pitmans
MAKING IT HUMANLY POSSIBLE

A Call to Economic Arms – Commercial and Legal Considerations in the Defence and Security Sector

In this briefing we examine the implications for business arising from the Government's recently published Green Paper on Equipment, Support and Technology for UK Defence and Security. The Green Paper follows the publication in autumn 2010 of the Government's National Security Strategy (NSS) and the Strategic Defence and Security Review (SDSR). The UK is now perceived to be facing "a different and more complex range of threats",[1] against the backdrop of constrained public finances due to the budget deficit. The Government has placed the focus on the private sector to harness technology, skills and job creation to lead the economic recovery. How should business in the Defence, Security and Technology sectors interpret these policies and respond to the opportunities created? What are the issues and risks and how can they be mitigated?

Introduction

The UK Government is addressing the budget deficit and is relying in large part on the private sector successfully creating and sustaining jobs and being in the vanguard of the economic recovery. With the decline in public sector jobs and public spending, there is renewed emphasis on the importance of exports and of domestic private enterprise.

The Coalition appears to anticipate a response from the private sector, playing to the private sector's strengths - a "can do" attitude coupled with agility in offering solutions. This sense of Government expectation of the private sector's willingness to join in a mission with the state to secure financial recovery will however only successfully turn into reality if, i.) the Government's objectives are sufficiently defined, ii.) there exists greater transparency of Government's future intentions, and iii.) the Government properly recognises businesses' need to be competitive and profitable. Only then will industry have the confidence to invest its money, time and resources in projects which will further the Government's objectives. If the Government can engender that trust then this 'period of austerity' in fact presents exciting opportunities for those businesses which take up the challenge of meeting the Government's 'call to economic arms'.

Defence and Security – the Strategic Context

The publication of the NSS and SDSR in October 2010 represented the most significant review of the UK's defence strategy since the Strategic Defence Review in 1998. The NSS recognised that protection of the realm cannot be defined by reference to 'Defence' in the military sense alone and that 'security' considerations which play into a much wider spectrum of life are an inherent part of the protection covenant to the country's citizens. A new reality has been acknowledged – that the UK is facing, and will continue to face, a different and more complex range of threats than ever before.

[1] P.5 of The Green Paper

The NSS, the written culmination of a detailed risk assessment undertaken by Government, identified key objectives or 'ends', stated as, "*the need to prevent and mitigate the specific risks identified, focusing most on those that are of highest priority.*" [2]

It has provided direction in terms of four key priority threats – the 'Tier One' risks, namely the threat of international terrorism, attacks on UK cyberspace, a major accident or natural hazard, or an international military crisis. The language describing the strategic 'ends' hints though at a theme running through the NSS and SDSR which no observer can ignore - that strict prioritisation (and concurrently a much tighter focus on spend) will be a reality of the means used in achieving the ends.

How then can industry in the defence and security domain position itself to adapt to this financial reality which includes additional cuts from Planning Round 10 beyond SDSR, and yet benefit from the Government's need for the private sector to dig the economy out of its mire?

A starting point for industry?

An understanding and recognition of the Government's key intent is a pre-requisite to industry exploring and then exploiting the opportunities in the defence and security environment. The Green Paper provides a starting point to interpret this with the key issues summarised in basic terms as:

- Providing the right equipment, training and support at the right price at the right time.
- Maintaining access to 'critical technologies and skills' for national security whilst accepting that this cannot be at any price to the taxpayer.
- Using the 'competition in the global market' to meet the national security requirements and to buy off the shelf wherever appropriate. [3]

This summary of intent could well be read negatively by UK industry - financial constraint is at the forefront of considerations and there is risk facing any business which operates in the defence and security domain in the current economic climate. However, it is arguable that those businesses which in fact appreciate the emerging themes from the NSS and SDSR will be in the best position to bring influence on how the Government's intent is realised, and so secure their own economic advantage – businesses will need to help Government "set the conditions" for recovery. This will in turn involve the application of services and products in novel and cost effective ways to deliver into the new strategic space to which Government is committed.

The Green Paper is only a start. The consultation responses and ensuing White Paper will confirm the direction of travel which will be re-enforced by forthcoming Government Growth Strategy guidance and the Defence Acquisition Reform Programme (DARP).

[2] Para 0.17 of the National Security Strategy

[3] See the Executive Summary of The Green Paper

Considerations for the private sector in the context of 'Tier One' risks

The 'threat' landscape identified by the Tier One risks in fact lends itself to some of the core strengths and skills offered by the private sector in the UK - that is that we have both a developed and highly skilled base in innovative high technology industries. The Government has assigned these risks strategic priority and it has also now expressly stated the vital importance of managing two key factors in underpinning UK national security - technology, and the supply of equipment, support and services.[4]

Although technical superiority is but one element of a strategy which recognises the equal requirement for effective soft power, the very nature of the Tier One risks is such that dealing with them requires constant innovation and technological development. International terrorists actively utilise, and understand the power of, advanced technology as a means to further their aims; dealing with the threat of extreme natural hazards involves sophisticated planning using advanced technology as much as, say, deploying troops in the UK to deal with civil emergencies when they occur; UK military operations are reliant on advanced technology in equipment and systems which need to be serviced and the technology constantly refreshed in order to stay ahead of the threats. Recent campaigns also demonstrate the multi-national nature of responses to international crises, with coalition operations dependent on the ability to interoperate both procedurally and technologically. Much prominence has been given recently to dealing with the threat of cyber attack, the Government having published a dedicated Cyber Security Strategy in 2009 with a further consolidation due later this year. The cyber domain, by definition, will draw heavily upon the skills and capability of the technological community.

The challenge for the private sector therefore is how it can grasp opportunities presented by the current landscape and strategic impetus but within the confines of current fiscal constraints. The Green Paper provides some indication of those areas on which the Government intends to focus in order to support and fulfil its intent. Understanding of these areas will be one pointer to businesses about how they can plan their approach to fit into and benefit from the strategic picture.

The Green Paper - some key areas for consideration

Pitmans will be producing a series of detailed briefing papers on each of these key areas for industry over the coming months - in summary they are as follows:

Cyberspace

The Green Paper acknowledges the threat, both to national security and from criminal activity, posed by Cyberspace, noting the development of a four year National Cyber Security Programme commencing in 2011/12, supported by £650m investment. The Green Paper notes the relative immaturity of the response and calls for urgent collaborative action involving academia and industry, particularly in areas of skills and capability development relating to Information Assurance. Flexibility, agility and reliability

[4] Para 9 at section 1.2.1 of The Green Paper.

in technological innovation are deemed as necessities to achieve cyber security. These attributes clearly play into the private sector's strengths – industry involvement in cyber security will be an imperative not an option.

Exports

Given the constraint on domestic budgets the Green Paper places a renewed emphasis on the promotion of defence and security exports, recognising the need – where possible – for simplified export control measures as an important indicator to businesses to think more widely than a national market limited by the pressures on domestic spend. With export related manufacturing representing one of the few growth areas of the UK economy this not only presents opportunity for business growth but will retain vital skills and capabilities within the domestic market place.

Support for SMEs

One cannot underestimate the pressures that exist for SMEs operating in the defence and security sectors from basic administrative issues such as late payment, to the cost involved in adapting to rigid procurement processes and fears over protection of IPR. This will not change overnight. However, the explicit desire to harness the ingenuity and creativity within the SME technology sector represents an opportunity that should be closely watched by SMEs operating in the space.

Acquisition Reform

The acquisition process must necessarily flow down from the MOD. Business has long called for reforms to reduce bureaucracy, increase agility and enable industry to make available innovative approaches earlier in the cycle without compromising competition. The Paper commits Government to introduce change which it is hoped will emerge through the forthcoming Defence Acquisition Reform Policy (DARP). A key element of business' ability to contribute and respond will be dependent upon the opportunity to provide innovative and cost effective solutions. This will be an evolving story and one we will cover in greater detail, in due course.

Partnering

An acceptance of the importance of working with other countries and allies to secure the UK's defence and security capabilities signalled by the UK's enduring relationship with US and the recent commitment to develop closer defence procurement relationships with France reinforces that industry must be open to engaging with partners abroad. Such collaboration brings with it the need for UK businesses to ensure that their commercial and legal frameworks are robust and well informed. In planning forward, UK industry still however needs guidance from the Government on the definitive list of specialist capabilities which the UK will continue to provide e.g. SF, CBRN, Intelligence, etc in contrast to those where we will rely on other nations.

Challenges and Practical Issues

There is a pervasive - and arguably necessary – mantra of reigning in the public purse in all of the papers referred to in this piece. We are seeing this in action now with the renegotiation of hundreds of defence contracts. Furthermore, it is anticipated that there

will be an increased exercise of the little used DEFCON 656 - the MOD's standard contract condition allowing it to unilaterally terminate a contract 'for convenience'. When combined with the clear signals of the Government's willingness to embrace the global market if it provides better value for money and the emphasis on open competition, UK companies tendering for contracts in the defence and security space are going to have to offer a competitive advantage over their rivals both here and abroad to stay ahead of the game – earlier pre-competition involvement in helping to specify requirements will be key.

This though is the reality of the situation. Those businesses that want to be successful will adapt to the reality and look to make the most of the wider picture of opportunity presented by the threat landscape, including thoroughly analysing the opportunity for the export of their skills and products, which the Government is actively encouraging[5]. After all, in a globalised world, many of the threats identified by the Government in the context of the UK's strategic security interests are as relevant in other countries similar to the UK – take the natural disaster caused by floods in Australia for example.

In anticipating the challenges and opportunities afforded by the strategic context, businesses should also review their risks. Practically, companies should consider the following issues:

- Understand that contracting mechanisms flowing down from Government through primes/systems integrators to the sub-contractor/SME level will change in the coming months and years. It will not be enough to rely on the perceived certainties of 'this is how we have always done it'. There is now an opportunity to revisit and improve commercial risk management at all levels.

- Be prepared for a tougher stance on the part of Government in contract negotiation or renegotiation of existing contracts. Pitmans can provide advice and guidance on aspects of commercial contract negotiation, T&Cs, flow downs, partnership and teaming agreements and contractual documentation.

- Given the increased emphasis on exports, it is essential that businesses which may be new to the export control environment understand its processes and pitfalls. Export opportunities may be lost if this is not considered early on as part of tendering and contract negotiation processes. Pitmans can assist in familiarising companies with the services provided by UK's Export Control and UKTI Defence & Security Organisations thereby improving company export strategy, capability and opportunity as well as mitigating risk.

- Ensure that your business is alert to the impact of the impending Bribery Act due in force later this year. The risks associated with non-compliance bear particular relevance for those companies with operations or agents abroad. Company directors should be ensuring that in order to mitigate the risk of potential financial and/or criminal sanctions for breach, they can demonstrate that their business has adequate procedures in place to prevent liability for bribery attaching to their company and/or themselves personally. Pitmans can advise companies on corporate governance considerations, guidance on the development of appropriate systems and interpretation of the Bribery Act in order to mitigate the risk of corporate reputational damage.

[5] P. 12 of SDSR and p. 6 of The Green Paper

- The international dimension of both the threats and the opportunities for businesses to engage in this market space mean that increasingly employees are, or will be, expected to work abroad in complex and challenging environments. Companies affected by this should ensure they are alert to specific duty of care issues to their employees in these circumstances. Pitmans, utilising its understanding of the culture of businesses operating in the defence and security market, provides advice to businesses and their employees with a particular focus on the reputational and commercial risks in making decisions concerning recruitment, retention and termination of employees, independent contractors and directors working throughout the world.

The current defence and security environment is unique in terms of the diversity of threats which this country faces. The strategic context is never static but the current analysis and assessment being undertaken by the Government should be used by the private sector as a timely, and indeed wholly necessary, chance to assess opportunities and risks in this space, some of which are highlighted in this paper.

Members of Pitmans' Defence and Security sector team take an active role in understanding the strategic drivers and engaging with the defence and security environment in order to provide informed legal advice to those operating in this domain. As well as advising in the areas outlined above, Pitmans' legal advice extends to a full range of services, including Information Technology, Intellectual Property, Corporate services, Employment and Dispute Resolution.

Jonathan Durrant
Director
T: +44 (0)118 957 0270
E: jdurrant@pitmans.com
W: www.pitmans.com/defence-security