Secret Advisory Board - Meeting Outcomes - June 1st, 2011

Meeting Date: June 1st 2011 1530 – 1630, at PM&C

Members: Rachel Noble (PM&C Chair), Hilary Russell (AGD), Matt Yannopoulos (Defence), John Sheridan (AGIMO), Mike Pezzullo (Customs), s38 [redacted] Tuan Dao (DFAT)

Attendees: Rachel Noble (PM&C Chair), Glenn Ashe (AGD), Matt Yannopoulos (Defence), Mike Pezzullo (Customs), s38 [redacted], Joe Attanasio (Customs), David Nethery (DFAT), Rupert Hollin (PM&C), Frank Lewincamp (PM&C), s38 [redacted] Will Courcier (PM&C)

Apologies: John Sheridan (AGIMO), Tuan Dao (DFAT)

Purpose: The purpose of the meeting was to review a paper presenting the key issues relating to the current state and possible future direction of the Secret classification domain. The Advisory Board considered the analysis and provided guidance for future work.

Three options were presented for the provision of a Secret classification environment:

1. The status quo

s33(a)(i) [redacted]

Discussion: Discussion included the following areas:

Single versus multi provider model, with concerns for a single provider model

- Defence stressed the need for any s33(a)(i) [redacted]

- Defence advised they were unable to provide a secret classification domain service for the whole community
- The proposed new national security classification nomenclature may have implications of agency business needing to move into the secret classification space
- The need for the new model to represent value for money for consumer departments to encourage them to use the community secret domain

Outcomes:

s33(a)(i) [redacted]

- The SAB agreed that PM&C and the current Secret classification network provider agencies, undertake further work to s33(a)(i) [redacted]

Action Items:

- PM&C will advise the IMPG and NSPCG/SPCG of the work undertaken, strategy and approach for progressing the secret domain model.
- PM&C, DFAT, Defence, ACBPS, AGD and DoFD will develop a more detailed Secret classification domain model including:
    - s33(a)(i) [redacted]
    - the roles of each provider
    - the approach for progressing coordinated developments and support
    - the governance arrangements for providers and stakeholders for managing the environment
    - an outline of the future environment

Overview of the Advisory Board Paper

Executive Summary

This paper presents the preliminary assessment of the key issues relating to the current state and possible future direction of the Secret Domain. The Advisory Board is asked to consider the analysis, refine it as necessary, and provide guidance for further work.

The attached paper presents the following information:

- Paragraphs 3-8 describe the multiple Domains. These Domains have developed in isolation, are being moved together but are a long way from the vision of providing the environment Government needs to support business needs.
- Paragraphs 9-19 describe the vision and assessment of the Domains. A more harmonised and aligned environment is needed to support international and domestic information sharing and desired business processes.
- Paragraphs 20-47 describe options for further progression of the Domain. Stronger coordination is suggested with central planning, management and development to align the environment with the needs of business. Detailed discussion on the state of the current infrastructure, data and applications is presented. s33(a)(i) [redacted] Service provision options are presented to: maintain the status quo; s33(a)(i) [redacted] Further options, initiatives and measures

Decision Points

- To accept in principle the other measures and initiatives outlined in the paper
- To agree in principle to s33(a)(i) [redacted] to meet the needs of the National Security Community
- To adopt the medium term goal s33(a)(i) [redacted]

Way Ahead

If agreed, it is proposed:

- this model for the Secret Domain is presented to IMPG, HPCG/SPCG; and
- a business plan is developed to progress and implement this Secret Domain business model, with intitiatives being incorporated into the National Security Information Environment Roadmap.

ADVISORY BOARD PAPER

ASSESSMENT OF THE AUSTRALIAN GOVERNMENT SECRET ICT DOMAIN: Progress Report, May 2011

1. Late last year, the Department of Prime Minister and Cabinet commenced an assessment of the current state and future direction of the Australian Government Secret ICT domain. NSCIO staff and a consultant, Frank Lewincamp, have conducted interviews with senior executives of relevant agencies to develop an understanding of the current and emerging business needs of agencies, and their associated communities, operating at the Secret level. NSCIO staff have also engaged with senior agency ICT staff to develop a picture of the current and planned Secret-level networks.

2. This paper presents the preliminary assessment of the key issues relating to the current state and possible future direction of the Secret Domain. The Advisory Board is asked to consider the analysis, refine it as necessary, and provide guidance for further work. At the Board meeting, the NSCIO will also invite discussion on the timeframe and approach for finalising this work, integrating it with other relevant initiatives, and bringing it to Government for its consideration.

Multiple Government Domains

3. ICT systems to support Australian Government business operate, and will continue to operate, at several different security classification levels – Top Secret, Secret, and Restricted/Unclassified. This situation remains complicated by a second classification system [Highly Protected, Protected and In-Confidence], used by some agencies. The initiative to move to a single security classification system is progressing – although there remain differences of view about how best to transition the disparate information at the Protected level into the single system.

- A key issue is what connectivity is allowed from internet-facing systems to higher security level systems, a connectivity required by many agencies for their interaction with State/territory agencies, the private sector and the public.

4. A number of recent reviews and reports have examined information management and sharing across the Australian Government and nationally. These include the Gershon Report, Ian Reinecke's *Independent Review of Implementation of the ICT Reform Program*, John McMillan's *Towards an Australian Government Information Policy*, AGIMO's *National Government Information Sharing Strategy,* and AGIMO's *Strategic Vision for the Australian Government's Use of ICT*. A number contain initiatives and recommendations relevant to the Secret Domain.

- Surprisingly, perhaps, a number also appear not to be aware of initiatives in the National Security Community (NSCy) [or even the role of the NSCIO].

5. There are several major challenges to the management and sharing of information across the Australian Government:

- Agencies conduct like or similar business functions predominantly at different levels of security classification;
- Many agencies have not yet made explicit decisions about the classification level or levels at which they wish to conduct specific business functions

s22 [redacted]

- In a number of cases, as additional agencies participate in the NSCy, they are adding Secret-level business operations to those previously done only at lower security levels, raising information sharing challenges both within the agencies and between them.
- A number of agencies have established separate ICT arrangements, including data storage, at each security classification level – or stove-piped arrangements at the one classification level - with limited capacity to capture and analyse enterprise-wide information;

- s33(a)(i) [redacted]
- Information must be transferred and integrated from different classification levels for analysis/assessment purposes, and then s33(a)(i) [redacted]
  - An additional complication is the timely transfer, assessment and transmission of time-sensitive, actionable information from an increasing number and variety of sources;
- s33(a)(i) [redacted]

6. A key operating principle should be that collectors of information [whether intelligence or operational agencies] have a responsibility to make information discoverable, accessible and available in a timely way. The NSCy is moving from a paradigm of agencies and individuals being supplicants for relevant information which others hold, to one in which agencies are responsible, and held accountable, for providing information – and it must complete that transition quickly. There is a corresponding paradigm shift from agencies being owners of information to being stewards of information which rightly belongs more broadly to government. This has significant implications for planning, business processes and ICT.

<u>Cross-Domain Issues</u>

7. Cross-domain issues to be addressed are:

(1) Clear and final guidance on the single security classification system/ nomenclature and speedy implementation, including
- How to transition information from the Protected level into the single system
- Agreement on protocols for interfaces with the internet-facing environment;

(2) Policy and protocols on the transfer of information across levels to meet defined business needs

s33(a)(i) [redacted]

(3) Decisions on other functionality required across security domains
- For example, email and voice communications;

(4) Multi-agency agreement on broader information management policy and protocols, and related business processes, including

s22 [redacted]

- The classification level(s) at which specific business functions are predominantly to be conducted
- The responsibility to provide information, of which agencies are stewards rather than owners, with agreed protocols on sharing of, and access to, information
- Physical, information and personal security, including identity management;

(5) s33(a)(i) [redacted] and its implications for the Secret level ICT infrastructure and assets.

s33(a)(i) [redacted]

8. A number of these issues are being addressed under the *National Security Information Environment Roadmap: 2020 Vision* [NSIER] or other initiatives, while others have not yet been addressed in a coordinated fashion across the NSCy. As they will impact on the future architecture and functionality of the Secret Domain, they will need to be addressed and resolved in Domain planning. But they will not be considered further in this paper.

Vision for the Secret ICT Domain

9. The vision for the Secret Domain is in accord with the NSIER. Specifically, the objective of Secret Domain ICT planning is to provide effective support to current and anticipated Government business as efficiently as possible, with the following key elements:

- A harmonised policy and legislative environment;
- The ability to access and share information and cooperate from the desktop with partners across government and industry and international counterparts;
- Real time collaboration and coordination using increasingly standardised tools and applications;
- An interoperable, secure and reliable ICT among and between all classification levels, with a single computer screen and keyboard per desktop so users can switch between classification domains;
- Nationally consistent interoperability standards, supported by mutual recognition of security clearances, consistent identity management and access controls, and a single security classification nomenclature;
- Focused ICT investment that aligns with government priorities, represents best value for money, and enhances interoperability domestically and internationally.

10. This represents a challenging vision, not only for WOG ICT but also for the Secret Domain. Developments since the endorsement of the NSIER vision also provide an opportunity to update and develop this vision further. In that context,

s22 [redacted]

useful information is available s33(a)(i) & s33(a)(iii) [redacted]

11. Broader, whole-of-government initiatives are also beginning to have some impact in the Secret Domain, in terms of greater standardisation and rationalisation of infrastructure, applications and tools. Such initiatives include policy and technical advice from AGIMO, the implementation of the findings of the Gershon Review, and the establishment of the position of NSCIO and the subsequent Cabinet endorsement of the NSIER.

- Further detail might be added here, in subsequent papers, on the ICT Vision and the Government's response to Reinecke.

12. A particularly important recent impetus for planning in the Secret Domain has been the broadening conception of national security since 2001 and new arrangements introduced following the PM's statement in December 2008. This has led to structural and business process changes within the Australian Government to anticipate, prevent and respond to a greater range of threats to national security, and to a greater focus on close cooperation with other jurisdictions and sectors – including state and territory governments, the private sector and the community in general. The full implications of these developments are still being identified, and have not yet been fully incorporated into business and ICT planning.

s33(a)(i) [redacted]

14. The s33(a)(i) systems operate a diverse range of applications and tools; often discrete communication channels to different agencies; a variety of data protocols

s22 [redacted]

[although the data standards have many elements in common]; differing information management regimes; and differing rules on system security and connection to other systems.

s33(a)(i) & s33(a)(iii) [redacted]

16. While they are owned and managed by different agencies, the s33(a)(i) [redacted] ICT systems are not completely discrete. More recently, there has been a greater [although still largely informal] effort, consistent with the s33(a)(i) [redacted] NSIER principles of governance, to coordinate the further development of the different systems, and to encourage agencies newly operating at the Secret level to obtain an ICT service from an existing provider.

s33(a)(i) [redacted]

17. There are particular information management challenges associated with the separate systems:

- s33(a)(i) & s33(a)(ii) [redacted]
- s33(a)(i) [redacted]
- s33(a)(i) [redacted]
- Additional agencies are likely to seek to establish the capacity to conduct business at the Secret level, or transition elements of their existing HP/P system to a Secret system.

18. Once all information sources are identified, the following key steps are required for a comprehensive information management system at the Secret level:

- Defined data structure – data standards/protocols
- Agreed business processes for the capture of data and its entry onto defined systems

- The capacities to discover and to access or retrieve the data s33(a)(i) [redacted] – either directly or through community data repositories
- The capacity to assess and analyse the data – facilitated by mining, visualisation, linkage and predictive tools.

19. Overall, the technology issues, for the Secret Domain and its interfaces with other systems and domains, appear relatively straightforward [although perhaps not always simple to achieve]. The major and most difficult issues remain related to business planning and processes, and to culture and behaviour – ranging from an excessive agency focus on the immediate and urgent [busyness] at the expense of strategic planning, to continuing siloed development of ICT capability, to cultural barriers to the sharing and management of information across agencies and jurisdictions.

Further Development of the Secret Domain

20. As with the issues identified across the multiple domains, a number of the issues identified for the Secret Domain are currently being addressed under the NSIER and other initiatives. These include:

(1) Identity management
(2) Common security clearances and standards
(3) Data standards and protocols
(4) Overall information management governance arrangements
    - There are numerous actors and committees related to information policy, information management and ICT across the Australian Government – and more involved in cross-jurisdictional issues. Roles and responsibilities for information management in the Secret Domain should be articulated clearly.
    - The Reinecke Review identifies simple and effective governance arrangements as one of two critical areas for reform. It found that current governance arrangements [from Cabinet down] are not producing the appropriate business focus, clarity of vision, or supporting strategies to drive WOG reform.

21. The following paragraphs address the additional major issues identified for consideration under this review of the Secret Domain ICT.

<u>Stronger central planning, management and development of the Domain</u>.

22. Enhanced planning and management of the Domain has the potential to deliver a more effective and efficient ICT service, through common approaches to and coordination of upgrades and refresh of technology; rationalisation of infrastructure, data holdings and applications and tools; and enhanced interoperability. Specific measures might include:

- Establishing agreed governance arrangements for the Domain
    - Planning, policy setting, management and coordination
- Developing an agreed vision, strategy and capability plan, with the desired business improvements for each stage described
- Promoting and ensuring compliance with strategic directions and standards
- s33(a)(i) [redacted] greater standardisation and integration of the Domain.

s22 [redacted]

23. In simple terms, the three layers of an ICT system are the infrastructure or transport layer; the data management layer; and the desktop or presentation layer [applications and tools]. Initiatives to federate the Secret Domain systems and capabilities would logically best begin with the infrastructure layer, where there is currently the least diversity between the s33(a)(i) [redacted] Secret systems, and then progress to each of the data and application layers. Such a progression is presented at Attachment A.

- Such a strategy would de-risk the transition to a more federated Secret Domain, through progressive implementation and proving of changes.

Infrastructure Layer

24. The infrastructure layer can be broken down further into the following major components:

- Wide area or long distance transport
- Metropolitan area transport
- Major hardware such as servers
- Additional hardware such as routers and encryption devices.

Attachment B provides an overview of the existing Secret Domain infrastructure.

Wide Area Transport

25. Generally, wide area or long distance transport for the current Secret networks is provided by private sector companies [telcos], through fibre-optic cable. s33(a)(i) [redacted]

s33(a)(ii) [redacted]

- s33(a)(i) [redacted] in concept, relatively simple. As current contracts with providers expire, service provision could be transitioned to a smaller number of providers or even a single provider. Alternatively, the Commonwealth might seek to use the bargaining power of its overall volume of business to negotiate better value for money service provision from one or more providers – currently, each network negotiates its contracts independently, with duplicated, under-utilised links to many major centres.
- Such s33(a)(i) [redacted] would require a detailed understanding of whole-of-government business requirements, for locations and capacity, both currently and for any surge or additional requirements for disaster or emergency management [that is, increased capacity or links to additional locations].

s33(a)(i) [redacted]

26. Currently, there are three principal providers of long distance transport communications services to all major centres in Australia – s33(a)(i) [redacted]

s33(a)(i) [redacted]

s22

s33(a)(i)

[redacted]

27. This picture is complicated further by the different approach of s33(a)(i)

[redacted]

- DoFD advised that discussions have commenced with AG's for the MCN and the ASN to share communications links, with the MCN proposed to be responsible for links to Commonwealth agencies and the ASN responsible for links to State agencies.

28. This data suggests that there is capacity, subject to further analysis of surge implications, s33(a)(i)

[redacted]

Metropolitan Area Transport

29. Further work needs to be done to separate more carefully different elements of metropolitan area transport – for example, within the capital city, within a suburb, within a building complex, and within an agency [the last usually being referred to as the local area network]. In some cases, these elements involve a number of different communications link owners.

30. Metropolitan area transport is currently provided s33(a)(i)

[redacted]

s33(a)(i)

[redacted]

Hardware

31. Further work needs to be done to identify the major elements of infrastructure hardware for the s33(a)(i) systems. s33(a)(i)

[redacted]

s22 [redacted]

- It may be more appropriate to group some hardware such as routers and encryption devices with the transport, depending on the point at which traffic is routed and encrypted.
- Further advice is needed on COMSEC and TRANSEC issues s33(a)(i) [redacted]

Data Management Layer

32. The s33(a)(i) Secret system agencies own and manage a large number of systems for the collection, management and storage of data, using a variety of data management standards and protocols. Attachment F provides an outline, but there is no clear view of current data management and storage, the servers and applications used, data storage capacity or the scope for federation, rationalisation and cost saving. Further work needs to be done to identify clearly the data management regimes of the s33(a)(i) systems.

- In general, data resides with the applications on the system servers, with data standards being specific to the application being used.
  - A number of agencies have different initiatives in train for data management. s33(a)(i) [redacted]
- The use of a variety of data standards and protocols may not necessarily be a significant issue. s33(a)(iii) [redacted]
  The critical issue is the commonality or compatibility between the various standards – and, principally, whether they require the inclusion of a minimum common set of metadata [such as source, place, date, and time].
- s33(a)(i) [redacted]
- Access to data for authorised users is relatively straightforward. Identification and discovery of relevant data are more difficult, particularly across networks and across jurisdictions, and require further investigation.

33. With sufficient commonality of metadata and data standards, progressive synchronisation of data holdings [either actually or virtually] is possible. An enhanced [and rationalised] suite of data management tools [such as exploitation, visualisation, presentation, and storage and retrieval tools] could then be provided across the Secret Domain. Significant savings appear achievable in data storage costs, both within agencies and across communities.

Desktop Layer

34. Network owners and agencies currently own and operate a very large number of different applications and tools. Most agencies have invested, over many years, in the "look and feel" of their corporate ICT and the applications to support their business processes. Retention of an independent corporate ICT identity will likely be a significant consideration for agencies. Rationalisation of applications and tools, if

agreed, would likely take some considerable time, given the close linkages with long-standing agency business processes, significant data holdings and current licences.

35. At Attachment G is an initial, high level description of the Secret Domain application layer. Attachment H describes the ICT services each of the s33(a)(i) Secret system providers s33(a)(i) [redacted] deliver to the other agencies they service. But, again, there is no detailed information available on the desktop or application layer across the Secret Domain.

- There does appear to be significant scope for federation and rationalisation of the applications and tools provided at the desktop. s33(a)(i) [redacted].

Options for network service provision in the Secret Domain.

36. Broadly, there are s33(a)(i) options for the provision of network services in the Secret Domain – the status quo; s33(a)(i) [redacted] together with a plan and timetable to transition to that service provision.

37. Service efficiency and effectiveness would suggest s33(a)(i) [redacted] particularly since most of the systems are relatively small scale with small numbers of users. s33(a)(i) [redacted]

- As an initial step, the NSCy could readily move to s33(a)(i) network service providers, based on the following:

s33(a)(i) [redacted]

- The current s33(a)(i) [redacted] The s33(a)(i) networks provide an infrastructure and connectivity able to meet the overall information management business needs of the Australian and state/territory governments.

s22 [redacted]

38. A key element of a transition to a reduced number of providers would be to ensure that agencies seeking to establish the capacity to conduct business at the Secret level [or transitioning from the HP/P system to a Secret system] use one of these s33(a)(i) service providers for their ICT.

- Under the arrangements suggested above, agencies would in the first instance s33(a)(i) [redacted]
- s33(a)(i) [redacted]

39. A reduction in the number of network service providers would assist in reducing the number of outstanding systemic issues related to governance, business processes, and the diversity of applications. Such issues would be negotiated and resolved in the process of developing a service agreement with one of the s33(a)(i) providers.

- s33(a)(i) [redacted] of network service providers would also make it easier to coordinate the direction and timing of future development of the Secret Domain.
- s33(a)(i) [redacted]

A Single Provider of Secret Level Network Services?

40. Further consideration should be given to moving to s33(a)(i) [redacted] level network services to all Australian Government departments and agencies. A transition to s33(a)(i) [redacted] Alternatively, s33(a)(i) [redacted]

41. The following are the principal arguments s33(a)(i) [redacted]

- This would facilitate coordinated, holistic and systematic planning, development and management of the Secret Domain
  - It would provide a s33(a)(i) [redacted] discussions on the provision of ICT support for its business needs, and simplify action to address governance and business process issues
  - It would facilitate decision-making on priorities and resource allocations
  - It would simplify Domain governance arrangements, and responsibility and accountability
  - It would assist in harmonising information handling and sharing protocols across agencies
  - It would simplify security of the Secret Domain and the information held within it, and provide greater assurance about that security
  - It would simplify future upgrades or technology refresh, and better "speed to market"

s22 [redacted]

- It would provide greater value for money for the current investment in ICT, and increased efficiency, through:
  - A reduction in transport and other infrastructure costs [through rationalisation and removal of existing duplication and unnecessarily large spare capacity in multiple systems]
  - A reduction in overall ICT management and service costs
  - A better return on investment through pooled resources and economies of scale
- It would enhance the ICT service and support to smaller agencies which currently have a lower level of provisioning – through sharing the greater current capability of larger agencies. It provides a framework for smaller, and additional, agencies to enhance the quality of their ICT support, for a relatively limited cost – and for those agencies to acquire the capability through operating expenses rather than major investment [a useful argument in a "no new funding" environment].
- It would facilitate the management of ICT interaction/connectivity with the states/territories
  - It would provide a s33(a)(i) [redacted] point of contact/interaction
  - It would provide better coordinated and easier reach into both the Australian Government community and the State/Territory agencies
- It would facilitate management of ICT s33(a)(i) [redacted] by providing a single point of contact and authoritative advice
- A single provider of the infrastructure layer would facilitate the next step of better coordination and rationalisation of the data management layer.

42. The following are the principal arguments s33(a)(i) [redacted] level network services:

- Agencies are concerned or unconvinced about the likely resulting quality of service – because of doubts either about the capacity of s33(a)(i) [redacted] or about the likely responsiveness of the single agency in the event of problems, changes or crises
  - An element of this is a concern that the provider will focus on the major issues or functions [or politically sensitive matters] and give less attention to other needs

s33(a)(i) [redacted]

- s33(a)(i) [redacted]
- s33(a)(i) [redacted]

s33(a)(i)

- Smaller agencies may believe that their ICT will cost more, either because the single supplier will provide a level of service with greater functionality or complexity than those agencies need or because the supplier charges too much
  - For example, the single supplier may seek to amortize all of its costs, including overheads, through its charges to other agencies.
  - From initial advice received from the network providers, there are significant differences in the costs charged to other users s33(a)(i)
  - Agencies would require assurance that the current and future cost of the ICT service is reasonable and value for money. Such assurance might be provided through the use of cost comparison charts, benchmarking or independent assessment.
- It is argued that the principal business functions of agencies in the Secret Domain are too diverse for a move to one service provider to be sensible
  - This might be countered by having a single provider of infrastructure and data management, with the diversity of business supported through the required applications and tools
- There are concerns in the agency likely to s33(a)(i) service that this is a "poisoned chalice" – a lot of additional work and responsibility, and likely tension and criticism [common to ICT service provision] for little evident return or benefit
- There are concerns about business continuity and assurance of ICT with a single network provider s33(a)(i)
  - The counterpoint would be that business continuity planning is facilitated s33(a)(i) compared to the current arrangements in which the plans of respective providers and agencies are not fully coordinated or visible to each other.
  - The s33(a)(i) provider could plan and develop the required system redundancy.
- It is argued that there is not any good precedent for such s33(a)(i) service provision working well [at least in the early stages]

s33(a)(i)

- The trend over recent years in the Australian Government has been to decentralisation and devolution of authority and responsibility for departmental functions. Central oversight has consisted of policy guidance and direction

[for example, participation in centrally managed panels of service providers], rather than central provision of services.

- s33(a)(i)
- s33(a)(iii)

Implement practical measures for immediate enhancement of interoperability

43. Independently of the decision on the number of network service providers, there are a number of practical measures which can be implemented quickly to address identified problems. Attachment I outlines the current state of the overall Secret level ICT capability.

s33(a)(i)

Continue planning the further development of the capacity to reach, engage, and share information with other jurisdictions.

s33(a)(i)

- Develop the capacity [plans, processes and technology] to engage or integrate new agencies into national security arrangements temporarily for specific issues or crises. These may be Australian Government or State/Territory agencies, or in some cases private sector organisations. In these cases, there is a need for short-term, rather than ongoing, connectivity and information sharing.
- A particular area of focus should be communities of interest which straddle traditional boundaries between jurisdictions – eg domestic/foreign,

s22 [redacted]

national/state/local, public/private. s33(a)(i) [redacted]

- s33(a)(iii) [redacted]

Further, broader initiatives which might be investigated

45. As part of the coordinated planning and development of the Domain, further broader initiatives might be investigated:

- Encourage and, where practicable, mandate agency re-use and sharing of ICT assets, licences and applications.
- Develop and share expertise in ICT planning, procurement and implementation – for example, through the development of an ICT procurement toolkit and shared staff skills/training packages.
- Develop more sophisticated performance measurement and benchmarking.
- Develop an explicit statement of risk management policy – related to the protection of information, systems, sources and methods.
- Develop information management and sharing communication programs, to raise awareness, especially amongst the staff of "non-core" agencies.
- Establish a [virtual] team to scan the horizon for, and analyse/assess the benefits of, new and emerging technology – including, for example, with cloud computing.
- Establish, perhaps in cooperation with a supplier, an ICT testing environment where agencies can test updated or new products to ensure fit and compatibility with the planned Secret Domain.
- Establish central oversight and clearance of all ICT expenditure on the Secret Domain, to ensure that developments and new acquisitions accord with WOG strategic plans and objectives.

46. Two broader areas warrant further consideration. Firstly, a more formal review might be conducted to identify the information needed to support the various communities of business operating at the Secret level to which different agencies belong [for example, counter-terrorism, border management, passenger analysis or transport security], the sources of that information and the means by which it will be harnessed.

- There must be a high level of confidence that all data from all relevant sources is able to be identified and is available for integration, analysis and transmission so that a timely operational response is possible.
- s33(a)(i) [redacted]
    - A team of community members might investigate the NS environment to identify the highest risk areas, in which the need for better information management is most urgent.

s22 [redacted]

- In some cases, it appears that the sharing of relevant information might be constrained by legislation or agency practice
  - s33(a)(i) [redacted]

47. Secondly, further attention might be given to simplifying, rationalising and standardising Secret-level business processes across agencies, particularly in specific functional communities [such as border management or transport security].

- It is difficult, time-consuming and expensive to provide bespoke ICT solutions [requiring tailoring of OTS applications or writing of code] for unique or excessively complicated agency processes. Unique agency processes are also a fundamental barrier to the rationalisation of applications and tools.

s33(a)(i) [redacted]

Attachments:

s33(a)(i) [redacted]