PSR | Protective Security Requirements

Review of the New Zealand Government Security Classification System

Change proposal document

February 2020

V1.1 – 19/02/2020

(V1.1. Update to errors in table of contents, classification rating on all pages, and fix on page 22 to reference change to placeholder for lowest classification level of MOGI)

newzealand.govt.nz

Contents

Background

Purpose and application of the System

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

The System applies to all New Zealand government state sector organisations and the information the organisation collects, stores, processes, generates, or shares to deliver services and conduct business. This includes information received from or exchanged with external partners and personal information collected from the public.

A classification indicates the sensitivity of the information (in terms of the likely impacts resulting from compromise, loss, tampering, or misuse) and the special handling and management required to protect it. An endorsement marking may be combined with a security classification to provide additional security measures for particular types of government information.

Each classification provides a base set of personnel, physical, and information security controls that offer the appropriate level of protection against common threats and therefore minimise the risk of compromise. Classification must limit access to the degree necessary for protection, while enabling access to realise the value of the information and justify the effort and intrusion involved with acquiring and keeping it.

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).[1]

Document purpose

This document has been developed by the Protective Security Requirements (PSR) to seek input on a proposal to reform the current System.

In response to the findings of 'A review of the New Zealand Security Classification System' (IGIS Review), the New Zealand Government committed to progress developing a simpler and more intuitive System for consideration by Cabinet.

This document summarises:

- The case for change and desired objectives of a reformed System
- The Review scope and next planned activity
- Three options that will be evaluated as part of the impact assessment and cost benefit analysis: Do nothing, Option A – Current System + Standardised Education, Option B – Simplified and fit-for-purpose System.

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

Case for change

2018 IGIS Review of the System

In August 2018 the Inspector-General of Intelligence and Security (IGIS) undertook a voluntary review of the System. The IGIS Report outlined the history of the System in New Zealand and other international partners, drivers for reform, and made recommendations for changes to the System. The IGIS asserted that the existing System was not well understood, consistently applied, or well supported by effective systems or processes across wider government.

In recent years, two of New Zealand's international partners have undertaken projects to reform its classification systems. The United Kingdom (UK) commenced changes to its classification system in April 2014 and is largely fully implemented. Australia commenced changes to its classification system in October 2018 which are still in transition for implementation.

The IGIS Report recommended a simplification of the System by reducing the number of classifications. Their findings were that there is need for:

- a fit for purpose classification system which caters for:
    - changes in information handling (e.g. from paper to electronic)
    - major shifts in the security environment and increased threats
    - changes in public policy relating to official information
    - learnings from reviews of significant sensitive information leaks.
- more accuracy and consistency of classification decisions which reduces:
    - non-classification resulting in a lack of clarity on its protection and disclosure requirements and under-classification resulting in not applying appropriate protections. Both issues can lead to:
        - accidental and inappropriate sharing of sensitive information
        - embarrassment for the organisation and New Zealand Government
        - high costs and impacts of managing and cleaning up after an incident or breach
        - reduced trust and confidence by the public and partners in New Zealand Government's ability to protect information.
    - over-classification resulting in impeding the effective sharing of information and can lead to:
        - increased costs and impacts of maintaining greater protections on higher classified information (personnel, physical and information security measures)
        - inefficiencies across government through the duplication of information
        - intelligence failures
        - lack of government transparency
        - reduced trust and confidence by the public and partners in New Zealand Government's effectiveness and integrity.
- addressing common issues and observations identified by users of the System such as:

- Classifiers need to make inherently difficult judgements about degrees of harm to national interests.
- The distinction between policy/privacy classifications and national security classifications is not widely understood and serves little purpose generally.
- IN CONFIDENCE and CONFIDENTIAL are very often confused; often naturally assumed to mean the same thing.
- There is little difference between the handling measures and protections between SENSITIVE and RESTRICTED.
- CONFIDENTIAL has been removed as a classification level by both the UK and Australia in their recent classification system reform projects. U.S.A. is exploring if they should remove CONFIDENTIAL and has asked organisations to refrain from its use.

In response to the IGIS Review, the New Zealand Government acknowledged these points and committed to addressing them in its own review of the System (the Review).

The Review launched

The Review was launched in December 2018 with the publication of a Discussion Document. The Review team actively engaged with individual organisations to understand their appetite for change, and to identify benefits and implications for them and those they deal with. In total the team received 26 written responses to the Discussion Document and gathered further evidence through research and meeting with key stakeholders. The findings from this engagement were:

- There was unanimous support for changing the classification system. The current System was seen to lack clarity, was overly complex, difficult to understand and apply, and required too fine a subjective judgement.
- If the existing classification system was retained, there would be risks, and potential costs, to government; either through breaches or through taking action to ensure government organisations understand and consistently apply the existing classification system and have the systems in place to support it.
- A multi-agency Reference Group was formed to consider options to simplify it and make the System more fit for purpose.
- Working with the Reference Group, the Review team explored whether improved education on the current system was a viable alternative (Option A). It was believed by some within the Reference Group that education alone has not been successful to date and a change was likely required to simplify and make the System more fit for purpose. The barriers to education will be assessed as part of the impact assessment and evaluation of Option A.
- Further analysis was undertaken to define what the simplified and fit-for-purpose System would look like (Option B).

Both investment options will be taken into the impact assessment phase to identify the impacts and analyse the costs and benefits.

Investment objectives and required benefits

Objectives

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

- 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
- Improve alignment with international partners
- Make it easier and less costly for Government and suppliers to do business securely.

Benefits

A change based on these objectives should achieve the following benefits (and possible success measures) for each organisation and government. Benefits measures would need to be confirmed, baselined, and assessed against each option within the business case should work proceed to that phase. The impact assessment will use these as indicators to assess the relative size of benefits for organisations and government.

- Reduced risks, costs, and impacts from information security compromises
    - Reduced security risk profile
    - Reduced number and/or impact level of security incidents/breaches
- Improved information security effectiveness and efficiency
    - Improved protective security capability maturity
    - Greater government and supplier compliance rates with protective security requirements and controls
    - More secure and appropriate information sharing across government and with international partners
    - Improved clarity on its appropriateness and secure use of cloud providers
- Higher confidence and trust in New Zealand's capability to protect information appropriately
    - More information transparency and openness
    - Greater regulatory, legislative and contractual agreement compliance
    - Higher partner and public trust levels with government
    - Improved efficiency and effectiveness in responding to OIA requests
    - Reduction in complaints to the Ombudsman and the Privacy Commissioner.

About the review

Scope of the review

The purpose and scope of the Review is to:

- identify a preferred option for a fit-for-purpose classification system
- understand the high-level impacts of the change for government organisations
- learn from and leverage the experiences and lessons of the UK and Australia in their changes to classification systems
- identify an implementation approach
- define and analyse the indicative benefits and costs
- define the next phase roadmap and estimates
- make an evidence-based recommendation to Cabinet on whether to proceed or not to the next phase.

Out of scope for the review

Out of scope for the Review is the work required in the Detailed Design and Implementation phases. Should Cabinet approve the initiative to proceed, the next phase (Detailed Design) would include:

- detailed design work (including policies, standards, controls, changes) - how the System would work in action alongside defining other legislative and policy changes
- detailed programme, change, and implementation planning – how the change will be achieved, over what time period, roles and responsibilities, and how the changes will be managed to deliver the benefits
- business case development and approval following Treasury's Better Business Case guidance.

Impact assessment process

Currently underway is the planning of the impact assessment and cost benefit analysis work. The Review team will engage with a representative subset of state sector organisations that will provide the basis for estimating the indicative size of costs and benefits across government.

The high level plan for this remainder of the Review work is below.

2020: JAN FEB MAR APR MAY JUN

DESIGN & PLAN	RESEARCH & ENGAGE	ANALYSE & REPORT
• Stakeholder segmentation and targeting • Identify high level benefits and cost impacts • Define change options and change proposal • Develop CBA measures and collection tool • Communications and invitations to targeted organisations • Schedule and plan engagements	• Conduct interviews and workshops with targeted organisations • Conduct desk based research • Conduct subject matter expert interviews to develop cost assumptions • Gather education insights and barriers • Conduct international research to learn from partners and overseas experiences	• Theming and consolidation • Inference and extrapolation • Apply and test assumptions and cost benefit analysis model • Develop next phase roadmap and costings • Agree recommendation • Prepare SIB / Cabinet paper

Options for analysis

Summary of the options to be analysed

The following options will be considered in the impact assessment and indicative cost benefit analysis. Each of the identified benefits and costs will be tested and estimated during the impact assessment process to enable evaluation of each option.

Do nothing	Option A – Current System + Standardised Education	Option B – Fit-for-purpose System
• No change to the System – status quo continues.	• 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.	• 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.

Do nothing

Do nothing – paint the picture

The System is unchanged. The problems and observations with status quo continue with variable adoption and compliance across the state sector. The System's complexity makes it difficult for organisations to understand and address changes in the modern environment.

Classification decisions continue to be inconsistent and result in non-classification (resulting in lack of clarity on its protection requirements and releasability), under-classification (resulting in not applying appropriate protections) and over-classification (resulting in impeding the effective sharing of information).

Security measures and controls continue to be highly complex with organisations unsure what they must do to mitigate their specific risks. This increases their risk exposure to information security incidents and breaches.

Do nothing - benefits

There are no additional benefits for this option. The impacts of change are avoided. The investment objectives and benefits would not be achieved.

Do nothing - cost drivers

There are no additional costs introduced with this option. There are continued cost drivers of doing nothing which are:

- Continued risks, costs and impacts associated with the System's complexity and associated issues with non-classification, under-classification, and over-classification
- Increased risk of security incidents due to increasing security threats which outpace the organisation's ability to improve their security capability to counter them
- Increased costs of security incident management, information sharing inefficiencies and duplication of effort, and lack of standardisation and consistency across the state sector
- Reduced trust and confidence by the public and international partners in the government's ability to protect and manage sensitive information.

Option A – Current System + Standardised Education

Option A – paint the picture

The System is unchanged. A centrally co-ordinated, resourced, and standardised education and awareness programme and resources are implemented. This would help ensure the System is adopted in a unified and coordinated manner, and is understood and used consistently and correctly across government.

- Improved guidance on:
  - the legislative and best practice requirements for information security and management
  - the value of government information and the impact of unintended disclosure
  - what and how to classify and use endorsement markings correctly
  - the management, storage, transfer, and disposal of government information and equipment
  - how to treat and manage aggregated, digital forms of information, and private sector information entrusted to government
  - the regular review of information holdings
  - sharing and holding information between organisations, third parties, other countries, and the public
  - mapping to other countries classification systems, and between the old and new system (if changed)
  - how to assess and understand the specific security risks an organisation faces and what protective measures are needed to address those specific risks
  - accountability and responsibility for the security education programme across government.

Option A - benefits

Option A should result in:

- Improved understanding of the System and greater knowledge for staff on how to classify information
- Reduction in misclassification; especially reduction in non-classification
- Improved security culture through better education and communication
- Reduction in information security breaches; in particular accidental breaches.

Overarching Benefit	**Expected Benefit Level**	**Assumptions**
Reduced risks, costs and impacts from information security compromises	Low (depending on the level of adoption across the state sector)	Improved education should make it easier for some organisations to classify and improve some adoption. Improved security culture should reduce some risks. Continued complexity of the System may limit the ability to reduce misclassification, achieve consistency of application, apply correct application of security controls, or reduce security compromises. The benefit level is likely lower than Option B.
Improved information security effectiveness and efficiency	Low (depending on the level of adoption across the state sector)	Correct classification should improve the ability to find and appropriately share information and result in less duplication and recreation of information. Continued complexity of the System may limit this benefit as misclassifications and inconsistencies are likely to continue.
Higher confidence and trust in New Zealand's ability to protect information appropriately	Low (depending on the level of adoption across the state sector)	Improved education is likely to improve an organisation's experience and compliance with key legislation e.g. OIA, Privacy Act. Continued complexity of the System may limit this benefit as the application of classifications and controls will continue to be inconsistently applied across the state sector.

Option A - cost drivers

In addition to the costs associated with the Do Nothing option, this option's additional cost drivers are:

- Developing and implementing improved security guidance (e.g. PSR, NZISM)
- Designing, developing, and implementing a centralised and standardised education and training programme (including communication, systems and tools required to deliver the training)
- Supporting organisations to incorporate the improved guidance and education programme into their own protective security framework (including people capability and capacity changes)
- Lost productivity across government and cost of planning and carrying out the training and

education programme for all staff (including contractors and supplier personnel)

- Ongoing costs of resourcing, maintaining and operating a centralised security education programme (including underlying systems and tools licensing, support, and lifecycle management).

Option B – Fit-for-purpose System

Option B description – paint the picture

In addition to the changes to improve guidance and centralised and standardised education identified in Option A paint the picture section, Option B proposes to:

Develop and introduce a simplified and fit-for-purpose System which includes the following changes:

- Simplify the classification system by reducing from 7 to 4 levels and make it easier for organisations to incorporate good information security practice into their organisational risk management frameworks and guidance. Refer to separate document "Proposed NZ Government Information Classification System". Refer to Appendix B for the proposed changes to the System and assumptions on changes to other protective security policies and processes.
- Make the government protective security guidance and controls easier to adopt and implement by ensuring it is fit-for-purpose, clear, and aligned to the 4 classification levels (including revisions to the PSR and NZISM guidance.)
- Implement the new System over a multi-year transition period based on change impact and risk assessments. Clear transition timeframe and process needs to be established as part of the detailed design phase. Some changes may be implemented at the beginning and some may be delayed or a decision taken not to implement some changes if not cost effective to do so. For example, some changes may be delayed until the next planned update, expiration, or renewal periods.

Option B - benefits

Option B should have all of the benefits of Option A plus:

- Reduce information security breaches and incidents and their resulting impacts and costs
- Easier to classify correctly and reduction in non-classification, under-classification and over-classification
- Improve staff awareness and understanding of the System and their personal obligations for managing information securely
- Improve security culture through better education and communication
- Easier to understand, adopt and apply adequate security measures to address the risks the organisation faces
- Improve access and usage of government information – e.g. finding information faster, making quicker decisions, less duplication and replication
- Lower costs of maintaining security measures (less physical security zones, networks, and controls at fewer classification levels)
- Support government's mandates (e.g. openness and transparency, use of cloud) in a more secure way through effective assessment of risks and application of appropriate measures

- Greater consistency of classifications and controls across different teams, organisations, and partners making it easier to share and ensure adequate protections are in place
- Greater alignment with the revised classifications systems of Australia and the UK. Note though this option creates less alignment with U.S.A. and Canada.

Overarching Benefit	**Expected Benefit Level**	**Assumptions**
Reduced risks, costs and impacts from information security compromises	Moderate to High (depending on the level of adoption across the state sector)	Improved education should make it easier to classify. Improved security culture should reduce some risks. Alignment of fit-for-purpose security guidance and policies will improve the correct application of security controls, improve agency security capability, and reduce security risks and compromises.
Improved information security effectiveness and efficiency	Moderate to High (depending on the level of adoption across the state sector)	A simplified system, centralised and standardised education, with aligned and clear controls makes it easier for Government and suppliers to comply with security requirements and improve overall government security capability. Correct classification should improve ability to find, use and share government information. Better application of controls should result in less incidents and reduce effort and costs to manage incidents.
Higher confidence and trust in New Zealand's ability to protect information appropriately	Moderate to High (depending on the level of adoption across the state sector)	Improved education that clearly links legislated obligations to classification and handling requirements should improve an organisation's compliance with relevant legislation e.g. OIA, Privacy Act. Improved consistency and accuracy of classification may make OIA request response processes more effective as information is correctly classified and well understood on what information can/cannot be shared. Fewer incidents and greater transparency should improve overall trust and confidence.

Option B - cost drivers

Option B will have a range of one-off impacts that will drive additional costs within each organisation and across government. For impact assessment, note that:

- This list is comprehensive to enable organisations to assess them as part of the impact assessment process.
- Some of these costs are required to develop increased governmental capability and assets which should be leveraged to reduce overall costs of government over time.
- Some activities defined in this section are undertaken by organisations as part of business as

usual and may be able to be subsumed into normal business operation.

- When considered over a multi-year transition period, some costs may be deferred to coincide with typical renewal, upgrade, or change cycles and may be accommodated under normal expenditure.

Security governance and policy

- Changes to the PSR and NZISM to align to the new classification system and to make the guidance more fit for purpose
- Assessment of the policy changes and their implications
- Clear advice will be required to minimise the need to recertify and accredit existing physical sites, ICT systems, and suppliers
- Development of guidance to help organisations assess and understand the specific security risks they face and what protective measures are needed to address those specific risks
- Support for organisations to undertake change impact and risk assessments of systems, equipment, physical locations, information holdings, suppliers and roles and defining a plan for change (Note that some changes may not be viable and mitigation plans would be developed)
- Support for organisations to undertake the changes identified in the change impacts and risk assessments. Some organisations think central funding will be required for changes, especially to ICT systems, as they would be unable to fund these from baseline budgets.

Education and communication

- Designing, developing, and implementing a centralised and standardised education and training programme (including communication, systems and tools required to deliver the training)
- Supporting organisations to incorporate the improved guidance and education programme into their own protective security framework (including people capability and capacity changes)
- Lost productivity and cost of planning and carrying out the training and education programme for all staff (including contractors and supplier personnel)
- Ongoing costs of maintaining and operating a centralised education programme (including underlying systems and tools licensing, support, and lifecycle management).

People capability and capacity

- Transition and implementation programme management, project management, and organisational change management across government and within each organisation
- Ongoing workload impacts as a result of the changes (could go up or down) and their implications on staffing and contractors
- New or changed capabilities that need to be introduced that do not exist today and their implications on staffing and contractors.

Information security

- Changes to information and communication technology systems and equipment (e.g. document management / enterprise content management systems, SEEmail, cryptographic systems) to cater for the new System while enabling continued use of the old classification levels until the information is reclassified (if ever).
- Support for implementation of new or changed information security measures such as:
    - Review and update of information security policies, processes and procedures
    - Review of physical and digital information holdings where possible and cost effective to do. Existing information holdings may not be reclassified. The limited value this exercise would deliver may not justify the cost in effort, time, and resources
    - People and systems required to enable regular review of information holdings going forward
    - Organisational personnel policies to cater for information security policy changes
    - ICT systems, equipment, policies, processes and procedures to cater for the new System
    - Ongoing information security management costs (could go up or down) including contracts, licensing, support and maintenance.

Physical security

- Support for implementation of new or changed physical security measures such as:
    - Physical work environment changes (e.g. changes to current zones, separating low side vs high side space in offshore posts, changes in physical hardware and products, floor layout and fit out)
    - Changes to rent and physical storage requirements
    - Changes to organisational personnel policies to cater for physical security policy changes
    - Changes to physical security systems and processes such as alarms, monitoring, and access control systems
    - Ongoing physical security management cost impacts (could go up or down) including contracts, licensing, support and maintenance.

Personnel security

- Support for implementation of new or changed personnel security measures such as:
    - Changes to organisational and supplier national security clearances if cannot wait for renewal
    - Implementation of role-based security clearance risk assessment process
    - Changes to organisational personnel policies to cater for personnel security policy changes
    - Ongoing personnel security management cost impacts (could go up or down) including contracts, licensing, support and maintenance

- Implications of volume changes for national security clearances on the NZSIS Vetting service.

Legislation

- Review and undertake any potential changes to either the System or to current legislation which specifies the control of official information (e.g. the Official Information Act 1982, the Privacy Act 1993, Public Records Act 2005, Crimes Act 1961)
- Review and alignment of the System changes with new or changed legislation underway (e.g. Public Service Bill, Privacy Bill).

Supply chain

- Assessment of supply chain impacts. For example, if information classified at CONFIDENTIAL is pushed up to SECRET this could increase compliance costs for vendors, which could be passed to organisations
- Procurement processes and changes to supplier contracts and agreements
- Re-certification and accreditation of AoG common capabilities, suppliers and their products including national security clearances
- Managing suppliers through the change
- Potential cost savings for suppliers who deal with government.

Information sharing

- Review and updates to international information sharing agreements (e.g. NZDF, MPI, and MFAT)
- There may be a need for transitional and replacement agreements
- Changes may need to be delayed until existing contracts or agreements are due for renewal.

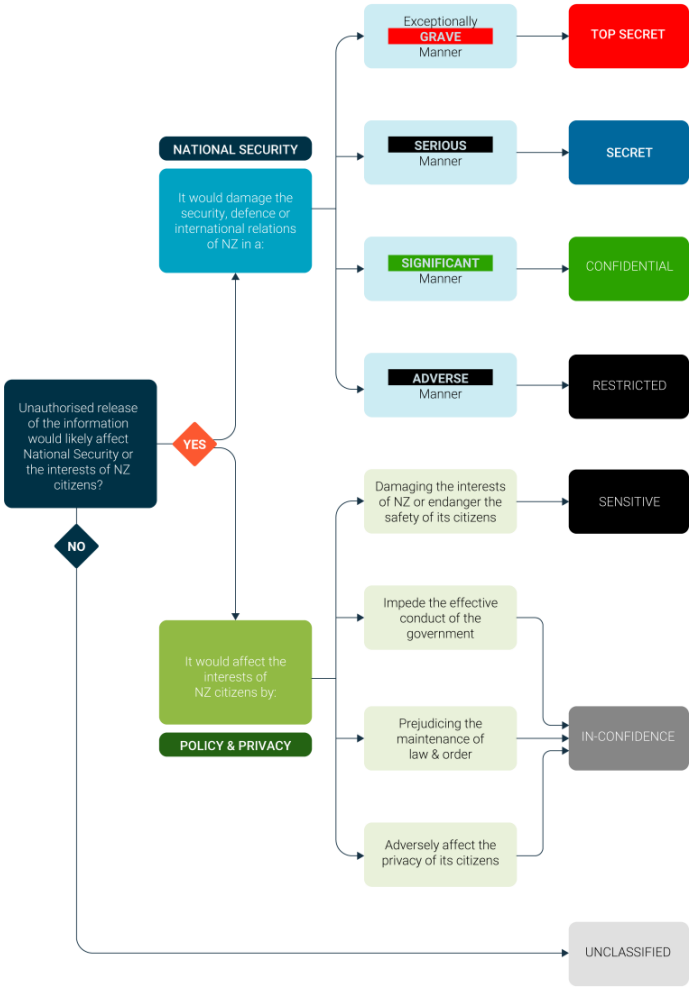
Appendices

Appendix A: Current security classifications

Our current classification system divides official government information into information that needs increased security and information that does not. The information that needs increased security is divided into two categories; policy and privacy, and national security.

Policy and privacy classifications (IN-CONFIDENCE and SENSITIVE) are used for material that should be protected because of public interest or personal privacy. National security classifications (RESTRICTED, CONFIDENTIAL, SECRET, and TOP SECRET) are used for material that should be protected because of national security. Most official government information does not meet the threshold for increased security and is referred to as UNCLASSIFIED.

The basis for applying a classification to official government information is an assessment of the risk of harm if the information was to be made generally available. The following chart shows how risk should be assessed to determine an appropriate classification.



The policy and privacy security classifications are IN CONFIDENCE and SENSITIVE, with sensitive being the higher classification.

IN CONFIDENCE

The IN CONFIDENCE security classification should be used when the compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens.

For instance, where compromise could:

- prejudice the maintenance of law
- adversely affect the privacy of natural persons
- prejudice citizens' commercial information
- prejudice [an] obligation of confidence
- prejudice measures protecting the health and safety of members of the public
- prejudice the substantial economic interest of New Zealand
- prejudice measures that prevent or mitigate material loss to members of the public
- breach constitutional conventions
- impede the effective conduct of public affairs
- breach legal professional privilege
- impede government commercial activities
- result in the disclosure or use of official information for improper gain or advantage.

SENSITIVE

The SENSITIVE security classification should be used when the compromise of information would be likely to damage the interest of New Zealand or endanger the safety of its citizens.

For instance, where compromise could:

- endanger the safety of any person
- seriously damage the economy of New Zealand by prematurely disclosing decisions to change or continue government economic or financial policies relating to:
- exchange rates or the control of overseas exchange transactions
- the regulation of banking or credit
- taxation
- the stability, control, and adjustment of prices of goods and services, rents and other costs and rates of wages, salaries and other incomes
- the borrowing of money by the New Zealand Government
- the entering into of overseas trade agreements.
- impede government negotiations (including commercial and industrial negotiations).

The national security classifications are, in ascending order of sensitivity: RESTRICTED, CONFIDENTIAL, SECRET, and TOP SECRET.

RESTRICTED

The RESTRICTED security classification should be used when the compromise of information would be likely to affect the national interests in an adverse manner. For instance, where compromise could:

- adversely affect diplomatic relations
- hinder the operational effectiveness or security of New Zealand or friendly force
- hinder the security of New Zealand forces or friendly forces
- adversely affect the internal stability or economic wellbeing of New Zealand or friendly countries.

CONFIDENTIAL

The CONFIDENTIAL security classification should be used when the compromise of information would damage national interests in a significant manner. For instance, where compromise could:

- materially damage diplomatic relations and cause formal protest or other sanctions
- damage the operational effectiveness of New Zealand forces or friendly forces
- damage the security of New Zealand forces or friendly forces
- damage the effectiveness of valuable security or intelligence operations
- damage the internal stability of New Zealand or friendly countries
- disrupt significant national infrastructure.

SECRET

The SECRET security classification should be used when the compromise of information would damage national interest in a serious manner. For instance, where compromise could:

- raise international tension
- seriously damage relations with friendly governments
- seriously damage the operational effectiveness of New Zealand forces or friendly forces
- seriously damage the effectiveness of valuable security or intelligence operations
- seriously damage the internal stability of New Zealand or friendly countries
- shut down or substantially disrupt significant national infrastructure.

TOP SECRET

The TOP SECRET security classification should be used when the compromise of information would damage national interest in an exceptionally grave manner.

For instance, where compromise could:

- threaten the internal stability of New Zealand or friendly countries
- lead directly to widespread loss of life
- cause exceptional damage to the security of New Zealand or allies
- cause exceptional damage to the operational effectiveness of New Zealand forces or friendly forces
- cause exceptional damage to the continuing effectiveness of extremely valuable security or intelligence operations
- cause exceptional damage to relations with other governments
- cause severe long-term damage to significant national infrastructure.

Appendix B: Option B changes & assumptions

Classification System

The following changes have been proposed to the System (Option B):

- Rename of the System from 'New Zealand Government Security Classification System' to 'New Zealand Government Information Classification System'
- Removal of UNCLASSIFIED, IN CONFIDENCE, SENSITIVE, RESTRICTED, and CONFIDENTIAL classification levels
- Addition of PROTECTED as classification level
- MOGI standing for Most of Government Information set as a temporary placeholder for the lowest level and will be renamed to something else (still to be agreed)
- Linkage of the classification level to the consequence category
- A reduced set of endorsement markings - these will be refined and further defined in the detailed design phase if approved to proceed.

The proposed mapping from the current classification levels to proposed classification levels are:

Current Level	UNCLASSIFIED	IN CONFIDENCE	SENSITIVE	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
Proposed Future Level	MOGI (Most of Government Information)		PROTECTED		*Risk assessed & reclassified up or down* ↔	SECRET	TOP SECRET

Education and culture

Note that these change assumptions equally apply for both Option A and Option B

- A significant culture change is required across the state sector and with government suppliers. Standardised and centralised security education, training and communication is required to shift to the desired security culture and practice. The effort and leadership required should not be under-estimated. Some of the issues identified are:
    - Low capability in identifying and managing risks
    - Some organisations have a high-risk tolerance without understanding or addressing the risks that they face
    - Prevalent attitude of "she'll be right mate" and "the issues that happen overseas won't happen here in New Zealand".

Business Impact Levels / Consequence Categories

Business impact levels (BILs) are used to assess the likely impacts of security breaches.

- Rename BILs to Consequence Categories to align to an organisation's risk management framework
- Reduce from 6 levels to 4 levels to align with the classification levels

- Redefine impact descriptions into sub-impact categories and refine the language and definition to reduce the difficulty in making classification judgement calls.

National Security Clearances

- No change to SECRET, TOP SECRET, or TOP SECRET SPECIAL security clearance levels
- Discontinue CONFIDENTIAL security clearance level
- Introduce a 'base' national security clearance
    - This clearance would be used for positions that have access to information, people, or assets that could pose a 'high risk' to the protection of New Zealand's national security, international relations, or economic well-being of New Zealand
    - It would use the same vetting processes, checks and lifecycle management as the current CONFIDENTIAL security clearance
    - The clearance name, definition and eligibility criteria would be developed in the detailed design phase if this option is approved to proceed to the next phase
    - The eligibility criteria would be aligned with the Intelligence & Security Act (ISA) 2017. To accommodate this change, some minor amendments may be required to the ISA.
    - A position risk assessment process would need to be undertaken to demonstrate a clear need for the security clearance. The risk assessment process, criteria, systems, and materials would be developed in the detailed design phase.
- Government organisations would need to review and amend their employment policy and procedures to address the implications of individuals receiving an adverse and not recommended for obtaining a national security clearance.

Physical security

- Reduce from 5 to 4 zones to align with classification levels
- Review, rename and realign zone definitions and requirements to the revised classification levels and consequence categories
- Review, simplify and align physical security requirements to four zones and four classification levels. Today, compliance with requirements is a massive issue so review and revision is required to be more fit-for-purpose. It should be easier to map approved products to four zones
- Provide better guidance to help organisations assess and understand the specific physical security risks they face and what protective measures are needed to address those specific risks.

Information security

- PSR and NZISM change assumptions are:
    - No change or impact to SECRET or TOP SECRET controls
    - Review, simplify and align all other information security control requirements to the changes with the System and consequence levels
    - Need a clear and effective risk assessment process to determine appropriate security

controls that are required for low side systems. We need to ensure that a security control chasm is not created between PROTECTED and SECRET

- Ensure that the guidance is more fit-for-purpose to improve the organisation's ability to comply with the requirements, is affordable to New Zealand Government, and improves overall government information security
- Provide better guidance to help organisations assess and understand the specific information security risks they face and what protective measures are needed to address those specific risks (e.g. when should optional controls become mandatory).

- ICT systems and equipment change assumptions are:
  - Changes to classification levels would be grand-parented enabling system reclassification to be staged and aligned with other changes planned to those systems
  - Systems, equipment and networks classified at CONFIDENTIAL would have a risk-assessment conducted to determine its future classification level and change required. They may be elevated to SECRET or downgraded to PROTECTED. The impacts of the changes would be assessed, costed and planned as part of transition
  - To minimise the impact, CONFIDENTIAL systems and equipment could be reclassified at PROTECTED with a special endorsement marking and corresponding handling procedures that are equivalent to the handling requirements currently defined for the system or equipment at CONFIDENTIAL today
  - SENSITIVE and RESTRICTED systems, equipment, and networks would most likely change to PROTECTED
  - Changes are planned for SEEMAIL in the future and any changes required as a result of a System change could possibly be accomplished at the same time
  - Changes to technical systems may require recertification and accreditation which will be assessed during the impact assessment and if required will be planned during transition planning
  - There would be no requirement to change legacy systems, infrastructure and equipment nearing the end of their useful life. Replacement would be prioritised over upgrade where the costs of change are too high
  - COMSEC equipment is purchased and transported from overseas and any changes to classifications and handling procedures will need to be aligned with the requirements from the originating country. Agreements, controls, and handling procedures will need to be reviewed and possibly updated (including ITAR)
  - Any change to the classification of a system, equipment or network may have flow on impacts to physical security of sites, secure equipment, handling requirements and procedures, national security clearances for staff, and contracts and accreditation for suppliers.

Legislation

- Legislation was reviewed to determine if changing the System will have any impacts on current legislation. It is believed that the proposed changes would not have direct impact on any current legislation. The NZSIS Legal team has reviewed the proposed changes and made the following recommendations:

- Provide guidance to agencies that information is marked to indicate all applicable classifications
- Clarify the distinction between the System and other legal classifications in the guidance issued and for information to be subject to dual classification, and which duties prevail over others
- Provide a reasonable timeframe before the new System comes 'into effect' to allow agencies to make the necessary changes.