USE information. | Most state sector organisations create or handle PROTECTED information. | Few state sector organisations create or handle SECRET information. | Very few state sector organisations create or handle TOP SECRET information. |
| **CONSEQUENCE LEVEL**<br>(See Matrix) | **LIMITED** | **MODERATE** | **MAJOR** | **CATASTROPHIC** |
| **BASELINE PROTECTIONS** | At this level, information must be protected using robust and effective personnel, physical, technical, and procedural security measures that maintain the information's integrity, availability, and confidentiality. Endorsements may be used to restrict its use or dissemination. | *As at FOR OFFICIAL USE, plus:*<br><br>Strict security measures are needed to protect information from compromise. These may include physical, personnel, technical, and procedural measures to control who has access to information, and how it is used and handled (measures that cover how information will be created, stored, used, shared, transported, or disposed of). Endorsements may be used to restrict its use or dissemination. | *As at PROTECTED, plus:*<br><br>Heightened security measures are necessary to keep information safe. These may include additional physical, personnel, procedural, and technical measures. Access is restricted to people with a national security clearance at the SECRET level and a 'need to know.' Endorsements may be used to restrict use or dissemination. Systems at this level are largely isolated from other systems and internet access is controlled. | *As at SECRET, plus:*<br><br>Requires the highest protection from the most serious threats. Access is restricted to people with a national security clearance at the TOP SECRET level and a 'need to know.' Due to the extreme risks associated with the information, there are very strict restrictions to access and dissemination. Endorsements may be used to restrict use or dissemination. |

1 Placeholder phrase that will be used during initial design until a final term or phrase is agreed for this level.
2 'National interest' means a matter that has or could have an impact on New Zealand's defence, security, international relations, law and governance, economic wellbeing, emergency services, and national infrastructure.

## Matrix of consequence categories (Assessing the impacts of a compromise of the information)

| Sub-impact category | LIMITED<br>Compromise of the information could be expected to have **limited impact** to individuals, organisations, or the national interest: | MODERATE<br>Compromise of the information could be expected to **disadvantage, threaten, or cause damage** to individuals, organisations, or the national interest: | MAJOR<br>Compromise of the information could be expected to **cause serious damage** to individuals, organisations, or the national interest: | CATASTROPHIC<br>Compromise of the information could be expected to **cause exceptionally grave damage** to individuals, organisations, or the national interest: |
|---|---|---|---|---|
| **Personal Impact** | • Causes short term loss of trust in the organisation or sector for an individual<br>• Causes minor or short-term inconvenience for an individual<br>• Causes or could cause limited harm to an individual, for example harm that is short term and not serious | • Causes loss, detriment, damage, or injury to the individual<br>• Causes serious ongoing impact relating to one or more individual's rights, benefits, privileges, obligations, or interests<br>• Results in significant humiliation, loss of dignity or significant or life-threatening injury | • Leads to loss of life of an individual or small group | • Leads to widespread exceptionally grave harm to a large number of people<br>• Causes widespread loss of life |
| **Reputation, trust, and confidence** | • Causes limited impact to the organisation's standing or reputation or confidence in NZ Government:<br>  • Raises low-level ministerial concerns<br>  • Creates minor credibility issues with stakeholders (internal and from other organisations) | • Causes short term damage to the organisation's reputation:<br>  • Attracts serious ministerial concern or parliamentary scrutiny<br>  • Prejudices the entrusting of information<br>  • Reduces confidence in the NZ Government with the public, other nations and international organisations | • Causes serious damage to the reputation or confidence in NZ Government:<br>  • Disrupts public order across the nation for a prolonged period (e.g. riots)<br>  • Threatens the political stability of New Zealand or other nations | • Results in exceptionally grave or long-term damage to the political stability of New Zealand or other nations |
| **Legal and regulatory** | • Causes limited impact for breach of legislation, contracts, agreements, commercial confidentiality, or legal privilege<br>• Impedes the development of policy | • Causes damages for breach of legislation, contract, agreement, commercial confidentiality, or legal privilege<br>• Impedes the ability to operate a major government policy | • Causes serious damage to the national interest:<br>  • significant lawsuit against the Crown<br>  • failure of constitutional law<br>  • serious damage to multiple major policies such that the policies can no longer be delivered | • Causes exceptionally grave, long-term impact on, or the collapse of:<br>  • rule of law<br>  • democracy<br>  • human rights<br>  • natural justice |
| **Organisational operations** | • Causes limited impact to the organisation's finances, assets, or capability:<br>  • Degrades non-critical business operations, assets, or service delivery | • Degrades or disrupts critical business operations, assets, or service delivery to the extent that the organisation can't perform one primary function<br>• Leads to a financial loss that can be accommodated within existing appropriations<br>• Creates moderate social or environmental consequences | • Disrupts critical business operations, assets, or service delivery to the extent that the organisation cannot perform any of its primary functions<br>• Leads to a serious financial loss that cannot be accommodated within existing appropriation | • Causes exceptionally grave, long term impact on the operations of the NZ government<br>• Creates exceptionally grave and irreversible financial costs to the NZ government |
| **Social and environmental** | • Creates limited social or environmental consequences | • Creates short term social or environmental consequences | • Creates serious or long term social or environmental consequences | • Creates exceptionally grave and irreversible social or environmental costs |
| **New Zealand economy** | • Causes limited impact to activities related to the production, consumption, and trade of New Zealand goods and services:<br>  • Causes limited impact to the financial viability or productivity of New Zealand based or owned organisations<br>  • Causes limited impact as a result of disclosing prematurely decisions to change or continue government commercial, industrial, economic or financial policies | • Disadvantages or damages the financial viability or productivity of one major or many minor New Zealand based or owned organisations<br>• Damages to the economy by disclosing prematurely decisions to change or continue government commercial, industrial, economic or financial policies<br>• Damages global trade or commerce, leading to a short-term recession or hyperinflation in New Zealand<br>• Impedes government negotiations (including commercial and industrial) | • Causes serious damage to the financial viability or productivity of multiple major New Zealand based or owned organisations<br>• Causes serious damage to New Zealand's commercial, economic, or financial interests or those of friendly nations<br>• Causes serious damage to global trade or commerce, leading to a prolonged recession or hyperinflation in New Zealand | • Causes exceptionally grave or long-term impact on the New Zealand economy or friendly nations |
| **International Relations** | • Causes limited impact to the international relations of the New Zealand Government (e.g. incidental and minor impairment to diplomatic relations) | • Causes damage to the international relations of the New Zealand Government (e.g. short-term disruption to diplomatic relations)<br>• Prejudices New Zealand in international negotiations or strategies | • Causes serious prejudice to New Zealand interests in international negotiations or strategies<br>• Causes serious prejudice to the international relations of the New Zealand Government | • Causes exceptionally grave damage to New Zealand's interest in international negotiations or strategies<br>• Causes exceptionally grave damage to the international relations of the New Zealand Government |
| **Crime prevention and law enforcement** | • Causes limited impact to the maintenance of law | • Prejudices the maintenance of law, including the prevention, investigation, and detection of offences, and the right to a fair trial | • Causes serious damage to the maintenance of law, regarding the prevention, investigation, and detection of serious or international organised crime or counter terrorism activities | • Causes exceptionally grave or long-term damage to the maintenance of law, including crime prevention, counter-terrorism and law enforcement |
| **National infrastructure**[3] | • Causes limited impact on national infrastructure | • Causes short-term impact on the security or resilience of national infrastructure | • Causes serious or medium-term disruption or shuts down significant national infrastructure | • Causes exceptionally grave damage or long-term impact on significant national infrastructure |
| **Emergency services** | • Causes limited impact to emergency services | • Causes short-term damage to emergency services (e.g. local or regional impact with recovery mechanisms available) | • Causes serious or medium-term disruption of emergency services (e.g. national impact with medium-term recovery mechanisms possible) | • Causes exceptionally grave damage or long-term disruption to national emergency services |

3 National infrastructure refers to the fixed, long-lived structures that facilitate the production of goods and services, including transport, water, energy, social assets, and digital infrastructure such as broadband and mobile networks

| SUB-IMPACT CATEGORY | LIMITED<br>Compromise of the information could be expected to have **limited impact** to individuals, organisations, or the national interest: | MODERATE<br>Compromise of the information could be expected to **disadvantage, threaten, or cause damage** to individuals, organisations, or the national interest: | MAJOR<br>Compromise of the information could be expected to **cause serious damage** to individuals, organisations, or the national interest: | CATASTROPHIC<br>Compromise of the information could be expected to **cause exceptionally grave damage** to individuals, organisations, or the national interest: |
|---|---|---|---|---|
| **DEFENCE AND SECURITY** | • Causes limited impact on the operational effectiveness or security of New Zealand or allied forces (e.g. affects non-operational services without causing risk to life)<br>• Causes limited impact on national security services and intelligence operations (e.g. degrades non-critical or non-operational services) | • Causes damage to the operational effectiveness or security of New Zealand or allied forces (e.g. affects non-operational services which could result in risk to life)<br>• Causes damage to national security assets or moderate impact on non-critical national security services and intelligence operations | • Causes serious damage on the operational effectiveness or security of New Zealand or allied forces, such that:<br>  • current or future military capability or installations would be rendered unusable; or<br>  • lives would be lost<br>• Causes serious damage to critical security services and intelligence operations | • Causes exceptionally grave or long-term impact on the:<br>  • defence or security of New Zealand or allied forces<br>  • continuing effectiveness of critical security and intelligence operations |
| **AGGREGATED DATA**[4] | • An aggregated holding of information that, if compromised, would cause **limited damage** to the national interest, organisations, or individuals. | • An aggregated holding of **sensitive information** that, if compromised, would **cause damage** to the national interest, organisations, or individuals. | • An aggregated holding of **sensitive information** that, if compromised, would **cause serious damage** to the national interest, organisations, or individuals. | • An aggregated holding of **sensitive information** that, if compromised, would **cause exceptionally grave damage** to the national interest, organisations, or individuals. |

## Information security principles

**Principle 1**: All New Zealand Government information[5] has intrinsic value and requires an appropriate degree of protection to maintain its integrity, availability, and confidentiality. The 'information classification' determines the level of protection it needs to keep it safe. An 'endorsement' determines any special handling or dissemination requirements. All classified information must be appropriately marked.
**Principle 2**: Everyone who works with the New Zealand State Sector (including staff, contractors, and service providers) has a duty of confidentiality and responsibility to safeguard any government information that they access, irrespective of whether it is marked or not and must be provided with appropriate training.
**Principle 3**: Access to information must only be granted on the basis of a genuine 'need to know' and managed with appropriate security controls.
**Principle 4**: Information received or exchanged with external partners must be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

## Endorsement markings[6]

| | | | |
|---|---|---|---|
| **BUDGET** | This marking may be used for proposed or actual measures for the Budget before their announcement. | **MEDICAL** | This marking may be used for material relating to:<br>• medical reports<br>• medical records and other material related to them. |
| **CABINET** | This marking may be used for material that will be presented to, and/or require decisions by Cabinet or Cabinet committees. | **NZEO** | This marking indicates that access to information is restricted to New Zealand citizens with an appropriate security clearance on a need-to-know basis. |
| **COMMERCIAL** | This marking may be used for commercially sensitive processes, negotiations, or affairs. | **ORIGINATOR CONTROLLED** | This marking identifies information where the originator controls the dissemination and/or release of the information. |
| **[DEPARMENT] USE ONLY** | This marking may be used for material intended only for use within the specified department(s). | **PERSONAL PRIVACY** | This marking identifies information under the control of the Privacy Act on access to, or use of, personal information collected for business purposes. |
| **EMBARGOED FOR RELEASE** | This marking may be used on material before a designated time at which an announcement or address will be made, or information will be disseminated. | **PUBLIC** | This marking indicates that the information is intended for release to the public. |
| **LEGAL PRIVILEGE** | This marking may be used for material that is subject to legal privilege. | **RELEASABLE TO (REL)** | This marking identifies information that has been released or is releasable to the indicated foreign countries or citizens of those indicated countries only. For example, RELEASABLE TO // GBR, NZ or REL // GBR, NZ means that the information may be passed to citizens and the governments of the United Kingdom and New Zealand only. |

4 Aggregated data is a collection of information (physical documents or digital collections) that may be more valuable than the single pieces of information it's made up of and may require a higher classification and greater security controls to protect it. A risk assessment of the aggregated information should consider "What could be deduced if the collection were compromised?" When viewed separately, the components of the collection retain their individual classification.
5 'New Zealand Government information' is any information created or held by the New Zealand state sector. This includes official information as defined in the Official Information Act and personal information held by the state sector as defined in the Privacy Act. Information exists in many forms (for example, electronic, printed, or spoken) and may reside inside or outside an organisation, including with its providers and clients, and in the cloud.
6 Endorsement markings warn people that the information has special requirements. Endorsement marking may indicate the specific nature of the information, temporary sensitivities, limitations on availability or releasability, and how recipients should handle the information. Organisations should use endorsement markings when applicable. Note: Additional endorsement markings may be used by an organisation that pertains to specific sensitive information requirements in their industry or domain.

## Appendix C: Option A and B Overview

# Classification System Review

The purpose of the New Zealand Government Security Classification System (the System) is to define how government information is classified to ensure it is appropriately protected and meets relevant requirements.

A classification indicates the sensitivity of the information and the special handling and management required to protect it.

### Current state findings

- The System is overly complex, not well understood, and difficult to use. Many agencies do not classify at all.
- Inherently difficult to make judgements about degrees of harm to national interests.
- IN CONFIDENCE and CONFIDENTIAL are often confused.
- There is little difference between SENSITIVE and RESTRICTED.
- CONFIDENTIAL has been removed by both the UK and Australia; USA has asked organisations to cease using it.
- Occurrences and costs of security breaches are increasing. Cost is estimated at $1.15m average per major breach.
- Security education is identified as a gap within agencies.
- Some security guidance is considered not fit-for-purpose and some requirements too costly to implement.


Desired benefits of change

- Reduced risks and impacts of compromises
- Improved security efficiency and effectiveness
- Higher confidence & trust in New Zealand's ability to protect information appropriately.

## Option A
## Focused guidance and education

- No change to the System
- Improve guidance with standardised and centralised security education and training programme and tools
- More support for organisations to implement security education, induction and culture improvement
- Improve guidance to help organisations understand, assess, and address their specific security risks
- Simplify use by phasing out of UNCLASSIFIED, SENSITIVE, & CONFIDENTIAL classifications and focusing guidance in line with desired future state.

**BENEFIT SAVINGS**

SAVINGS $0 to 59.8M

BREACH SAVING Up to $18.5M

EFFICIENCY SAVING Up to $41.3M

**ESTIMATED INVESTMENT**

COST $12.6m

| | |
|---|---|
| ☑ Detailed design | $0.5M |
| ☐ Programme team | $1.7M |
| ☐ Transition (2 years) | $2.0M |
| ☐ Education support | $0.4M p.a. |

The Return on Investment is estimated at never to at best 3 years, based upon the 21 year modelling period.

**OUTCOMES**

- Achieve economies of scale through a single source of education resources
- Improve adoption, understanding, and correct usage of the System, information handling and secure behaviours (including security risk assessment capability)
- Make protective security more relevant, relatable, and easy to use for all staff (including suppliers)– not just security practitioners
- Overcome security education barriers and constraints.


## Option B
## Fit-for-purpose System

All Option A improved guidance, support, and standardised and centralised training plus:

- Change to a simplified and fit-for-purpose System
- Align security requirements and controls to the revised System and improve guidance to be more fit for purpose, easier to adopt and comply with
- Stand up a centralised programme to facilitate and support organisations to implement the fit-for-purpose system over a multi-year transition period.

**BENEFIT SAVINGS**

SAVINGS $179.4M

BREACH SAVING $55.4M

EFFICIENCY SAVING $124M

**ESTIMATED INVESTMENT**

COST $35.4M

| | |
|---|---|
| ☑ Detailed design | $2.3M |
| ☐ Programme team | $4.1M |
| ☐ Transition | $20.7M |
| ☐ Education support | $0.4M p.a. |

The most likely case Return on Investment is estimated at 6 years, based upon the 21 year modelling period.

**OUTCOMES**

- Act as a catalyst for increased focus on protective security
- Improve protective security effectiveness and efficiency and lower costs of maintaining security measures at fewer classification levels
- Reduce information security risks and breaches and the resulting impacts and costs
- Support government's mandates (e.g. openness and transparency, use of cloud) in a more secure way
- Greater alignment with the revised classification system of Australia and the UK.