INVIGORATING SCIENCE AND TECHNOLOGY FOR NATIONAL SECURITY

This submission is Professional Scientists Australia's response to DSTO's invitation to provide comments and feedback on the policy and program which will articulate Government's strategic direction for National Security Science and Technology (S&T) over the next decade.

About Professional Scientists Australia

Professional Scientists Australia is a division of Professionals Australia (formerly the Association of Professional Engineers, Scientists and Managers, Australia). We represent several thousand professional scientists from a broad range of specialisations including health science, automotive design, biomedical science, ecology, veterinary science, neuroscience, mental health, genetics and genomics, astronomy, biochemistry, mineral processing, environmental science, defence research, synchrotron science, environmental science, immunology and water science.

Professionals Australia is an organisation registered under the *Fair Work Act 2009* representing over 25,000 Professional Engineers, Professional Scientists, Veterinarians, Architects, Pharmacists, Information Technology Professionals, Managers, Transport Industry Professionals and Translating and Interpreting Professionals throughout Australia. Professionals Australia is the only industrial association representing exclusively the industrial and professional interests of these groups.

Professional Scientists Australia promotes the views of their scientist members on a wide range of policy issues to government, industry and the community.

We have three objectives:

- to provide a strong voice for professional scientists. This includes considering the kind of support, policies and practices at the enterprise and structural levels that will be necessary to create a sustainable science workforce capable of realising optimal levels of innovation, productivity and competitiveness;
- to play a leading role in encouraging dialogue between industry, government and the higher education sector. This means advocating for investment and structural reforms, building the platforms for collaboration and change and initiating and leading projects to foster collaboration; and
- to promote public understanding of science and the key role professional scientists play in ensuring Australia's future. This involves influencing public policy and resource allocation decisions and promoting the value of science to decision-makers and the wider community. We seek to highlight the critical role science plays in enabling productivity and innovation, promoting economic prosperity, protecting the environment, improving human welfare and quality of life and protecting national security. In doing so, we raise the status of the profession and the professionals who work in it.

Professional Scientists Australia
GPO Box 1272, Melbourne, Vic. 3001
e: scientists@professionalsaustralia.org.au
w: www.professionalsaustralia.org.au/groups/scientists/home
t: 1300 273 762

Contents

List of tables

List of figures

Foreword

Professional Scientists Australia acknowledges the challenges facing DSTO in developing a policy and program for invigorating science and technology (S&T) for national security.

We recognise the constantly changing nature of defence and security threats ranging from biological attacks to pandemics to environmental crises to cyber-terrorism, the high rate of change in S&T, the number of agencies involved in national security-related areas, the spread of S&T across a broad range of policy domains and the multitude of funding and collaborative arrangements in place for S&T providers internationally, across federal and state government, industry and multiple disciplines within universities.

We acknowledge the challenges in balancing fiscal prudence and protecting our national security interests. This being said, we hold the firm view that national security should be driven by strategy not finance.

We believe the policy for invigorating S&T for national security should be managed for the long-term and be underpinned by appropriate risk assessment and strategic planning.

Strategic planning for the next decade will include workforce development which ensures the maintenance and updating of the S&T skills base and sustained technological and industrial expertise. Building and maintaining research capability must take account of the long lead time needed to develop appropriate levels of expertise and experience. It will rely on effective collaboration between the secondary and tertiary education sectors, industry and government to ensure our long-term STEM capability. The defence workforce must have the agility, depth and in-house skill sets to be able to provide advice on emerging technologies and threats and to support potential new industries, as well as a commitment to transparency and collaboration in order to maximise the use and application of research across different and/or multiple contexts.

Growing a science and R&D workforce with the capabilities needed to support national security over the next decade will also require stable, strategic and sustainable investment in science and R&D and the development of world-class infrastructure to support it. Sound independent research saves money and most importantly lives and reputation. Ensuring that there are sufficient skilled, experienced professionals within DSTO is essential and underpins both professional and technical integrity.

Now more than ever we need a strong and growing S&T sector. An advanced S&T capability will be critical to protecting the safety and security of our nation and its citizens, and safeguarding our infrastructure and national resources from threat. It is our responsibility to maintain and strengthen our national security capability.

We thank the Department of Defence for the opportunity to have input into this consultation process.

Chris Walton
CEO, Professionals Australia

Robyn Porter
President, Professional Scientists Australia

Purpose of this document

We consider it critical that our members are consulted about policy and program issues in the areas in which they work – in this case, in relation to S&T for national security. Our member consultation comprised an online survey which mirrored the structure of the NSSTC consultation paper. It was our intention to provide feedback on the specific questions asked in the paper and any other significant issues raised by members in relation to S&T and national security.

Background

Section 1 – The role of science and technology in Australia's national security

Imperatives or drivers that justify the creation of a national security S&T policy

The survey asked members if there were any imperatives or drivers that justified the creation of a national security S&T policy in addition to those identified in the consultation paper. Our members are well-positioned to comment on such imperatives and a sample of the answers submitted is set out in Table 1:

Table 1 - Imperatives or drivers that justify the creation of a national security S&T policy

a.	Having leading S&T capabilities and infrastructure are critical for providing flexibility of responses to the diverse and ever-changing threat landscape. Policy-makers can be provided with more evidence-based options to counter threats. They also provide a multiplier effect by stimulating industries through innovation. A healthy S&T infrastructure should have a strong base in both the public and private sectors (as is the case in many countries such as Germany, Sweden, Israel, US, South Korea and Singapore).
b.	S&T is available to all sides of security. Those who invest in S&T have the best chance of meeting their strategic objectives. An S&T policy will allow for better planning which is necessary as an S&T capability can require decades to build and is difficult to recover when lost.
c.	S&T investment results in increased national wealth. S&T innovation creates new value.
d.	S&T is critical to winning any wars or conflicts, not just by being able to adapt more quickly than any adversary in any situation, but by repeatedly or continuously demonstrating that rapid adaptation ability to deter or deflect the adversary before they choose that path.
e.	National security-related S&T will also inform the counter-intelligence agencies of the knowledge domains to be protected against threats. That is, if we don't have a leading S&T program, it will be difficult to know what S&T areas are of value to others' national security S&T and hence are worth protecting.
f.	Only with a national security S&T policy and program will Australia get best practice at affordable cost.
g.	Lemon detection - as DARPA have found over years, their biggest impact on cost saving (justifying their budget many times over) was stopping expenditure on ideas which broke the laws of physics, or were operationally undeployable, or which had high, unexposed risks not mentioned in the glossy sales brochure. Engineering staff are more likely to develop systems (human and machine) which consider feasibility, optimisation, reliability, maintainability and adaptability. Some decision-makers in government and business have no idea of the possibilities and impacts (good and bad) of newer technologies, yet have to make decisions on where to put limited resources. Knowledge and experimentation de-risks investment in the future. STEM staff are best placed to advise and evaluate those options.
h.	Strong investment in S&T in times of significant economic rationalisation strengthens our current and future position in a global community, by providing outcomes that others do not. In doing so S&T provides an imperative advantage that protects Australian industry from external threats in so doing strengthens our economy both in the short and long-term.
i.	We need it so we can develop policy/procedures on getting the people working in these fields recognition and the ability to share information at appropriate security levels. Perhaps memorandum of understanding style agreements between various agencies providing a means of identifying and sharing information.
j.	National self-reliance in defence. In times of war, overseas suppliers cannot guarantee supply of materiel needed to defend our country. If we rely on overseas supply, if our sea lanes and

	supply lines are cut, then the defence of Australia can only be maintained for a limited period of time. This is unless we have a self-sustaining defence sector which can produce the consumables, ammunition and repair parts we need to continue a war. S&T is an essential part of any production capability and is therefore an indispensable part of the defence of our nation if we are to avoid the strategic weakness which our island nation's geographic position places us in.
k.	A national approach to energy security?
l.	I believe the statement should be more explicit as to the fact that S&T is a primary dimension, indeed in some cases the primary dimension, in many national security issues; it is therefore an essential ingredient in addressing them, not an optional extra or secondary consideration. For example Power: The US is the world's dominant military power. The reasons for this lies not in it being the world's richest country, but rather in it having the worlds richest reservoir of S&T expertise and people and its ability to harness that reservoir for military and strategic goals. Similarly Israel has a demonstrated military superiority over its neighbours far beyond what might be expected given the population sizes and GDPs involved, primarily because it has been able to harness national S&T capabilities to provide a substantial technical edge over its opponents. Threats: Most of the threats to national security have a very strong or indeed dominant S&T component. In particular, while prioritising these threats is still very much a work in progress, the emerging consensus appears to be that cyber attack is a very great, perhaps even the greatest threat (see "Guide to Australia's National Security Policy" and the consultation paper cited above. This threat's defining characteristic is the technology by which it is delivered: S&T knowledge and S&T professionals will be essential to combatting it. Alliance: The US alliance is the rock on which Australia's national security strategy rests. In the absence of actual hostilities the primary ongoing benefit of the alliance is the access it provides to US technology and the information collected by US advanced systems, in particular platforms in space. On the reverse side of the coin, the value of Australia's contribution to the alliance depends very much on the degree to which it can be integrated with a technically sophisticated US military system. Thus S&T capabilities and knowledgeable S&T interlocutors are essential to maintaining the alliance.
m.	Australia has a very weak and still weakening manufacturing and engineering sector in all but mining-related domains. Indeed, even in the mining domain design engineering is being sourced offshore. This erosion of the Australian capability to field technology industry is a dangerous long term trend. That is particularly so when our neighbours are undergoing precisely the opposite trend. Defence is one area in which these skills can be maintained. Australia can't call on industry sectors to contribute science and technology advancement in defence. Failure to invest has run the capability in to the ground.
n.	S&T knowledge and experience in these areas is long-term, highly specialised and commercially unviable and accordingly does not exist in the public domain. A competitive edge is only possible if the knowledge and experience is exclusive to the ADF which precludes using commercial consultancies.
o.	We live in a technologically-driven world of extreme and growing complexity - we need to also prepare as much as is feasible for the "unknown unknowns".
p.	Strategic placement within the globalisation trend. IP is the emerging differentiator.
q.	The fact that we are constantly fighting a rear guard action against the exploitation of technological advances.
r.	Assertions 1. It is a high risk security environment 2. Spending money on technology saves money 3. Modelling behaviour is well developed. (In reality predictive tools are limited.) In effect this is one of the current roles of DSTO.
s.	While S&T can make an important contribution a side issue might be that with diminishing investment in science that a national S&T policy could deliver better coordinated scientific input, demonstrate the value of S&T and build a case for investment in other areas. An S&T policy that delivers might aid further collaboration.
t.	More than just defence and security is involved. S&T policy needs to encompass bio-security, actions needed to respond to climate change etc. etc.
u.	Includes all the arguments for non-security S&T.
v.	Employing and valuing engineers and scientists and technicians, who are fundamental to supporting much of the high-technology items that are purchased by Defence for the security of Australia. Keeping things working on a shoe-string budget requires "spending money to save money."

w.	Integrate S&T expertise to address current and future threats in a pro-active manner and aim to neutralise threat drivers in a systemic fashion without waiting for protagonists to take action. This would focus more on off-shore locations where political, social and environmental factors give incentives for threats to Australia's national security.
x.	Ensuring that our activities and equipment are the safest possible while delivering capability.

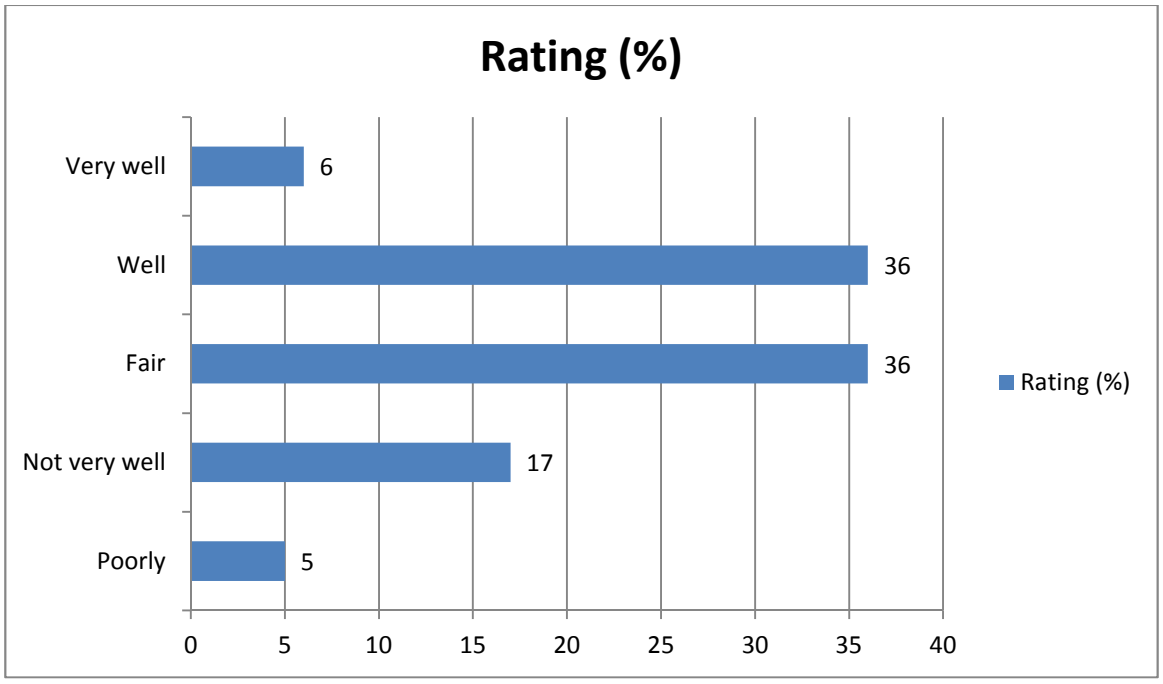
Section 2 – DSTO's role in national security

DSTO's national security role

The survey asked members to make a judgement on how well they thought DSTO fulfils its national security role and to make further comment to explain their judgement

Figure 1 sets out a summary of their responses. A total of 42 per cent of respondents indicated that DSTO fulfils its role in national security well or very well.

Figure 1 - How well does DSTO fulfil its national security role?



Member comments indicated that while DSTO was generally seen as fulfilling its national security role well, there were also a number of issues of concern including:

- stovepiping;
- lack of funding for developing new technologies;
- lack of collaboration;
- failure to develop the next generation of scientists, engineers and technology staff;
- heavy workloads impacting output, low levels of commercialisation of DSTO R&D; and
- lack of industry engagement.

Table 2 sets out a range of comments about DSTO's role:

Table 2 - How well do you think DSTO fulfils its national security role?

a.	DSTO is the right organisation for the role it fulfils in Australia's National Security and Defence.
b.	There needs to be embedded staff in the client agencies to understand and process to determine how S&T can assist them. (These agencies also need to realise that they need a budget for S&T support.)
c.	Recent funding for non-salaries is so small as to threaten the effectiveness of this organisation.

d.	In terms of dealing with client requests for advice, DSTO generally does well, prioritising and handling all OPSTERS (operationally imperative work), most of the high priority work and less of that of lower risk. What we aren't doing much of is the creative, forward-thinking work. Collaboration with our peers (often our only true peers are in UK/US) is stunted compared with 5-10 years ago We aren't developing a raft of younger scientists / engineers / techos to gradually take our places. When many of our most experienced people leave DSTO in the next 5-10 years, the new people coming in will be far less experienced and prepared for the leadership roles needed in this country. We also are bogging our S&T staff down with trivia - sucking the life and energy out of our most creative. Staff are often so overloaded, that there is little time to do things to improve our internal efficiency, learn new technologies and help staff development. Managers frequently express the concern that their workloads don't allow them the space to connect with and manage well - to plan and optimise their team's outputs etc.
e.	The various government departments and agencies involved in national security are stovepiped so in particular it is difficult for them to allocate money to research projects where the outcomes will benefit several agencies rather than just one.
f.	The guys on the ground are doing their job, but they are stovepiped by territorial managers not willing to share information and resources.
g.	To obtain the most of S&T investment in DSTO, then that investment must translate into production of defence materiel through commercialisation of R&D. The end-state should be self-reliance on defence materiel to overcome the large vulnerabilities an island state, located far from allied centres of power finds itself in. Australia is at present totally reliant on sea lanes of supply. This is well-known and acknowledged in our white paper. Due to the sheer size of the sea lanes and the ease with which they can be disrupted, degraded and cut, Australia will never have enough assets to secure these. It would take a world power to do this. The alternative is to reduce reliance on overseas supply by creating a domestic defence industry, tailored to production of the most important requirements and consumables necessary in military activities. The first step is R&D. The next step is transition to production. This is where DSTO could have a huge impact but where current commercialisation of DSTO R&D is at a very low level. When it does occur, more often than not it goes to a company where production is not in Australia hence does not meet the aim of creating a self-sustaining defence force. Furthermore, there is little incentive to commercialise R&D as the revenue goes into government consolidated revenue rather than defence or DSTO.
h.	Industry engagement and investment needs to be built in to a broad security framework.
i.	DSTO is the ideal agency for this role in principal.
j.	DSTO need to be accountable for achieving outcomes.
k.	Do not really have much visibility of what DSTO is doing about this, (despite being in DSTO).
l.	I think very often the S&T advice that DSTO provides is sound, however the translation onto outcomes is very dependant on other entities e.g. DMO, government.

Obstacles

The survey sought member feedback on the main obstacles to DSTO properly fulfilling its role. Respondents identified the areas of budget/funding/resourcing, the lack of long-term coherent S&T and national security policy and lack of a commercialisation strategy as possible obstacles. A selection of comments is set out in Table 3:

Table 3 - Main obstacles to DSTO fulfilling its role

a.	Resourcing has been inadequate and in the current environment seems unlikely to improve. Also DSTO is more focussed on defence and national security is secondary.
b.	Separated from DMO and lacking direction by Defence Minister and Capability Manager.
c.	Lack of resources. Blue/Green/White suit distrust/apathy/ignorance of DSTO's role/capability or viewing DSTO as an impediment to their project. Senior government apathy and ignorance.
d.	Political leaders make decisions that do not appear to have any rational basis whatever. Thus we buy inappropriate US hardware. We might as well not bother.
e.	Too many stakeholders in the decision loop which prevents a clear, consistent and coherent policy from being pursued over a period of time.

f.	S&T is not as highly-regarded in Australian culture which manifests itself by the way DSTO interacts with other agencies. DSTO needs to be viewed as fulfilling a strategic role in Australia's defence policy.
g.	DSTO has no current effective mechanism for commercialising its intellectual property. This is measured through patents, direct ventures, licensing and so on. Whilst DSTO has a commercialisation office, it's doubtful whether it actually pays for itself. Historically successive ministers have held the view that it is not the role of the public service to be involved in profit-making ventures - therefore DSTO should be concerned with only "capability improvement" - there are no effective IP transition processes or measures for DSTO. If DSTO is only to assist in informed technology improvement then get DMO or CSIRO to do that.
h.	Budget.
i.	A defence force that doesn't understand the technologies in the first place and wanting only to buy what they can identify on the internet or what is used by the US.
j.	Funding
k.	Culture - "not invented here" must be better Strategic Directions - lack of vision and "why not" approach Poor organisation - ADF, DMO and DSTO are not organised or resourced as technology developers.
l.	Funding limitations - attracting and retaining high-quality employees and low engagement with other agencies.
m.	Heavy reliance on academia.
n.	Resources $'s and staff.
o.	Resourcing. A lack of a Minister for Science.
p.	Lack of appreciation of the value and personal investment of experienced S&T staff. Lack of realistic and gently expanding numbers of staff to allow for good succession planning and to expand understanding into new areas, and the non-salary budgets to support their work. Travel cuts and barriers (e.g. having to ask permission of the PM). We need encouragement of travel to conferences and international panels to connect with the international community where time and money-saving collaboration can occur. It must be seen as a necessary input investment into having more knowledgeable people. Realistic, long-term guaranteed funding of long-term S&T work. Budgets and flexible accounting rules which extend to 3-5 years so that there is more ability to shift funds in response to arising conditions - to better manage the S&T program.
q.	Under investment in S&T capability programs. The inability to appropriately remunerate Engineers and Scientists for their worth. This leads to an erosion of capability within the organisation.
r.	Defence is generally a receptive and well-informed client for S&T, but in many cases other agencies involved in national security are not.
s.	A ludicrous amount of regulatory requirements that represent the triumph of CYA process over the requirements of reality.
t.	Resources as well as recognition of the importance of our roles in the areas national security.
u.	The two biggest issues are the inability of the infrastructure team to provide IT resources to enable efficient work to be done, and the lack of an administration framework resulting in SME's spending 30% of their day filling in forms unrelated to their work.
v.	Government policy governing direction of DSTO and aim of commercialisation activity + Government leadership in creating a self-sustaining defence force underpinned by a viable defence production industry +. Low knowledge base and skill sets in commercialisation of R&D in defence + Lack of policy and guidance on commercialisation of R&D in Defence.
w.	Inter-agency rivalry and differing priorities.
x.	In my view DSTO's performance is sometimes handicapped by a lack the links with external organisations and networks of contacts to enable them to be effective coordinators. In light of these limitations DSTO's coordination role needs to be structured in a way that does not allow these weaknesses to capture the process, e.g. by channelling the bulk of the available resources into internal DSTO programs, or in the other extreme by arms-length, hands-off funding of external S&T providers. DARPA is perhaps the operational model that the DSTO team undertaking this role might most usefully strive to emulate. Another substantial step towards overcoming the obstacles would be to encourage a greater flow of staff into DSTO from other elements of government, academia, etc., along with a counter-flow of DSTO into other elements of government, overseas partner agencies, etc.

y.	Funding streams are extremely flaky and aimed short-term. DSTO has no discretionary budget whatsoever.
z.	Funding.
aa.	Inadequate resources.
bb.	More national and international collaborations needed.
cc.	Not being fully engaged in procurement decisions and policy development.
dd.	Poor communication and leadership.
ee.	Unclear and changing goals.
ff.	Getting the balance between task work and administration correct. Current balance results in poor productivity.
gg.	The national security program lacks sufficient breadth and depth - it is starved of funds and FTE and as a result is unable to have more than a "watching brief" in some areas, and with large areas of "blank" where no staff or time is allocated to identifying and understanding potential threats.
hh.	Resourcing is heavily constrained.
ii.	Real engagement with the customer and overly restrictive defence policies that prevent comprehensive research from taking place. Policy also prevents DSTO from being a leader and engaging directly with some industry stakeholders.
jj.	The divergent roles of Defence and Foreign Affairs can result in differing requirements.
kk.	Being a scientist does not make you a big picture or innovative thinker or have the ability to understand the customer's needs. In other words the strategic thinking capabilities for this role may be found in other organisations.
ll.	Customer undervaluing long-term research and DSTO undervaluing of operational matters.
mm.	Motivation, raise train and sustain activities + the ability to explore/prove ideas/concepts within the wider scientific community (has it been done, can it be done better or in conjunction with other activities?).
nn.	Lack of suitable funding, changing or incomplete direction from government.
oo.	Lack of grass roots level engagement. It's all done at a high level in Canberra, and local Chiefs and Research Leaders and Group Leaders don't have this role on their radar.
pp.	Budget, vested/political interests.
qq.	Resourcing for research.
rr.	Staff caps, ever-increasing funding cuts, incentives for retention of quality staff.
ss.	Political interference. Decision-making due to non-scientific reasons but trying to appease our so called friendly nations clouds judgement and decision making.
tt.	Short-sighted government.
uu.	Lack of commercial experience and engineering support from DMO.

Section 3 – Challenges faced by national security user agencies and S&T providers

Members were asked to rate in importance the challenges faced by national security user agencies and S&T providers according to the four key areas of user requirements/priorities, S&T support, resources and delivery as set out in the consultation paper.

User requirements

Figure 2 sets out the average rating on a scale of 1-5 where 1 = not important and 5 = very important across the range of indicators for user requirements/priorities. Lack of knowledge of shared problems across organisations and therefore lack of ability to collaborate and/or jointly fund research and development was rated the greatest challenge in this area.

Figure 2 - Average rating - User requirements/priorities

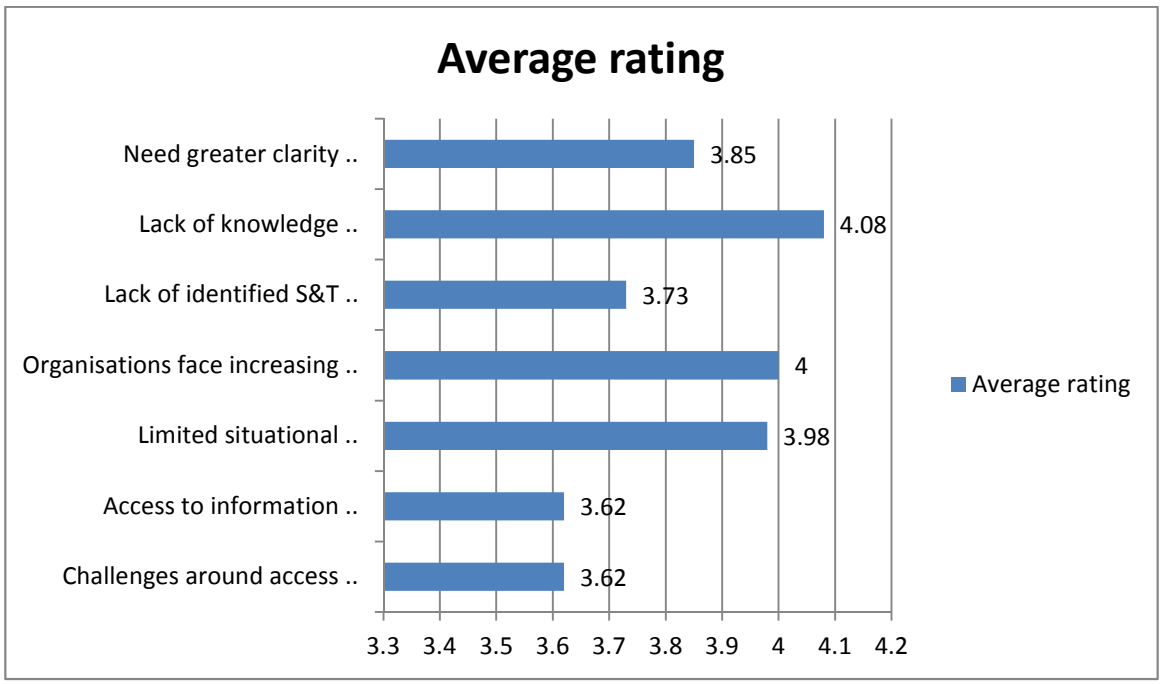


Table 4 - Data summary - User requirements/priorities

Table 4 sets out the percentage breakdown of responses by level of importance across the range of indicators for user requirements/priorities:

	Very important (%)	Important (%)	Fairly important (%)	Fairly unimportant (%)	Not important (%)
Need greater clarity in national security priorities (scope) e.g. traditional, all hazard, national interest; and implications for user agency priorities	27	40	27	4	2
Lack of knowledge of shared problems across organisations and therefore lack of ability to collaborate and/or jointly fund research and development	39	41	14	2	4
Lack of identified S&T opportunities	29	31	27	8	4
Organizations face increasing challenges of keeping up with emerging technologies and minimising new security threats such as in advanced analytics, network analysis and data integration, 3D printing, cyber and electronic security, intelligence including data mining and data management, and border security including identity security	42	35	6	15	2
Limited situational awareness of whole-of-government NS requirements for S&T support	35	33	29	4	0
Access to information (declassified where necessary) on NS requirements / priorities	23	23	45	9	0
Challenges around access to independent S&T advice and support for capability development	28	30	23	15	4

S&T support

Figure 3 sets out the average rating on a scale of 1-5 where 1 = not important and 5 = very important across the range of user indicators for S&T support. Lack of awareness of national security S&T capabilities was rated the greatest challenge in this area:

Figure 3 - Average rating - S&T support

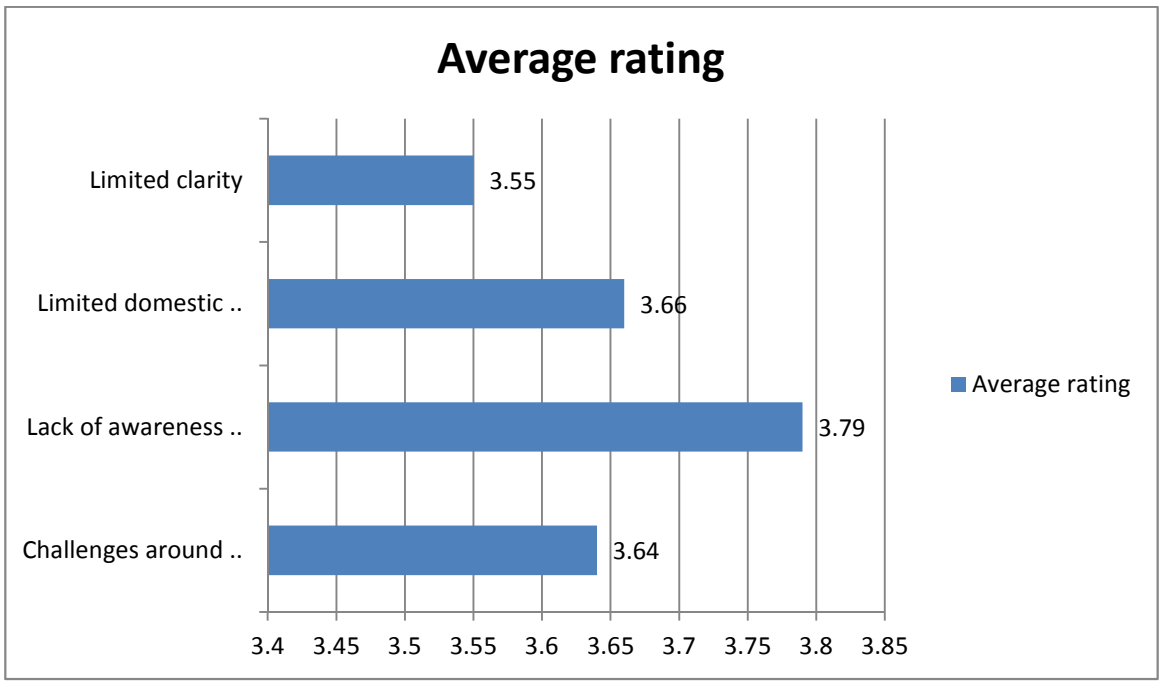


Table 5 sets out the percentage breakdown of responses by level of importance across the range of indicators for S&T support:

Table 5 - Data summary - S&T support

	Very important (%)	Important (%)	Fairly important (%)	Fairly unimportant (%)	Not important (%)
Limited clarity on the S&T programs to meet NS requirements of user agencies.	17	36	34	11	2
Limited domestic S&T development to support new regulatory activities such as air cargo	19	36	36	9	0
Lack of awareness of NS S&T capabilities	28	40	19	9	4
Challenges around access to relevant research data such as developmental or experimental data sets for big data	15	49	21	15	0

Resources - $, FTE, Physical, IT

Figure 4 sets out the average rating on a scale of 1-5 where 1 = not important and 5 = very important across the range of user indicators for resources. Poor funding and resourcing was rated the greatest challenge in this area:

Figure 4 - Average rating - Resources - $, FTE, Physical, IT

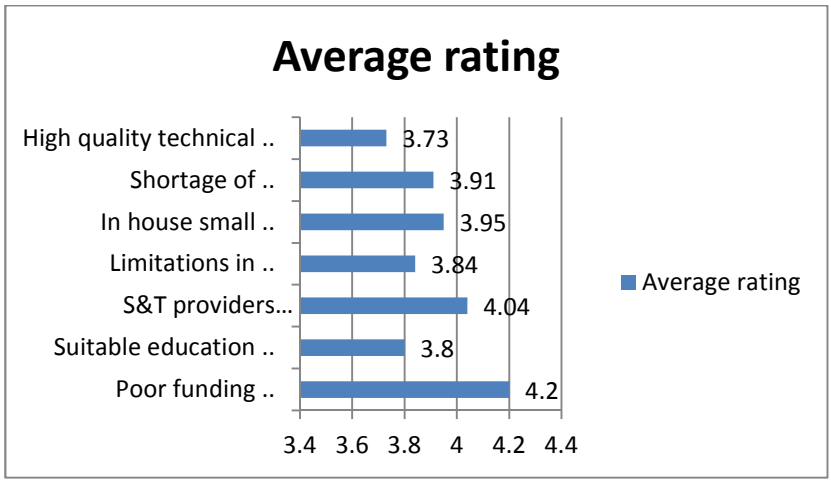


Table 6 sets out the percentage breakdown of responses by level of importance across the range of indicators for resources:

Table 6 - Data summary - Resources - $, FTE, Physical, IT

	Very important (%)	Important (%)	Fairly important (%)	Fairly unimportant (%)	Not important (%)
High quality technical advice and input to policy in key areas such as Chemical and Biological weapons is limited to a single specialist	31	31	27	22	9
Shortage of skilled IT and security professionals	31	40	20	7	2
In-house small analytical staff is stretched and difficulty in tapping scientific specialists to complement in-house staff and can effectively communicate with ministerial audiences	45	30	9	7	9
Limitations in access or owning computational resources and associated skills to undertake mathematical modelling. Yet organisations called upon to nationally coordinate such activity in response to NS incidents	31	36	22	9	2
S&T providers competing (not collaborating) for technical support – academia competes against industry often appearing as cheap labour but then without generating commercially viable or sustainable technological outputs	39	41	7	11	2
Suitable education (skilling) options in emerging areas such as big data is challenging	18	51	27	2	2
Poor funding and resourcing. What is to be delivered is known.	57	22	11	7	4

Delivery

Figure 5 sets out the average rating on a scale of 1-5 where 1 = not important and 5 = very important across the range of user indicators for delivery. The process to have new technology approved being too bureaucratic was rated the greatest challenge in this area.

Figure 5 - Average rating - Delivery

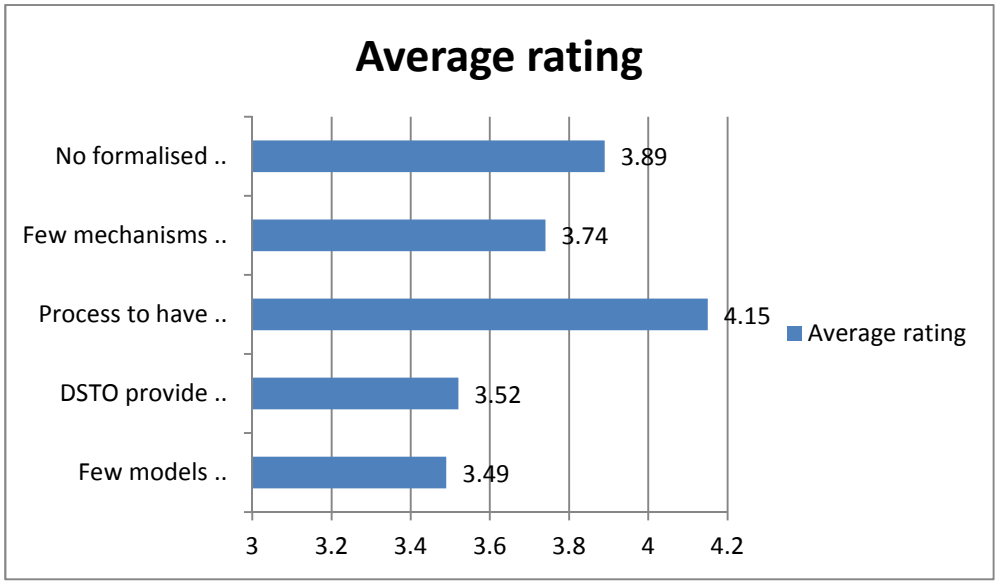


Table 7 sets out the percentage breakdown of responses by level of importance across the range of indicators for delivery:

Table 7 - Data summary - Delivery

	Very important (%)	Important (%)	Fairly important (%)	Fairly unimportant (%)	Not important (%)
No formalised mechanism to engage with DSTO and other S&T providers – publicly funded, academia or industry	27	40	29	4	0
Few mechanisms outside of pure research to engage with S&T providers	13	57	22	9	0
Process to have new technology approved too bureaucratic keeping SME's out of the market	52	24	15	4	4
DSTO provide greater transparency of S&T goals to enable industry to propose in which they can be supported.	20	41	15	20	4
Few models exist that meet the security requirements of various users such as intelligence agencies.	18	31	33	18	0

The survey asked respondents about the extent to which they agreed or disagreed that a particular set of issues around a policy for invigorating science and technology for national security (as set out in the consultation paper) were important.

Figure 6 sets out the average ratings across the indicators on a scale of 1-5 where 1 = not important and 5 = very important. The lack of visibility of S&T efforts was rated as the most important issue in this context.

Figure 6 - Average rating - Importance of issues

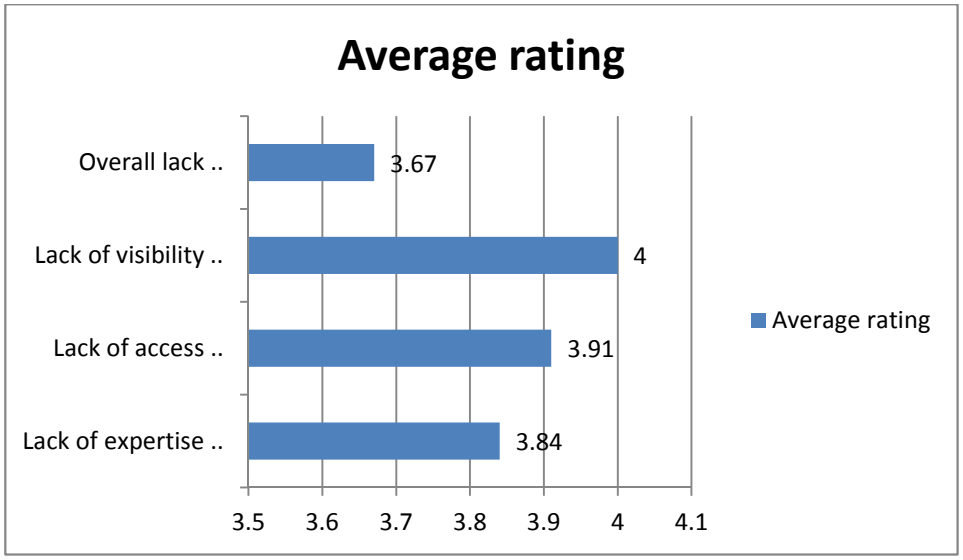


Table 8 sets out a percentage breakdown of the extent to which respondents agreed or disagreed that the indicator was important:

Table 8 - Data summary - To what extent do you agree the following are important issues?

	Agree strongly (%)	Agree (%)	Neither agree nor disagree (%)	Disagree (%)	Strongly disagree (%)
Overall lack of transparency of S&T efforts	22	41	24	9	4
Lack of visibility of S&T efforts	35	40	17	9	0
Lack of accessibility of S&T efforts	24	50	20	7	0
Lack of expertise to collectively meet the needs of national security agencies	33	36	16	13	2

Other challenges or opportunities

The survey also asked members if there were any other challenges or opportunities that needed to be addressed.

Challenges identified by respondents included the lack of science and engineering expertise of many decision-makers, the lack of career paths for technical professionals, lack of cooperation with other like agencies, time-consuming regulatory requirements, excessive bureaucracy and administration and a lack of consistency in funding arrangements.

Table 9 sets out a selection of their responses:

Table 9 - Other challenges or opportunities

a.	To be an informed customer, government must maintain in-house experts to address the chronic and critical shortage of skills essential to develop robust major capability proposals. External advice is over prices and not as accurate.
b.	Challenges: Policy and high-level decision-makers in many organisations are science/engineering illiterate. They do not appreciate the true value of real science/engineering capabilities and do not understand the significant costs in developing capabilities that have lapsed at short notice. The skills and expertise of S&T professionals are not valued and there is no incentive to develop them further or aim for excellence. Many S&T professionals are forced into project management type streams for career progression. Power, influence and credit are accumulated in professions such as project management where there is a value given to 'communicating' well, making 'decisive' decisions and giving an appearance of high activity when there is no quantifiable metric to evaluate performance and more often than not the decisions made by middle management are usually detrimental to S&T capability. Overall policy-makers do not make evidence-based decisions. There are usually no quantifiable metrics to be able to measure success/failure (mostly qualitative).
c.	Cooperation with like agencies in other countries to share expertise on how to deal with common issues.
d.	Government needs to realise that more resources are needed. Cutting back on S&T will not help address national security concerns.
e.	Lack of expertise is not a major problem - the expertise exists, we are just not using it (and of course, paying for it).
f.	Lack of belief/understanding by politicians of the need for long-term investment in S&T to generate quality advice / outputs.
g.	Constant shortage of, and uncertainly about, funding - the way that funding is assigned, and redistributed at short notice if not spent would bankrupt a business. Accountability is definitely a requirement, but does there have to be so much messing about with spreadsheets to get it sorted out? Sounds like I'm getting on my high horse about paperwork again - many regulatory requirements within DSTO are all about maximum spread arse-covering, and have very little to do with any actual net benefit.
h.	Management overheads and administration is disproportionate and detrimental to the actual work being done.
i.	Government direction in how S&T is to bolster Australian defence industry to overcome strategic weakness represented by overseas reliance and vulnerability of supply lines in time of war.
j.	The challenges listed above are all articulated in a depersonalised manner ("S&T effort", "S&T capabilities") that avoid articulating and addressing the "people" issues that I believe will be key to successful coordination. Individual DSTO staff will have to work closely with their counterparts in other government agencies to elicit S&T requirements or identify where S&T might help, and then set up and manage programs involving multiple players to develop and deliver.
k.	It is not necessarily a lack of funding in DSTO but a lack of consistency in funding linked to poor ability to navigate the 'valley of death' between S&T concept and process or technical implementation.
l.	Less focus on management bureaucracy and the growing absurd levels of compliance required for issues such as workplace safety. Labs are high amongst the safest workplaces in this community, yet they ordinarily deal with numerous perceived high hazards which draws

	disproportionate compliance demands. This situation is a real impediment and will only worsen in coming years as a nonsensically safety conscious culture takes root.
m.	International collaboration and place. Resourcing to do the job without imposed process by non-scientists. The process may be perfect for the broader defence e.g. DMO procurement process; but prevent DSTO being agile as required.
n.	Isn't the key issue to bring the best S&T to the table to work collectively for the greater good. Hence a governance structure and working/sharing arrangements that will also deliver visibility to those that need to know. Good direction on not just priorities but focus on where S&T can deliver the most benefit. This direction may be better delivered by a more neutral coordinating body.
o.	Actually doing research rather than the increasing degree of local administration.
p.	Excessive bureaucracy.

Policy context

Section 4 – Concepts, principles and actions from NSSIS in new program and policy

Concepts, principles and actions from NSSIS

The survey included a question asking members about which concepts, principles, actions from NSSIS (2009) (if any) should be incorporated into the new policy and program.

Many respondents suggested that all of the concepts, principles and actions should be included but others highlighted the need to include the people dimension in the policy and program, fix R&D infrastructure, strengthen connections with industry and ensure the national security agenda is not politicised.

Table 10 sets out a selection of responses.

Table 10 - What should be incorporated into new policy and program from NSSIS?

a.	Recognise the importance of science and innovation in protecting our national security, cyber-security, developing and promoting indigenous defence and national security capabilities.
b.	Recognition of S&T needs to be put into practise. DSTO needs a better defined role. S&T should not be optional, other defence agencies need to be engaged with DSTO as part of standard business. DSTO should not be optional, called to fix problems after the fact.
c.	All of them. We are weakened because we have no S&T centre of mass.
d.	All of them!
e.	All.
f.	All of them, note SIEV's are not a national security problem, they are a political problem, terrorists fly business class.
g.	The need to work on the human part of the problem. Technology merely facilitates the loss of security - it is people who impact on security.
h.	All of them. They made sense in 2009, and still do. My only concern is that other (non-security related) pure and applied research shouldn't be detrimentally affected.
i.	All this guidance is well and good. BUT if we don't fix the broken national infrastructure for R&D, then this will never progress beyond shelfware. Improvement attempts succumb to death by committee with no useful decisions.
j.	Stronger defence underpinned by defence industry ensuring self-reliance on materiel needed to maintain a war effort. Skilling and improving capability of other government agencies in their role of delivering national security outcomes (e.g. cyber-crime delivering tools, techniques and training). strengthening connections between science, research and industry and building new ones (a coherent policy and mechanisms to transition R&D to industry through commercialisation) to ensure they are available to defence as a) products and b) training (techniques/skills sets).
k.	All of them.
l.	I support the NSSIS emphasis on environments and mechanisms to encourage S&T coordination and delivery. Again, however, I feel this emphasis is undermined by the depersonalised language in which it is couched. The "mechanisms" mentioned above are ultimately all about finding processes, structures or incentives that encourage PEOPLE (either individuals or groups) to define, develop and implement S&T solutions. It's about setting up shared understanding and goals, networks based on trust and mutual appreciation of demonstrated competencies, etc.: without these S&T simply won't make it into policy or operations.
m.	The interaction of various areas to coordinate S&T initiatives.
n.	Generally, yes, national coordination is needed, but not if it entails the creation another level of bureaucracy with its funding drawn from the same small pool as the existing fund-starved research efforts. DSTO is the agency which should be tasked to take up the national coordinator role. The following statement from above is of great concern: "First and foremost, the national security S&T policy must align with and support the government's national security and science and research agendas and priorities." What nonsense - how does a government with such little understanding of science that it lacks a science minister have the

	ability to set an optimum agenda for NS S&T? What pork-barrelling and lobbying will "guide" setting the "research agendas and priorities"? There must instead be a mechanism for recognising and incorporating expert advice on existing and potential threats, how to rank them and how to deal with them within feasible budget means. One example: greater attention is needed for nuclear and radiological issues - these are true big threats.
o.	NSSIS 2009 as I see it is very broad and not very specific. It gives big statements but lacks the Why or How? Perhaps a focus on these two questions might be better for a policy and program.
p.	No view one way or the other. The big failure has been in actual delivery rather than design of policy.
q.	Integrates science and innovation into broader national security policy coordination efforts, develops specific mechanisms to bring together Australian government national security science and innovation agencies and others in Academia and private industry at a governance and working level. Set the framework for funding.
r.	All.
s.	Probably all of them.

National security

Section 5 – Objectives of the policy and program

The objectives of the policy were summarised as follows:

- define Australia's national security S&T priorities for the next decade;
- coordinate efforts to best take advantage of investment in S&T and address critical gaps to address immediate and future national security capability, operational and policy needs;
- develop and support S&T collaborations and networks that bring together, under a shared vision, the best in industry, academia, PFRAs and government; and
- create public and private investment partnerships in national security S&T through a Program that accords with government priorities and capitalises on our broader innovation system and international linkages.

Policy and program objectives

The survey asked members if in their view these were the right objectives for a national security S&T policy.

69 per cent of respondents said the objectives as set out in the consultation paper *were* the right objectives while 20 per cent said they were unsure. The respondents who answered in the negative – comprising 11 per cent - were asked to detail how the objectives *should* be articulated. These responses included the need to have a 3-5 as well as a 5-10-year view, the need for self-reliance and the need to be explicit about how the objectives should be achieved/implemented. Responses are set out in Table 11.

Table 11 - Other objectives for national security S&T policy

a.	Critical S&T for Australian national security and the transition into fielded new and improved capabilities. S&T that grows Australian national security self-reliance and national security industries and contributes to coalition demonstrated capabilities.
b.	Defining the 10 year view is the necessary context, but the security focus should also be focussed onto a 3-5 year window which moves forward each year to set funding priorities. Some long term 5-10 year priorities should also be set and funded.
c.	Change "government priorities" to "national interests". Government should not direct scientific endeavour, it should consult with the science experts to obtain a direction in the national interest.
d.	Focusing on building an indigenous Australian capability for international leverage is also an important focus point.
e.	The objectives are correct if they align with a general intent on what we are trying to achieve in terms of defence. What is the role of S&T? What is the role of R&D? It seems these are poorly understood by government hence the priorities are badly aligned with the Defence needs of the nation. Some popular terms such as cyber-security and terrorism are used but how is the best value for tax payer funded R&D going to be delivered? One view, is that they are used to develop and produce products and training to equip defence and our broader national security partners in fulfilling their mission.
f.	My main problem with the objectives is not that they are wrong, but that they are articulated in a quite abstract way that gives very little insight or guidance as to how they might be achieved.
g.	The policy should adopt these as principles but instead provide direction as to how the above may be achieved. The governance framework will deliver parties who will advise government on S&T priorities short and long-term noting things will be constantly changing. This governance body would coordinate efforts manage any program funding, build and manage partnerships, collaboration etc. The policy will establish if mechanisms are established to provide authority and get the resources needed. Also in all of this there are IP issues to resolve.
h.	There should be a tick-tock arrangement (10+10) The first for technology and the next from the client about fielding innovative equipment!

Achieving objectives with efficiency and minimal bureaucracy

Members were asked to provide suggestions for achieving national security S&T objectives in a way that improves efficiency and/or minimises bureaucracy.

Issues highlighted included the need to have science and engineering expertise embedded in middle management, for leadership in S&T, for accountabilities and clarity around required outcomes, funding of industry-based S&T, to streamline approvals processes so they are proportionate to levels of risk and the need to reduce administrative burden.

Table 12 sets out the responses:

Table 12 - Improving efficiency and/or minimising bureaucracy

a.	Less project management overhead in middle management. More individuals from a S&T background should be placed in middle management positions across nearly all agencies.
b.	Bureaucracy exists because decisions made externally do not consider the impact of policies on staff that have to implement. Principles should be used to develop efficient processes. Flexibility of policies and empowerment matched with responsibility is needed. Policy should have clearly defined objectives and be justifiable when all impacts are considered. Their practicality and effectiveness also needs to be demonstrated.
c.	National security is directly linked to S&T leadership. Our political leadership is concerned more about economic fundamentalism than measurable S&T outcomes.
d.	Set the timescales for delivery of answers or demonstrated capabilities, then adjust budget to suit, or cancel the program.
e.	Increase support to private enterprises that have good ideas in national security to take those into development.
f.	Put more resources into it. Have a single agency to manage and coordinate the S&T.
g.	Use of more free-moving agencies like the Cooperative Development Centres, comprising defence, universities, DSTO, intelligence agencies and industry as mechanisms to focus some of the activities (perhaps the consultation and planning aspects). This has the potential to reduce the waste of current government governance and finance burdens, while allowing staff from those agencies to interact in a centre focussed on the outcomes desired. Also embed liaison staff in the main players' organisations, similar to the S&T Advisor network between DSTO and ADF and Use System Engineering tools like CORE to capture requirements and assign them to programmes / agencies / individuals. This would allow for easier capture and automated reporting of results.
h.	Provide scientists and engineers with the appropriate resources unconstrained by external defence policy. Return trust back to the experts and allow them to assess the risks.
i.	More doing, less worthless documentation. Getting the people doing the work to do the work, and not loading them down with administrivia, would be a good start.
j.	Fix the IT System and Bring administration support back.
k.	Ease access for defence service providers to assist in niche R&D capabilities to avoid having to "do everything" internally. Vastly improve and upgrade commercialisation activities so R&D actually gets used in the development of products and services that defence and other national security agencies can directly benefit from.
l.	In my experience some US agencies have been quite successful in creating a shared vision of S&T delivering new capabilities to meet specific national goals (e.g. new space-based systems). This vision is shared between contractors, agency staff and the politicians who oversee the mission: The result is efficient ongoing innovation in which the mission (usually) manages to dominate process or bureaucracy. I think Australia should look to replicate successful models elsewhere, and think hard as to why they are successful.
m.	Look at DARPA's engagement mechanism's e.g. with Hacker Spaces.
n.	Offer CRC-like funding opportunities for collaborations between academia, government research organisations and industry involving national security research.
o.	Approvals processes are not matched to the cost of a particular objective. Smaller objectives should have simpler approval processes.
p.	National coordination should be led by DSTO, as should the majority of the research. It is the only agency with the breadth of expertise and scale to undertake this. Implementation in coordination with specialist agencies.

q.	Principles based decision-making.
r.	Needs to be more multi-stakeholder engagement, and publication of the results. What use is knowledge if no one ever hears about what has been discovered?
s.	Clear and concise objectives for national security so that science and technology can be applied efficiently to help achieve the objectives.
t.	Obviously an organisation not mired in government rules and able to get the people needed (not just available) would do a better job of governing the policy arrangements.
u.	Bring back admin/finance staff.
v.	Increased autonomy of agencies, making them responsible for their own programs without having overly burdensome reporting requirements.

Mechanisms for facilitating sharing capabilities

Members were asked what current mechanisms exist or what options there are for new mechanisms that would facilitate sharing capabilities located outside government.

Table 13 sets out a selection of their responses. Mechanisms suggested included use of budget for travel and training to facilitate collaboration and facility-sharing , co-investment, grants, collaborative projects, the need for shared goals, good IP advice and greater investment.

Table 13 - Sharing capabilities outside government

a.	Allow budget to be used for training and travel for DSTO and DMO to better interact with CDG and capability managers to work on whole of defence industry initiatives.
b.	Leases, co-investment, grants, purchase timeshare.
c.	Collaborative projects between S&T organisations s like DSTO, industry and academia.
d.	The CRCs were used successfully for years to bring related industry, government and academic sectors together to collaborate and cooperate.
e.	Collaboration with universities has just been made more difficult - go figure.
f.	None unless the IT system is fixed.
g.	In DMO - service providers can be accessed via DMOSS panel. However many SMEs miss out as DMOSS only gets reviewed periodically, is bureaucratic in itself (needs a tender selection process to access a specific company) and requires a range of Higher Delegate Submissions to access services every time an individual support request is required. Effectively a tender is required (including all financial approvals) to be run every time support is required to be accessed. This would better be conducted by setting up standing offer arrangements with various providers of niche capabilities.
h.	I suspect that the need is not just for any new mechanisms or organisational structures, but also for more investment. In particular I believe the government should be prepared to pay contractors, be they academia or industry. However, it should be prepared to demand that in return they buy into delivery of the full capability, not just their little bit. Thus the key need will be for mechanisms that create shared goals among disparate players: It is the same core problem as faced by any defence project, and by DMO in particular.
i.	Current travel restrictions make collaboration and facility sharing difficult to achieve.
j.	Very little - working outside of government agencies in practice (i.e. conducting lab & field research and development, not just attending joint meetings) is loaded with tripwires from IP issues through who makes what salary commitments, local HSW etc. A really difficult mess to navigate at present.
k.	DSTO needs to get more involved in social media. We are using yesterday's tools to research tomorrow problems.
l.	Research agreements exist between DSTO and universities which can allow sharing These can be expanded and modified to encompass most requirements.
m.	The defence RPDE arrangements are an example of a different approach. There are other non-government authorities (quasi-government) that might provide suitable models of operation.
n.	Collaborating with academia and industry.

Section 6 – Priorities for Australia's national security S&T

The following priorities were listed:

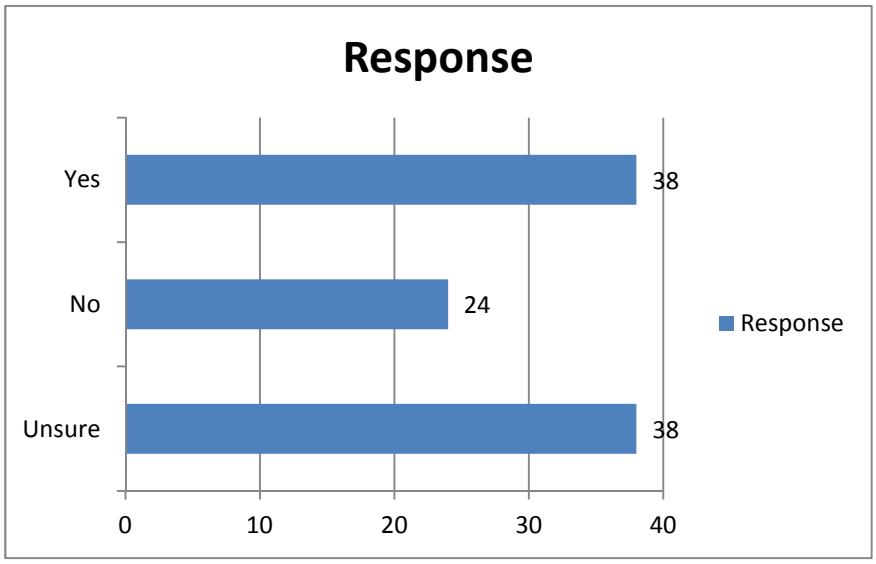
- cyber security;
- intelligence exploitation;
- border security and identity management;
- preparedness, protection and incident response; and
- investigative support and forensics.

Most significant national security challenges

Members were asked whether or not these priorities address the most significant national security challenges Australia will face over the coming decade, and which warrant a collective, strategic approach to the application of S&T effort.

As set out in Figure 7 below, responses were mixed with 38 per cent saying Yes, 24 per cent saying No, and 38 per cent unsure.

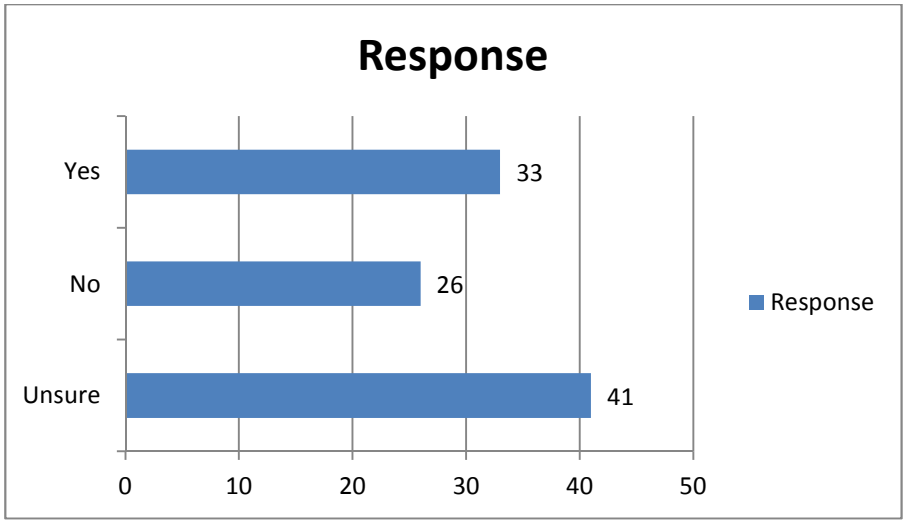
Figure 7 - Do identified priorities address most significant challenges?



Scope of priorities

Members were also asked if the scope of these priorities appropriate and again responses were mixed.

Figure 8 - Is the scope of these priorities appropriate?



What would be more appropriate?

The 26 per cent of respondents who responded in the negative were asked what would be more appropriate. Table 14 sets out their responses which include acknowledging the human dimension of national security threats and enhancing conventional technologies.

Table 14 - More appropriate scope

a.	Also should include enhancing conventional technologies such as radar, weapons and EW.
b.	Again these priorities and their wording do not adequately capture the human dimension of the threats listed above. For example cyber-attacks are directed and carried out by human agents with a variety of different motivations (greed, espionage, etc.); understanding and analysing this dimension of the threat will be essential. Similarly border protection requires an understanding of the forces driving attempts to breech borders, while long experience has shown that combating terrorism is seldom successful unless root causes are identified and resolved. In short sociology and other soft sciences should be important components of any national security S&T plan.
c.	Include "biological threat agents" in "Preparedness, Protection and Incident Response".

Other priorities

Members were then asked what other priorities, if any, the government should consider in the immediate future. Responses are set out in Table 15 and include monitoring trends and emerging technology, looking in detail at cyber and telephony-based threats and participation in international alliances.

Table 15 - Other priorities

a.	Support to acquisition and defining a capability properly should be a priority.
b.	A focus on cyber and telephony-based threats and building networks of trusted intelligence gatherers sounds like a good start. Doing periodic rigorous threat assessments and acting on them would also be useful. Run red vs blue exercises (i.e. fund some people to work out how to attack the country). Pay a bunch of bright young cyber specialists to do whatever they think is a good idea in regards to cyber security. i.e. provide seed money and infrastructure for them to play with - it'll stimulate good ideas if they are not bogged down with the usual government employment induced loads.
c.	Useability of IT and internet services by its own people. We're only just moving to Windows 7.
d.	Participation in international alliances on cyber-security and contribution to and implementation of recognised and standardised practices. Focus on specific niches as part of an international alliance.
e.	Extreme weather events are clearly ongoing actual threats so they should have priority over Preparedness, Protection and Incident Response, which to date still only remains a potential problem in Australia.
f.	Develop novel medical countermeasures to tackle anti-microbial resistance.
g.	Not much can be achieved in a 0-3 year period.
h.	Monitoring trends and emerging technology.
i.	Environmental impacts from climate change on water and energy in Australian region.

Cyber-threats

Members were asked for their views on what specific cyber-threats and/or mitigations should be considered in developing a cyber S&T program and who the key stakeholders that should be involved are. The responses are set out in Table 16.

Table 16 - Specific cyber threats and key stakeholders

a.	DMO Electronic Systems Division esp. EW areas.
b.	Developing secure network infrastructure. Key stakeholders: technology companies such as Google etc. and computer security experts from ASD for example.
c.	Clearly DSTO has the leading role in national cyber-security S&T. The question is how is DSTO S&T R&D pulled through into a national capability.
d.	Cyber touches everything, but should not be the commanding agency. It is more than a tool, but less than the end goal.

e.	External rogue states deliberately attacking our networks. Reliance on single source companies (Microsoft) for a majority of our IT infrastructure or on open source products line Linux for our operating systems. Many smaller government agencies are not well protected. Provide them with the resources (human and money) necessary to reduce the risk.
f.	Key stakeholders. NATO, US, ABCA.
g.	Industry, and in particular the ISPs and large web service providers, are clearly key stakeholders in cyber and therefore in cyber S&T. I'd be surprised if DSTO has any substantive links with any of these stakeholders; building them should be a high priority.
h.	The use of social engineering by cyber threat actors warrants further investigations as it is often overlooked in favour of purely "technical" issues. This may be partly mitigated by improving the education of users to thwart such attacks. Would involve all cyber-stakeholders.
i.	The dependence on Microsoft bloatware defines the cyber threats seen by most large government departments, including defence and foreign affairs, stock exchange and banks and other major financial institutions. In addition data switched provide possible additional weak points.
j.	Most people are about creating capabilities. Cyber is merely one vehicle. These topics should all be treated equally.

Section 7 – Coordination

The following key coordination strategies were detailed in the survey as set out in the consultation paper:

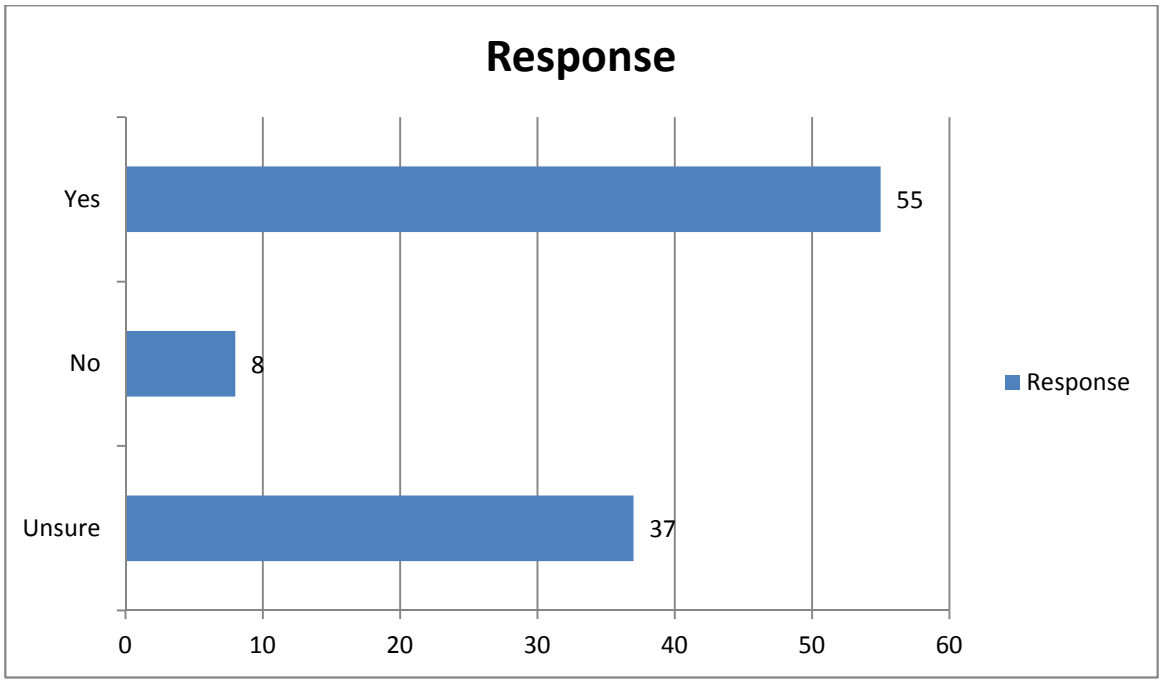
- leveraging existing coordinating committee structures (such as ANZCTC, ANZEMC), and
- raising awareness through dissemination across the national security community, of information, data and research outcomes of national security relevance (through conferences, workshops, websites, portals, databases, scientific adviser networks). This will require standardised and robust arrangements for sharing classified information.

Appropriateness of coordination approaches

The survey asked whether or not the coordination approaches as listed were appropriate.

As set out in Figure 9 below, 55 per cent of respondents thought the coordination approaches were appropriate.

Figure 9 - Are the coordination approaches listed appropriate?



The 8 per cent who responded in the negative were asked to explain why the coordination approaches set out in the consultation paper were not appropriate and responses are set out in Table 17 below. The main issues raised were around collaboration, measurement and implementation.

Table 17 - Why are these coordination approaches not appropriate?

a.	Shared information is lost and technical advantage and power against national security threats is also lost. We are too free with our S&T directions and even results as we are keen to be a contributor, unlike others.
b.	I think that there is a need for a central agency with the resources ($ & staff) to bring about the coordination, to fund agencies to do the work etc. A central agency with the resources can direct the research much better than trying to do it by committee.
c.	Again I have no problems with the stated goals, but I don't get any feeling from the words how they will translate into concrete actions involving individuals.
d.	International collaborations should also be included.
e.	How do we measure these things?
f.	Lots of talk but little action. Government is reducing the size of the APS, while increasing the scope of projects. They must be kidding, right?

Other coordination challenges

The survey asked respondents to identify other coordination challenges and a selection of responses is set out in Table 18 below. Additional coordination challenges identified include the credibility and technical competency of providers, the need to embed professional scientists in agencies so their expertise is used in shaping programs and initiatives, the danger of "over-coordination" affecting diversity of views and becoming bureaucratic, willingness to share across agencies and the need for balance between tasking and coordination.

Table 18 - Other coordination challenges

a.	Unfortunately national security S&T is the new black. Every vendor and snake oil salesman is now selling product and services most completely inappropriate for national security purposes. The challenge is that there are very few actors in this space with real credibility and technical depth to deliver.
b.	Individuals are the key to coordination of S&T. Embed more scientists in the agencies to assist the delivery and shaping of S&T programs, whilst at the same time gaining a extremely valuable understanding of the problem space.
c.	Coordination also encourages conformance. One-size-fits-all thinking. It can be also useful to have agencies trying novel ideas by themselves, or duplicating work on a problem.
d.	Territorial disputes' over who 'owns' information or a particular topic or area - there can be unwillingness to play nice, and share with the other kids in the sandpit.
e.	Identifying what the goals of the partnerships to be "nurtured" are. What are we trying to achieve and who is going to do what. Identifying clear lines of accountability, authority structures and Agency goals that align with broader goal and direction.
f.	Back channel discussions.
g.	Clearly - political motivations by groups and individuals.
h.	Obtaining approvals from national agencies tasked with maintaining security.
i.	Of course. Everyone has an axe to grind to chop out the legs from someone else.

Extant coordinating committees

Members were asked what extant coordinating committees could be utilised. A range of suggestions were made and a number of respondents noted that committees could function as obstacles to, rather than facilitating, coordination. Responses are set out in Table 19 below:

Table 19 - Extant coordinating committees

a.	Not aware of any extant good ones.
b.	Committee's are generally a road block.
c.	Unaware. There may be some TTCP panels which are appropriate.

d.	Defence Security Council to articulate what it wants and clarify chain of command and accountability of individual heads of agencies.
e.	TTCP, CBR MOU and the Quadrilateral Medical Countermeasures Consortium.
f.	NATO.
g.	Too many committees, I think. The Defence minister needs to take responsibility and not pass the buck.

Transfer of coordination function from MP&C to defence

Members were asked about potential issues with the transfer of the coordination function from MP&C to defence. Issues raised included increased bureaucracy, the need for investment/funding/resources, the need to have clear purpose and structures, appropriate performance measures, interaction with other agencies and appropriate recognition and reward for staff. A summary of issues raised is set out in Table 20 below:

Table 20 - Issues with transfer of coordination function

a.	Bureaucracy and overheads.
b.	Political and foreign relations impacts of national security actions and S&T directions.
c.	Defence needs to put enough resources into the program (it is currently underfunded as is most S&T in Defence).
d.	The extra resources required to do the work. Don't give it to defence and pocket the change.
e.	Clarity of purpose. Agency goals that align clearly with purpose. Clear chains of command and authority structure. Clear agency and individual accountability. Performance measures which identify success or failure.
f.	Unlike MP&C Defence has relatively poor links with other departments, relatively little experience in dealing with them, and probably not a lot of leverage over them. Similarly Defence S&T has relatively little overlap with civil S&T.
g.	Within Defence, DSTO is the organisation where the NS coordination and research effort should sit. The issues Defence should be aware of are those pertaining to efficient DSTO interaction with national security customers.
h.	Comes with FTE question and reducing budgets by arguments of like functionality.
i.	Greater interaction with non-defence agencies - differing cultures.
j.	Paying its people 20% higher salaries.

Section 8 – Governance

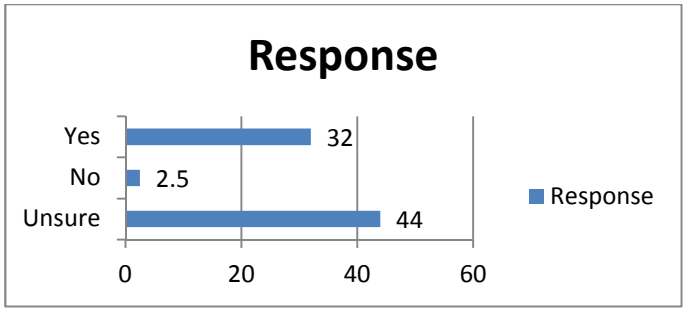
The proposed governance arrangements as set out in the consultation paper were summarised.

Governance arrangements and policy objectives

Members were then asked whether or not the proposed governance arrangements meet the overall policy objectives. Responses were mixed with a relatively high proportion of respondents saying they were unsure.

Figure 10 sets out the responses:

Figure 10 - Will the proposed governance arrangements meet policy objectives?



More effective and efficient ways to meet policy objectives

The survey asked respondents to identify alternatives that would allow for meeting policy objectives in a more efficient and effective way. The responses are set out in Table 21 below and suggestions include the appointment of a Chief Defence Engineer, clarity around role and structure of steering committee, clarity around authority and accountability for inter-agency tasking, adequate resourcing and the need for industry input.

Table 21 - Alternative governance arrangements

a.	Defence also needs a Chief Defence Engineer or CTO.
b.	How will a steering committee at high level provide assurance of the quality and impact of the research? Meeting all the policy objectives is in the detail of the committee set-up and operation.
c.	Provided there is one agency with control of the resources.
d.	Who will chair steering committee and task individuals in attendance? Mutual agreement??? This needs to be clear. Accountability for action needs to be clear. Authority for inter-agency tasking and commitment of resources needs to be clear. Participation seems to be broad enough but bot all should have an equal say as logically some agencies will bear the brunt of the work and have more general involvement than others.
e.	The bullet "ensure the research team/s are held accountable for their deliverables" is very laudable, but nowhere do I see any statement of intention that adequate resources will be provided to perform the task fully. The ARC approach, for example, is to give the "funded" projects substantially less than was requested, often making the delivery of the full goals impossible.
f.	Needs industry input. The people listed have limited leadership outside a series of government silos.
g.	I think a Board with government and non-government members with some actual powers and defined role and clear objective is needed. Another government talk fest will deliver very little.

Composition of steering committee

In response to the question “Is the composition of the steering committee appropriate?”, 37 per cent said Yes, 26 per cent said No and 37 per cent were unsure. This spread across responses suggests a diversity of views in this area.

Stakeholder representation

Members were asked which stakeholders should or should not be represented on the steering committee and why. A selection of their responses are set out in Table 22 below. Suggestions included a Chief Defence Engineer, the Australian Federal Police, Attorneys General, Department of Education, Department of Industry, academia, the Department of the Prime Minister and Cabinet and the Land Engineering Agency. Respondents also made the point that a committee which is too large is not effective and that decision-making powers of all the bodies represented should be tiered/differentially allocated to ensure maximum efficiency and effectiveness.

Table 22 - Stakeholder representation on steering committee

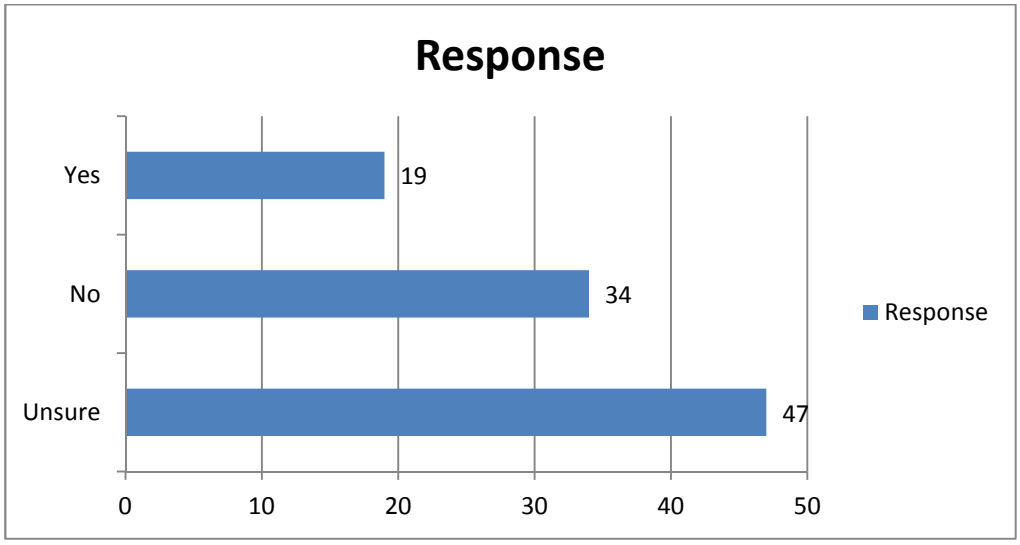
a.	Defence needs a Chief Defence Engineer or CTO.
b.	Department of Industry - may create more conflicts on what industry sector must be represented; whatever security issues are addressed should be applicable to any industry anyway.
c.	Isn't AFP part of AG department?
d.	How do states fit into this picture? I believe there is a national police committee that looks at technology.
e.	Should include non-government representatives from e.g. Universities Australia, defence industry representatives etc. or at least the Education Dept.
f.	Composition is appropriate however some members such as Federal police and AGs should only be second tier participants. Who will conduct the S& work? Most of the agencies will articulate the need. Others will produce the solutions to meet the need. Not all participants should participate on an equal basis as the decision-making ability of the group will be laborious, bureaucratic and ineffective. A smaller group under general but focussed guidance will be faster, more flexible and decisive.

g.	In governance, the CEO is frequently not the chair of the board due to conflicts of interest. An additional member is needed to represent the interests of the general public, who will be affected by the program but otherwise have little say in it. This additional member should be the head of the board, not CDS.
h.	Too big nothing will be achieved.
i.	I wonder if there is an international element that should be considered.
j.	The proposed steering committee is at the wrong level as the list is at a governance level. Leadership should be at least 2 levels down to ensure appropriate level of application in the development of policy ideas without competing agendas.
k.	I think it needs more representation from outside government and representation with broader views.
l.	Industry and academia representatives should be represented.
m.	Department of Defence; the Attorney General's Department; the Department of Prime Minister and Cabinet. Only the Prime Minister should sit on this important committee.
n.	LEA as they are the ones that take the blue sky research and turn it into practical products and/or solutions.

Steering committee co-chaired by a user agency?

The survey included a question which asked whether or not the steering committee should be co-chaired by a user agency. The relatively high proportion of "Unsure" responses suggests fairly widespread uncertainty around this issue. Figure 11 below summarises the responses:

Figure 11 - Should the steering committee be co-chaired by user agency?



What agencies could co-chair and why?

The survey went on to ask "What agencies could co-chair and why?" and a selection of the responses are set out in Table 23 below. Suggestions included DMO, LEA and P&C. Others commented that co-chairing may complicate the function and some expressed the view that the military should not co-chair.

Table 23 - What agencies could co-chair?

a.	DMO.
b.	To ensure that whatever is being discussed meets at actual need or outcome.
c.	What does it achieve, the key user agencies are on the committee so I assume their concerns will be heard.
d.	One chair. Tier 1 participants: P&C, Defence , etc. 2: Tier 2 (non-voting advisory capacity only) participants: Peripheral user agencies.
e.	Australian Federal Police.
f.	I see no crucial reason for CDS as head of the program, to also be chair or co-chair of the steering committee.

g.	I see no advantage in co-chairing: "keep it simple".
h.	Have a look at the members! Nothing will be achieved!
i.	A military person must not lead.
j.	Land Engineering Agency

Steering committee reporting

The survey included a question about where the steering committee should report into. While the Secretary of Defence and Parliament were also identified, responses indicate that there is fairly widespread support for the steering committee reporting into the NSCC. Responses are set out in Table 24 below:

Table 24 - Steering committee reporting

a.	NSCC.
b.	National Security Comm of Cabinet.
c.	NSCC.
d.	NSCC.
e.	Yes NSCC is appropriate. The problem with reporting what you are going to focus your Security R&D on for 10 years is that it signals to hostile states where your vulnerabilities currently are, which they may choose to exploit before you fix the gaps.
f.	The steering committee should report to the general public via the Open Government mechanisms.
g.	Yes - NSCC is appropriate.
h.	NSCC is OK but Secretary of Defence would seem appropriate too.
i.	The above governance committee!
j.	Parliament.

Expectations of DSTO

The survey asked members to detail their expectations of DSTO as Australia's coordinator for national security S&T. The responses ranged from providing 'frank and fearless advice', coordination, client focus, technical leadership, impartiality, priority-setting to allocating funding. A selection of responses is set out in Table 25 below:

Table 25 - Expectations of DSTO

a.	Fair, impartial and fearless advice combined with genuine and valued S&T leadership.
b.	I do not think they should be a coordinator.
c.	To talk to and take advice from relevant experts within LEA.
d.	Too many to name here. Big things, like making sure that FSP produces something we can be proud of, etc.
e.	Technical leadership and coordination of activities.
f.	DSTO has a client-focused culture that it should bring to the client agencies, for example by posting staff into those agencies to develop S&T requirements for the scientific agencies & industry partners.
g.	To be an impartial coordinator, to push for excellence and impartiality in decision-making, to encourage best methods of thinking, coordinating and doing.
h.	DMO is better placed to coordinate translation of S&T outputs into products and services that could provide direct benefit to national security user groups. This is due to business acumen.
i.	DSTO are the appropriate body to oversee this program given their S&T background and independence.
j.	To be a type of clearing house.
k.	The role expectations are largely covered in the preambles to above questions. The reality is that the complexity of the threat space and number of responsible agencies/organisations makes a national coordination framework necessary, and the committee outlined above seems very suitable. The issues then become priority-setting and allocation of meaningful funding.
l.	To both deliver advice and undertake S&T research.

m.	Frank and fearless.
n.	Ideally placed to undertake this role.

Section 9 – Collaboration

Management of barriers to collaboration

The survey asked members about their views on the barriers to collaboration and how they might be managed under a new policy framework. Barriers identified included the lack of mechanisms for cooperation and collaboration with other agencies, industry and academia, stovepiping within agencies, lack of funding/resourcing, lack of proper security frameworks, lack of direction from government, failure to clearly identify performance objectives, lack of in-house business acumen, lack of understanding of skill sets in other agencies, lack of attribution or recognition and red tape. A summary of responses is set out in Table 26 below:

Table 26 - Barriers to collaboration

a.	No mechanism to co-operate. Stovepiped configuration of separate agencies. Business as usual attitude without a desire to change.
b.	Lack of funding. Collaborators need to be paid, the government is source of income. If government organisations do not have money to spend, collaboration will dry up quickly.
c.	Collaboration is impeded by various acts of parliament that require separation between the main national stakeholders when working on S&T projects, particularly when it relates to data analytics.
d.	People on all organisations are driven by timelines to be internally-focused, so collaboration is a low priority. Need to set up full time X-agency teams with one objective.
e.	Security and funding - proper security frameworks and increased funding is required.
f.	Staff availability and resources are the usual barriers, for some areas security can be an issue.
g.	Niche markets like cyber-security are hard for small Australian companies to support with innovative products, especially if the Government funding is off-and-on. Providing more continuous funding through project work enables building of capability to then crank up when a problem hits (i.e. to be a part of first response). Suspicions of industry as being mercenary, and of Government as being bureaucratic, dictatorial and inefficient need to be overcome and bridges built. Using each part for the things they do well should be paramount.
h.	Clear direction from government. No performance objectives at present. Poorly defined mechanisms and low skill sets in business acumen to achieve this outcome.
i.	DSTO's culture, the relative paucity of previous engagement of the academic S&T community on defence and national security problems.
j.	Despite a national security classification system, organisations may still be reticent to share classified information. Could be mitigated by forming cross-organisation teams with a common security policy.
k.	Travel restrictions. Recognition needs to be made of the importance of face-to-face meetings at the working level. It is recognised at leader level but downplayed by leaders at the working level.
l.	There is a low appreciation of operations research in Australia, the scientific practice that informs collaborative, multidisciplinary decision making. DSTO even proposes to reduce operations research at this critical time.
m.	Lack of knowledge of specialised skills sets and facilities existing in other organisations and "non-collegial" pricing of research to external "clients", i.e., the external funds are sought principally as a budget input item rather than as the means to facilitate research - the money is the goal not the output.
n.	Poor attribution and acknowledgement. Accountability for actions (or non-actions)
o.	People who consider that a rigid policy and program is required and fully in place before processes start are a real problem to success.
p.	Paperwork, red tape, getting agreements written and signed.
q.	Getting people and organisations to give up what they know. Management of this should be worked out under the direction of the new policy.
r.	Money and opportunities.

s.	Sharing of information, particularly classified information.

Models to improve collaboration

Members were asked about models to improve collaboration. They detailed a range of options including developing integrated project teams with sufficient funding to allow face-to-face meetings, implementation planning, clear measures of performance, embedding staff between agencies and within academia, structured dialogue and a range of other techniques to improve decision-making. Responses are set out in Table 27 below:

Table 27 - Models to improve collaboration

a.	US university funding model where defence funds university academics/students/PhD to investigate/collaborate on projects.
b.	Funding availability, not just for established programs. Money needs to be spent on areas that have potential. A good funding model should allow for this.
c.	Dedicated teams, with expiry dates. Embedded staff officers an operatives-term appointments.
d.	What doesn't work is pretending to collaborate, with undernourished resources, no travel funds and no clear resolve to get a job done properly. Video conferencing is fine for some coordination, but collaboration needs a meaty problem to solve, resources of money and time and access to relevant equipment/ systems/data and appropriately trained and experienced people to run and do it.
e.	Integrated Project Teams are the way to go.
f.	Not aware of any models other than motherhood statements on defence industry collaboration on DMO and DSTO web sites. Unfocussed intentions without clear goals, targets, implementation plans and measures of performance.
g.	In the US the long-standing, extensive funding of academic research programs by defence R&D agencies has created much closer links between defence industry and academia than those in Australia.
h.	Boundary critique methods (so that people understand how and why they may disagree), structured dialogue methods (to reduce power problems), voting schemes and group preference methods (to establish decision-making norms), negotiation analysis templates and analytical hierarchy process (for multi-criteria decision making), dialectical reasoning (to ensure productive coverage of opposing viewpoints), and trade methods such as Pareto frontier (for a quantitative approach to optimising across multiple criteria).
i.	Long-term placement of staff between organisation and into academia is the best way to improve collaboration. This deepens understanding of the relevant capabilities of the partner organisations, and therefore enables optimum use of personnel skills and specialised facilities. When the seconded staff return to their home org they take with them the IP and knowhow they have gained; their organisation can then benefit for years. A second approach is that of funding research packages, this is fine for small-scale projects where the commissioning org has the expertise to then take up the outputs, but on a larger scale this approach is often of limited long-term value to the commissioning org as the know-how stays with the provider.
j.	Shared values and principles are a keystone.
k.	Open discussions and clearly defined problems. Not vague jibber-jabber and process.
l.	Private industry always come down to money. Government people just need to be told that what we know is owned by the Commonwealth not the agency.
m.	There is no one size fits all. Get rid of the buddy systems and introduce entitlements approach to allow equity in share the funding that becomes available.

National security S&T program

Section 10 – Co-investment models

Co-investment models which warrant consideration

The survey asked members for their views on what collaborative co-investment models warranted consideration. The responses are set out in Table 28 below and include the US defence department model which provides for collaboration with private industry as well as universities, NATO and RPDE. A comment was made about the importance of funding core work and that co-investment models were not a substitute for this.

Table 28 - Collaborative co-investment models

a.	US defence department collaboration with private industry as well as universities.
b.	Equal contributions by all stakeholder (either funds or in-kind).
c.	Co-investment is the cheap option, Agencies are funded to do their core work and unless that is focused on national security then they will not put a lot of time/resources into an essentially unfunded program of work.
d.	Joint developments of technology, contracted development of technology, public/private partnerships, research agreements, project arrangements.
e.	In niche areas where it is not value-for-money to establish in-house capabilities on an ongoing basis.
f.	NATO SG2.
g.	The model outlined seems reasonable with one caveat: models will require to take full account of "in-kind" contributions in lieu of cash. For example, collaborations with academia requiring significant cash from the academic partner will almost invariably not proceed - the likely feasible model will be an agency paying for the salary (HDR student or post-doctoral fellow) and consumables component of a research project, and possibly filling some specialised apparatus gap, with the university contributing a staff time component and facility access.
h.	Who is investing what? Leverage can only occur when there is the possibility of mutual gain of the co-investors at a value greater than what is provided. It is unclear whether this is possible here.
i.	I can only suggest the RPDE mode as useful consideration. Not as a solution. Again policies don't need solutions.

Collaborative models which do and don't work

The survey included a question asking members which collaborative models do and don't work. Members suggested that co-investment might be suitable for some projects and not others. Table 29 sets out a selection of responses:

Table 29 - Collaborative models which do and don't work

a.	Co-investment doesn't work that well, if you want an S&T program you need to put resources into it. In defence you may be able to change DSTO's priorities and this means that work on some defence areas will suffer.
b.	Fitting the right development model to the problem, and resourcing it appropriately is more important than picking one size fits all solutions.
c.	Time & materials based contracting is recommended.
d.	Diggerworks in DMO.
e.	TTCP is difficult to make work because of the politics played in such collaboration.
f.	One-size-fits-all approaches will not work. The research space in Australia is varied in the range of organisations involved, in the "patchy" occurrence of facilities and quality researchers, and also in the year-to-year level of staffing and funding available in any given area. Co-investment strategies will need to take all this in to account on a case-by-case basis. PPP's are not a good way forward - too much is expected of private organisations for the money they receive, and the private organisations are largely only interested in the money they receive.
g.	Shared goals and benefits.

h.	Look at the success or otherwise of the CRC's. Are you really asking for a collaboration involving investment outside government? The proposed steering committee can't invest monies outside their existing budgets and department of finance guidance. Why call it co-investment when it is from a single source.

Pros and cons of collaborative co-investment delivery model

Members were asked what the pros and cons of a collaborative co-investment delivery model for national security S&T might be. Collaborative co-investment was seen as a positive by some respondents with the benefits including guidance for managing projects, sharing of outcomes and optimising of resources. Negatives identified included loss of skill sets and short rather than long-term focus. A summary of responses is set out in Table 30 below.

Table 30 - Pros and cons of collaborative co-investment

a.	Guidance for managing and sharing outcomes.
b.	Pro's ???
c.	Co-investment means sharing. You want to limit exposure of national security considerations (need to know principle) while optimising resource use. It's important to expose novel solutions or sensitive data only to those organisations which have a culture of security and undivided loyalties. It may be possible to collaborate problem specifications upwards and generally, but limit solution development and discussion to a limited circle (including the relevant problem-owners).
d.	Loss of skill sets within government in these areas however we must acknowledge that we cannot do everything. Limited resources are best placed where they can deliver best outcomes and value for money for taxpayer dollar.
e.	Collaborative co-investment is only likely to work if the collaborators share common goals. In particular these need to centre on national well-being as opposed to commercial gain. Achieving such shared, high-level goals will be difficult.
f.	By requiring a cash and in-kind investment, user agencies may only focus on short-term needs not long-term issues.
g.	Pro - better facilities if collaborative co-investment.
h.	Pro: leverage, as mentioned above con: difficulty of arranging the real work to happen - geographic factors means large (=unproductive) travel budget components; potential for IP issues to absorb much resource.
i.	Why would any organisation provide co-investment on security issues outside their department? Common issues and inter-departmental communication spring to mind.

Preferred option for collaborative co-invested model

Members were asked about their preferred option for a collaborative co-invested model. Responses to this question were limited. While some respondents re-stated their concerns with such a model, others restated some of the positives of the collaborative co-invested model. Table 31 sets out the responses:

Table 31 - Preferred collaborative co-invested model

a.	Depends. I guess in an ideal world, defence and national security organisations would be funded to do much of the planning and development work internally, with contracts for uni/ companies to participate in solution manufacture/T&E.
b.	Referral of specific niche areas or back-office functions to service providers to free up resources for work in areas of strategic significance.
c.	The presence of players outside the narrow definition provided by government departments and CSIRO that have real interest in cyber-security.
d.	Recycled policy that failed in the past.

Implementation

Section 11 – Monitoring , review and evaluation

Barriers to effective monitoring, review and evaluation

Members were asked about specific barriers or challenges that could impact the effectiveness of monitoring, review and evaluation and how they might be overcome. Members identified a range of barriers including the lack of metrics, transparency and accountability, lack of cost/benefit analysis, the requirement for security clearance, the need for simplicity in evaluation and the risk of over-management. A summary of responses is set out in Table 32:

Table 32 - Barriers to monitoring

a.	Evaluation is usually not qualitative and measurable. Many decisions are political or the preference of one user group with the absence of an evidence-base.
b.	No current metrics or evaluations of transparency and accountability No effective cost estimation for S&T programs and no rigorous benefits estimation.
c.	About the only measure that I would put in place is to ask the user agencies, have they benefited from the S&T support that they got and how do they value that contribution. If you are not satisfying the client and have their support the program is failing.
d.	Need for security in some aspects of the work. Cleared staff could do the evaluations. Unfortunately, most politicians aren't qualified to understand half of the problems, let alone know a good from a bad solution. Transparency and accountability are all well and good. Perhaps we should use a standard of transparency as used by the terrorist organisations we are fighting.
e.	It will depend on how onerous the reporting requirements end up being.
f.	Effective measures of performance and accurate reporting against these. Accountability for individual agency performance.
g.	Monitoring needs to be simple otherwise it will not be done effectively or efficiently.
h.	The government does not support the Open Government mechanisms, so the agencies won't be getting full cooperation from online communities who have early knowledge of cyber issues.
i.	The Steering Committee remit outlined reads as a potential recipe for excess-management given this discussion is regarding the national security research environment. The SC approach is appropriate for large projects (AWD, JSF etc.) but not when the likely project size and style in national security will be work packages in the 1-5 year range being undertaken by small (or very small) teams. The reporting process should be carefully designed to facilitate progress to achieving the project goals.
j.	The steering committee is providing governance and policy development and then measuring their own success? Rubbish in! Rubbish out! Baseline data is a moving meal with no meaning without clear definitions and limits.
k.	Metrics to monitor and record entitlements against actual expenditure. Stop the empire builders and facilitate meeting the S&T to actually provide science excellence and impartial advice!
l.	Security classification as a barrier, also as a means of hiding non-performance.
m.	"Ensure transparency and accountability" are motherhood statements used when you don't expect things to work properly.
n.	Security classifications are likely to make reporting difficult to communicate widely.

Baseline data

The survey asked members what baseline data should be collected and why. Responses were limited but highlighted the difficulty of tracking and measuring quality and benefits, that baseline data needed to monitor and evaluate is likely to differ between projects and that the function of determining baseline data required to measure outcomes should be undertaken at the stage of project scoping. A summary of responses is set out in Table 33:

Table 33 - Baseline data

a.	S&T Plan.
b.	What baseline can you define? Seems like a silly question, are you trying to understand what an agency does now, are you trying to measure quality, what are you trying to do? There have been a lot of attempts to try and measure S&T quality, most, if not all, have serious flaws.
c.	Metrics need to start at the working level: I think timesheets are the only way to start truly appreciating the underlying problems and start tracking LOE + overheads towards any tasks in national security (or any other tasks).
d.	Degree of benefit that defence and other national security users are obtaining from S&T investment presently. What products, doctrine and skill sets/training packages were developed from S&T investment in DSTO?
e.	Main point: follow the money trails. Cyber application: Immerse technical specialists in relevant online communities to observe baseline activity.
f.	That would vary project to project, and the establishment of a "baseline" should be part of the pre-commencement scoping in most cases.
g.	Industry's ability to deliver.
h.	What is measurable? What is the data quality of what you are measuring? Does the measure have meaning? Man hours and dollars are not measures of success but are measure of intent!
i.	Actual spend against actual planned allocation.
j.	Comparison against other countries' performance.

Section 12 – Resource management

A summary of the resources required for a range of functions as set out in the consultation paper were listed.

Resource management issues

Members were asked if there were any issues other than those listed that should be considered. Issues highlighted included adequate resourcing, resource prioritisation, transparency in resource allocation, formal process setting in resource allocation, the need to clarify where decision-making powers in relation to resource allocation should sit and the extent of waste evident in current resource management processes. Responses are set out in Table 34:

Table 34 - Other resource management issues

a.	Prioritisation of resources, timeframe and effort, given in particular that expectations will be high and delay is unacceptable.
b.	Transparency of resource allocation - in Defence? I'd like to see that.
c.	Formal process for project management Technical management
d.	Put new resources into the program, don't rely on a dribble of resources from individual agencies (in my experience most user agencies don't have a an S&T bucket of $'s to spend).
e.	Lots of accountants and lawyers to find clever ways to relieve S&T staff of the burdens of accountability stupidities.
f.	We will always be under-resourced. The trick is to maximise what we have and minimise overheads. This is something that will need addressing before any more overarching committees or policies are put in place.
g.	Resource allocation breakdown in terms of priorities. Delivery 90% of resources? Governance 2%? This needs to be decided to ensure we have a focus on effective action rather than bureaucracy.
h.	A company will require an expected outcome that they can use before investing any research money. National Security issues will have to match the requirements of large companies and institutions to attract investment dollars.
i.	Perhaps some understanding of who people work for when brought into programs.
j.	How do we get more? How do we say No? Who should say No?
k.	A commitment to appropriate resourcing is essential.
l.	The money wasted by the bureaucracy.

Other key issues

Members were asked if there were any other issues they would like raised in our submission to this consultation.

The following important issues relating to S&T and national security and the workforce required to support it were highlighted.

The dangers of outsourcing in areas relating to national security

Members highlighted the inappropriateness of outsourcing projects where national security is involved. A sample response is set out below:

Table 35 - Dangers of outsourcing

If functions are outsourced, then as an outsourced organisation the incentive is purely to pursue profit based contract research wherever that work may be found. Clearly any advice is partial and sensitive to commercial consideration. It is hard to imagine how this enables the kind of national security S&T leadership government would want.

Fresh thinking and new modes of operating

Members suggested policy and program planning would benefit from fresh thinking about possible ways to manage science and technology and national security. A typical response is set out below:

Table 36 - Fresh thinking and new modes of operating

Like anything in defence and national security, there is a tradeoff between accountability and transparency, and signalling too much to the other side what our foci are. It might be time to brainstorm some newer approaches to bureaucracy to manage things more flexibly, compartmentalise some data and circulate and socialise others. I'd recommend using some system engineers and forward thinking Business Process Development people to design some better ways of organising the responsibilities, resources and result reporting of this new system.

Acquisition of off-the-shelf products and services from overseas rather than developing domestic capability

Members expressed concern that Australia's domestic skills base and self-reliance will be compromised if off-the-shelf products are purchased from overseas rather than being developed in Australia. A sample response is set out below:

Table 37 - Acquisition of off-the-shelf products and services

The role of R&D in DMO needs to be clarified and addressed. Skill sets in engineering are dependent on hands-on experience as well as design work. If less and less of this is occurring due to acquisition of O/S MOTS/COTS products then the skill base will slowly degrade. Perhaps a rotation system with DSTO and industry will alleviate this but at present the problem is not acknowledged.

Recognition and reward

Members highlighted the need to attract and retain high-quality staff with appropriate recognition and reward strategies. The member's comment set out below was fairly typical of the feedback in this area:

Table 38 - Recognition and reward

Duty of care with respect to promotion or at least pay advancement (broad-banding) is critical. We need to reward employees and provide ongoing wage increases (promotion) rather than being just numbers and expected to chug-along.

* * * * *

Conclusion

A range of common themes emerged in the responses to this member consultation.

Members affirmed the view that S&T was a primary dimension in a hugely diverse range of national security issues and was therefore fundamental to addressing them[1]. The lack of recognition of the important role of S&T in national security was also highlighted with 75 per cent of respondents saying they either agreed or agreed strongly that the lack of visibility of S&T efforts was an important issue[2] and that there was currently a lack of awareness of national security S&T capabilities[3].

The issues of budget and funding were raised as critical issues across virtually every area the survey explored. The need for strong investment in S&T[4] and adequate resourcing generally[5] especially in times of significant economic rationalisation was seen as critical to strengthening our current and future position in a global community in the short and long-term[6]. Poor funding and resourcing was identified as an important or very important challenge by 79 per cent of respondents.

Staff resourcing as the basis of research capability was also an area that emerged as a key concern across many of the areas explored in the survey.[7] Failure to provide appropriate numbers of staff including research leaders with critical experience and staff with diverse skills sets was seen as likely to seriously impact DSTO's capacity to deliver strategic outcomes and respond to ever-changing security threats. Respondents stressed the need to maintain in-house capability in the skills areas essential to developing robust major capability proposals.[8]

The need to have in place leading S&T capabilities and infrastructure was widely regarded as critical for providing flexibility of responses to the diverse and ever-changing threat landscape[9] - for responding to "unknown unknowns"[10] in a technologically-driven world of extreme and growing complexity[11].

Evident also was frustration that while the S&T advice being provided by DSTO was high-quality, their capacity - and the structures in place to allow them - to work with other entities to translate their advice into outcomes was limited[12]. Mirroring this view were comments expressing frustration at the lack of accountability of DSTO for outcomes[13].

The need for coordinated strategic thinking across national security entities was highlighted and the difficulties associated with doing this because of differing priorities, cultures and values[14], desire for autonomy[15], territoriality[16] and stovepiping[17] acknowledged by many respondents. The need for S&T's contribution to national security to be better coordinated[18] was seen as critically important and a way of maximising value for taxpayer dollar. 80 per cent of respondents reported that the lack of knowledge of shared problems across organisations was an important or very important issue[19]. The need for big picture and innovating thinking was also broadly acknowledged.[20]

The difficulties involved in commercialisation and industry engagement were highlighted in member responses. While some regarded the commercialisation of S&T knowledge in relation to national security as "long-term, highly-specialised and commercially unviable", most saw industry engagement and commercial collaboration as an important part of a broad security framework.[21] Some suggested that the public service had not been involved in profit-making ventures historically and that there is therefore a reluctance to engage with IP transition processes – some suggested that a lack of in-house commercial experience may be a contributing factor.[22] These tensions were evident in responses across a range of areas explored.

Concerns with career-related issues were widespread and included the need to value the contribution of professional engineers and scientists who work in national security-related S&T[23], the need to not overload staff with administrative and other non-science-related work[24], the lack of recognition of the importance of the role of professional engineers and scientists in national security[25] and the need to provide appropriate recognition and reward[26] and career advancement options.[27]

We hope you find our input to this important consultation a useful contribution to developing a strategic direction for National Security S&T over the next decade.

About the survey

The survey was set up in Survey Monkey and a link circulated by email to a total of 457 members in defence and defence-related areas in April/May 2014 with two subsequent reminder messages. We received a total of 80 responses so a response rate of 17.5 per cent.

Contact us

For further information, please contact:
Professional Scientists Australia (a division of Professionals Australia)
GPO Box 1272, Melbourne, Vic. 3001
e: scientists@professionalsaustralia.org.au
w: http://www.professionalscientists.org.au/groups/scientists/home/
t: 1300 273 762

Related documents

Other Professional Scientists Australia publications that include content relevant to this submission include:

Still the Clever Country?

Available at
(http://www.professionalsaustralia.org.au/groups/scientists/Still_the_Clever_Country_web.pdf)

Realising Innovation Through Science and R&D

Available at
(http://www.professionalsaustralia.org.au/groups/scientists/Realising_Innovation_Through_Science_and_Innovation_web.pdf)

References

[1] Refer Table 1l and 10a
[2] Refer Figure 6, Table 8
[3] Refer Figure 3, Table 5
[4] Refer Table 1c, 1d and 1m
[5] Refer Table 3a and 3o, 3hh, 9m, 29b and 34k
[6] Refer Table 1h, 3y and 9d
[7] Refer Table 2d, 3l, 3n, 3t, 3rr and 26f
[8] Refer Table 9a
[9] Refer Table 1a
[10] Refer Table 1o
[11] Refer Table 1o
[12] Refer Table 2l
[13] Refer Table 2j
[14] Refer Table 20i, 27j and 3w
[15] Refer Table 12v
[16] Refer Table 2f, 18d and 26q
[17] Refer Table 2e, 2f and 26a
[18] Refer Table 1s, 10l and 10m
[19] Refer Figure 2, Table 4
[20] Refer Table 3kk
[21] Refer Table 3g
[22] Refer Table 3uu
[23] Refer Table 1v, 3p, 9b and 20j
[24] Refer Table 2d, 3u, 9h, 9o, 12i and j and 12u
[25] Refer Table 3t
[26] Refer Table 38 and 1i
[27] Refer Table 9b