POLICY ANALYSIS ASPI

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

51

Information Sharing in Australia's National Security Community

by Kelly O'Hara and Anthony Bergin

27 November 2009

The importance of information sharing

To improve decision making, information sharing is critical to Australia's national security: personnel across government agencies must share information in order to understand and respond appropriately to threats across the security spectrum. Progressing information sharing is therefore a vital means to protect Australia. It should be a high priority for improving our national security.

As outlined in the Prime Minister's National Security Statement issued in December last year, greater interoperability, integration and collaboration are central to the Australian Government's approach to national security.

The Smith Review of *Australian Homeland and Border Security* presented to the federal government in June last year emphasised this approach. It rejected the idea of a US style Homeland Security Department, but argued for better coordination among existing agencies and better mechanisms for strategic planning. And it stressed the importance of information sharing to achieve a more joined-up security community.

The Review found that information sharing in the national security community wasn't fulfilling the needs of agencies gathering and disseminating security information. Smith found that: 'While there have already been significant improvements in access to national security information, some legislative, technical and cultural barriers to information sharing—within and between governments and the private sector—remain.'[1]

Different approaches to security classification and vetting by agencies undertaking their own security vetting, as well as legal problems sharing material related to criminal prosecutions, were presumably canvassed in the Smith Review.[2]

Smith recommended that failure to share information should be addressed by a National Security Advisor, supported by a newly created position of a National Security Chief Information Officer.

The Smith Review followed a damning report in March last year into how the AFP worked with its partner agencies on counter-terrorism investigations. The Street Review found serious problems in information sharing between the Australian Security Intelligence Organisation and other national security agencies, including the AFP.[3]

The Street Review made recommendations relating to enhanced information technology systems and information sharing. As a result, there's now a new Joint Operations Protocol between ASIO and the AFP for regular exchange of information.

The appointment of a National Security Chief Information Officer in April this year marks the start of a reform agenda that aims to achieve a 'harmonised policy and legislative environment [that] will support the smooth flow of people, ideas and activities across boundaries' by 2015.[4]

The National Security CIO's role is to provide direction, co-ordination and oversight of the national security community's information communications technology architecture and strategy. The position is part of the National Security and International Policy Group within the Department of the Prime Minister and Cabinet, reporting to the National Security Advisor.

The appointment of the National Security CIO comes at a time when the Gershon Review of the government's use of ICT has placed pressure on Commonwealth agencies to rationalise their technology budgets. As a result of the Review's findings, large government agencies are being asked to find ICT savings of between 10-15%, while smaller agencies need to find between 2-5%.[5]

But it's not new

The information sharing agenda—that emerged out of counter-terrorism reforms after 9/11—is still relevant whether the question is about critical infrastructure protection, border security, serious organised crime, cyber security, counter-proliferation or biosecurity threats.

The good news is that a number of initiatives on information sharing have been introduced in recent years:

- The *Trusted Information Sharing Network* (TISN) was established in 2003 for the owners and operators of critical infrastructure to share information and work together on the security issues that affect them. It's hosted by the Attorney-General's Department.

- The *Critical Infrastructure Advisory Council* is a part of TISN and oversees the work of advisory groups, provides advice to the Attorney-General on infrastructure protection and feeds into counter-terrorism arrangements.

- The *National Threat Assessment Centre* was established to better address counter-terrorism in 2004. Hosted by ASIO it monitors, collates and analyses all threat intelligence available to the government. Integration is achieved through seconding staff from other agencies in the security community.

- A *Cyber Security Operations Centre* was created this year within the Defence Signals Directorate with staff from Defence, the Defence Science and Technology Organisation, Attorney-General's, the AFP and intelligence agencies. It will support ADF operations and respond to cyber incidents in other departments and advise on critical infrastructure protection.

- In November this year the Attorney-General, Robert McClelland announced the creation of a new government-owned *Computer Emergency Response Team*, CERT Australia. It will take over and expand the work formerly done by GovCERT on information sharing with private firms on cyber security issues.

Australian Government Information Management Office's whole-of-government agenda

For at least the last five years AGIMO has been exploring coordinated information sharing in government. Their work to date has been mainly focused on service delivery for the public. Is hasn't at this point specifically examined national security agencies.

In 2004 AGIMO produced, *Connecting Government: Whole of Government Responses to Australia's Priority Challenges.* The study included best practice case studies of effective coordination and information sharing.[6]

AGIMO's 2006 report on the *Australian Government Information Interoperability Framework*, addressed the drivers, benefits, and barriers to information interoperability across government. The vision was for information held by government to be 'valued or managed as a national strategic asset…'.[7]

The vision would be enabled by a culture of trust; agreed authoritative data sources; common business language/standards; appropriate governance structure; an understanding of the legal and policy framework and tools for information sharing.

In August this year, AGIMO released the *National Government Information Sharing Strategy*. It focused on information sharing as the key to improving the delivery of services to the broader community.[8]

AGIMO's work on information sharing and information interoperability across government has identified obstacles to change in the areas of privacy, policy, leadership and bureaucratic culture.

Information sharing vision

Earlier this year the National Security CIO released a short document outlining the strategy and principles to guide how the national security community can be more cooperative, integrated and effective.[9]

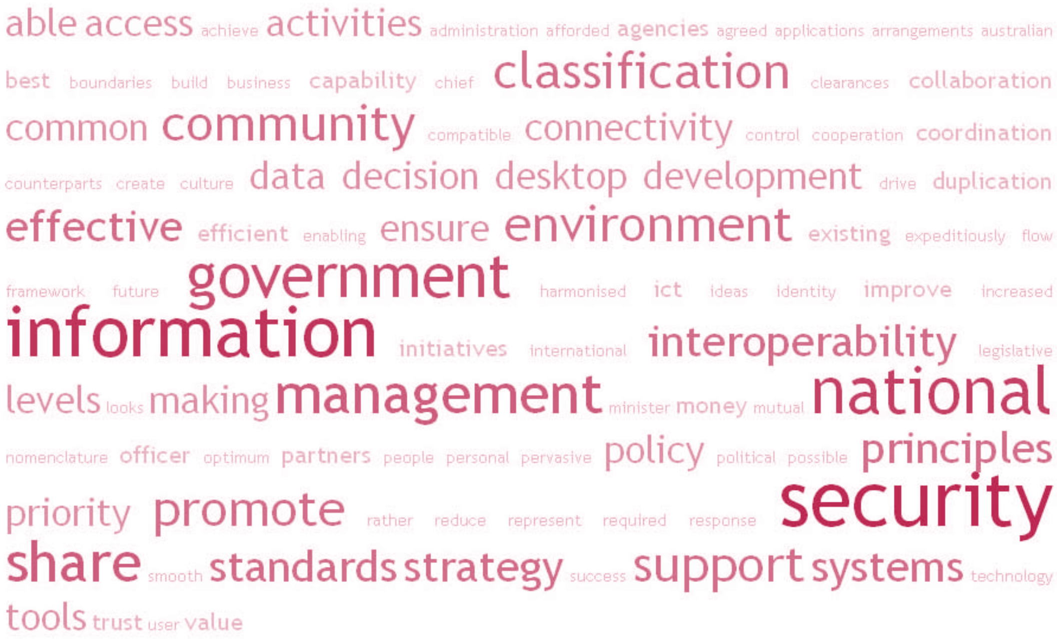
All members of the national security community will be able to: *access and share information and cooperate from their desktop with their partners across government, industry and international counterparts using interoperable, secure and reliable information and communications technology among and between all classification levels.*

The system will also: *support the expanding national security community and the increasing need for improved, real-time collaboration and coordination. There will be interoperable and increasingly standardised tools and applications. There will be secure physical connectivity at all classification levels. Agencies will also share fielded ICT solutions more readily to reduce duplication and costs and improve time to market*.

There will be an agreed information management governance framework underpinned by nationally consistent interoperability standards. The CIO noted that: *This will be supported by a culture of trust and cross-agency mutual recognition of personal security clearances, identity management and access controls and a common security classification nomenclature*.

It's clear from the vision statement that the overall objective in connecting-the-dots very sensibly goes beyond focusing on secure email connectivity between agencies.

A word analysis of the National Security CIO's vision document and another pithy statement issued by the CIO'S office, *Approach to National Security Information Management*[10] is shown below as a word cloud. Word clouds are useful for highlighting words that appear more frequently in the source text. [11]



The cloud indicates how the Prime Minister's Department is trying to improve information sharing policy: the focus appears to be about information management and technology. There's much less emphasis on the human dimension—relationships, trust and leadership.

Next steps in advancing information sharing

Make information discoverable and retrievable

The information sharing system that emerges needs to allow authorised users to discover and retrieve information in the security community.

Fortunately the means to do this are largely readily available in commercially available off-the-shelf technologies.

The Office of the Director of National Intelligence in the United States has recently made policy changes to improve discoverability and retrievability of information. This shift warrants closer study here.

The Office issued a Directive this year that requires the US intelligence community to make all information collected and all analysis accessible by automated means.[12]

Making information discoverable and accessible to authorised users by means of off-the-shelf technology is a goal that should receive high priority in developing Australia's security information sharing framework across the government.

Define the national security community

One of the first questions that should be asked in developing the governance structure for information sharing in the Australian national security community is: *who's in and who's out*?

The breadth of the information sharing vision in the National Security CIO's own statements, suggests that it would be useful to know the agencies that should be working to achieve an acceptable level of information sharing capability. This is critical to the success of any information sharing system.

A scoping study of the national security community would be a good place to start. Mapping the individual information exchanges between groups would reveal the extent of connectivity: who's in the space, capability gaps and the strength of relationships.

For this exercise, the concept of *megacommunities* is an important idea that might help. The building of larger relationship groups involved in solving problems, common to multiple organisations that none can solve alone, suggests we think about the desired national security community as a *megacommunity*.[13]

The power of the megacommunity idea is in the network of groups that emerge and may not have direct ties but are loosely connected through the megacommunity.

The benefit of this concept is that it helps in identifying those agencies outside the Commonwealth that have an interest in security information flows: it more formally recognises stakeholders in the states and the private sector at a time when national security, as outlined in the 2008 Prime Ministerial National Security Statement, is now to be understood as an *all-hazards* concept.

The National Security CIO's own timeline for success is 2015. Given the scale of the challenges, that's an appropriate time frame. And it makes sense to start at the federal level. The mapping task, however, must not neglect the states or business. They hold vital information and perform roles that contribute to Australia's security and national resilience.

Develop metrics

Where does our national security community stand now in moving from a *need to know* to a *need to share* culture?

Information is a key resource for national security decision making. It should be noted that unlike the *Financial Management and Accountability Act 1997*, which sets out the financial management, accountability and audit obligations of Commonwealth agency office holders, there's no *Information Management and Accountability Act* that holds agency heads responsible for their success in information sharing.

An agenda on information sharing with clear outcomes should establish performance metrics to evaluate progress. A gap analysis of current information sharing in the security community would reveal what shape the community is in and set a baseline for future measurement. Australian case studies of best practice in information sharing would be useful here.

There's also international examples which might be drawn upon. The US *500 Day Plan* of the Office of the Director of National Intelligence was evaluated by the ODNI's Inspector General and examined integration and coordination in the US intelligence community since reform began in August 2007. It used surveys, interviews and focus groups to gauge progress against a baseline, over six focus areas including accelerated information sharing and creating a culture of collaboration. [14]

In much the same way, surveys could measure attitudes to information sharing in Australia's national security community. The National Security CIO might conduct a regular audit to determine the extent to which national security community members have reached key milestones in making information discoverable and retrievable. This would enable greater accountability and commitment to the information sharing vision.

Ultimately, the success of the overall structure will be driven by people, not just technology. Effective information sharing relies on trust, goodwill and the creative leadership of members of the information sharing network to forge alliances across agencies.[15]

National security agencies, like most government organisations, will be inclined to address their own priorities first. Sharing will, therefore, need to be rewarded to overcome the tendency for information to be hoarded. Professional training is one important tool in changing the culture of agencies in favour of information sharing.

The Rudd Government has committed to establishing a National Security College in the near future. The College could incorporate training modules on how to advance a *responsibility to provide* culture for senior national security officials.

Establishing a centralised security vetting agency to issue clearances, rather than each agency 'doing its own thing', could also help build levels of trust over time in the information sharing network.

Protect information privacy

The success of the information sharing agenda also depends on having adequate information privacy protections in place.

The Australian community won't have confidence in the system if protections aren't in place to safeguard against inappropriate disclosure of personal information. And without such confidence there will be less support for national security efforts overall. Officials too will be reluctant to share if they don't know if sharing information is appropriate. As AGIMO has recently noted: 'the complexity of privacy laws often results in the default response to requests for information (that might be considered sensitive) as: "We cannot share our information because of privacy laws."'[16]

The Office of the Privacy Commissioner has developed the *4A Framework.* It has been designed to assist agencies consider privacy in their legislative measures specifically relating to new law enforcement or national security powers. It is underpinned by the recognition that measures that diminish privacy should only be undertaken where they are: necessary and proportional to address the immediate need; and subject to appropriate and ongoing accountability measures and review.[17]

The *Privacy Act 1988* contains Information Privacy Principles that cover parts of the private sector, and the personal information handling practices of Australian Government agencies. The Act does not extend to the jurisdictions. The acts and practices of intelligence agencies such as ASIO, ASIS and the Australian Crime Commission are exempt.

The Australian Law Reform Commission has noted in its review of the federal Privacy Act that Australian privacy laws are multi-layered, fragmented and inconsistent.[18] The Rudd Government will move towards national consistency by legislating a set of Commonwealth privacy principles to replace the separate sets of public and private sector principles.[19]

The National Security CIO should work in consultation with the Office of the Privacy Commissioner to develop a transparent national privacy framework of principles to guide information sharing in the national security community.

Privacy contact officers in federal agencies need to work closely with the National Security CIO to ensure that policies are in place to match the expected increase in security information flows.

Harness Web 2.0

Web 2.0 has not been well developed in the national security space to facilitate information sharing. It's commonly associated with public technologies such as social networking sites (e.g. Facebook) or wikis (open-source encyclopedias). Web 2.0 is about creating an effective communication tool out of the web for the purposes of improving knowledge and fostering collaboration.

Examples in the US intelligence community, for example, include the creation of *Intellipedia*, a Wikipedia-style of information sharing and *A-Space*, a type of MySpace for intelligence analysts to connect with colleagues working on similar topics.

Web 2.0 has recently been recognised for its utility in the UK civil service.[20] In Australia, the Minister for Finance and Deregulation and the Cabinet Secretary have commissioned a taskforce, headed by Nicholas Gruen, the CEO of Lateral Economics, to review how Web 2.0 techniques can make non-sensitive government information more accessible and usable, and increase government collaboration with the public.

The Gruen Review took as its starting point the OECD Principles for public sector information which emphasise openness and transparency. The taskforce is also, however, looking at ways of using Web 2.0 tools in emergency management,[21] promoting collaboration across agencies and fostering a culture of online innovation within government.[22]

The Gruen Review's report will be presented to the Minister for Finance and Deregulation later this year. Its findings should be drawn into thinking about transformation in the national security community information sharing environment.

One example relevant to the national security information sharing framework comes from the Australian private security sector. It has already developed an information sharing network for senior protective security executives.[23] In the public sector a site managed by AGIMO provides a secure web-based space for cross-jurisdictional government agencies to share information.[24]

Concluding remarks

The appointment of Australia's first National Security Chief Information Officer is an important step to achieve progress on information sharing. The security information sharing agenda should be central to achieving a collaborative culture amongst a diverse national security community.

Transformation, however, won't be quick. The ultimate success will come down to the human element: building trust and creative leaders developing processes that encourage information sharing.

It's on this base that the technical components of the information sharing network—getting the right information to the right people at the right time—can be built.

About the Authors

Kelly O'Hara is a research analyst at the Australian Strategic Policy Institute.

Anthony Bergin is the Director of Research Programs, Australian Strategic Policy Institute

Endnotes

1. *Report of the Review of Homeland and Border Security*, 4/12/08, http://www.pm.gov.au/sites/default/files/file/documents/20081204_review_homeland_security.pdf, p3.
2. The full Smith Review is embargoed. Only the conclusions and recommendations have been made public. The issue of security classification of information is governed by the Australian Government *Protective Security Manual*, which is managed by the Attorney-General's Department.
3. *The Street Review: A Review of Interoperability Between the AFP and its National Security Partners*, http://www.afp.gov.au/__data/assets/pdf_file/71833/The_Street_Review.pdf
4. *Approach to National Security Information Management*, National Security Chief Information Officer, http://www.dpmc.gov.au/national_security/docs/strategy_principals.pdf
5. *Review of the Australian Government's use of Information and Communication Technology* (Gershon Review), August 2008 http://www.finance.gov.au/publications/ICT-Review/docs/Review-of-the-Australian-Governments-Use-of-Information-and-Communication-Technology.pdf
6. *Connecting Government: Whole of government responses to Australia's priority challenges*, Management Advisory Committee Report, Australian Public Service Commission, 2004. http://www.apsc.gov.au/mac/connectinggovernment.htm
7. *Australian Government Information Interoperability Framework*. Australian Government Information Management Office, April 2006, p4.
8. *National Government Information Sharing Strategy*, Australian Government Information Management Office, August 2009. http://www.finance.gov.au/publications/national-government-information-sharing-strategy/docs/ngiss.pdf

9. *Enabling Optimum Decision and Response: Australia's National Security Information Environment–What success looks like*, 15/6/09, http://www.dpmc.gov.au/national_security/index.cfm
10. *Approach to National Security Information Management*, http://www.dpmc.gov.au/national_security/docs/strategy_principals.pdf
11. Image from http://tagcrowd.com
12. Office of the Director of National Intelligence, United States. Intelligence Community Directive number 501: *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, effective 21 January 2009. www.dni.gov/electronic_reading_room/ICD_501.pdf
13. Gerencser, Mark., Fernando Napolitano, and Reginald Van Lee. *Megacommunities Manifesto*, 7/3/08. http://www.changethis.com/44.02.Megacommunities
14. *500 Day Plan Follow-Up report*, Office of the Director of National Intelligence, United States. http://www.dni.gov/500-day-plan/500%20Day%20Plan%20Follow%20Up%20Report%20part%201.pdf
15. For an analysis of the qualities needed for leaders to bring together organisations or people to forge alliances and create unusual opportunities see: Judi Neal, *Edgewalkers: People and Organizations That Take Risks, Build Bridges, and Break New Ground*, Wesport: Praeger Publishers, 2006.
16. *National Government Information Sharing Strategy*, Australian Government Information Management Office, August 2009. http://www.finance.gov.au/publications/national-government-information-sharing-strategy/docs/ngiss.pdf, p.11
17. *Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009 [Provisions] Submission to the Senate Legal and Constitutional Affairs Committee*, Office of the Privacy Commissioner, August 2009. http://www.privacy.gov.au/materials/types/download/9385/6923
18. *Report 108: For Your Information: Australian Privacy Law and Practice, Australian Law Reform Commission*, May 2008. www.austlii.edu.au/au/other/alrc/publications/reports/108/3.html
19. Australian Government First Stage Response to the Australian Law Reform Commission Report, *For Your Information: Australian Privacy Law and Practice*, October 2009. http://www.pmc.gov.au/privacy/alrc.cfm
20. *The Power of Information Taskforce Report*, February 2009, http://powerofinformation.wordpress.com For an analysis on how the web can facilitate collaborative thinking, see: Charles Leadbeater, *We-Think: Mass Innovation, Not Mass Production*, Profile Books: 2008.
21. Emergency 2.0, Government 2.0 Taskforce, http://gov2em.net.au/
22. Government 2.0 Taskforce, Towards Government 2.0: An Issues Paper, July 2009. http://gov2.net.au/consultation/2009/07/23/towards-government-2-0-an-issues-paper-final/
23. http://www.secman.com.au
24. Australian Government Information Management Office, Department of Finance and Deregulation, https://www.govdex.gov.au/

About Policy Analysis

Generally written by ASPI experts, **POLICY ANALYSIS** is provided online to give readers timely, insightful opinion pieces on current strategic issues, with clear policy recommendations when appropriate. They reflect the personal views of the author and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI
Tel + 61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au