DCPP Defence Cyber Protection Partnership

CORE MESSAGES

1. Strategic context. Cyber attacks were classed a Tier 1 threat to the UK in the 2010 National Security Strategy**.** Subsequently, the 2011 Cyber Security Strategy recognised the scale of the challenge – not least the cross-border, international nature of the cyber threat – meant UK Government action alone would be insufficient: the most effective solutions would come from public and private sectors working together. Additionally, the UK Government is working with likeminded allies on tackling the cyber threat. The private sector owns and operates much of the infrastructure the UK needs to protect, and has the expertise and innovation required to keep pace with the threat.

The cyber threat is not just a direct threat to organisations, but also to the information they hold. The protection of that information is only as good as the security of the weakest link. If compromised, this could lead to adversaries gaining sufficient knowledge of our capabilities to reduce or negate our operational advantage. It is also in the interest of industry to protect their information, as loss of key intellectual property will reduce competitive advantage.

2. The threat. The cyber threat faced by Defence comes from criminals, hacktivists, terrorists, commerical espionage and foreign intelligence services. Government, industry and academic studies all point to the cyber threat increasing on an upward trend, in both frequency and sophistication. Defence as a whole must be prepared to counter these threats, protect capability and increase its resilience through working collaboratively across Government and Industry.

3. What is the Defence Cyber Protection Partnership? The Defence Cyber Protection Partnership (DCPP) is a joint Industry and Government response to this threat. The DCPP was initiated in 2012 and formally established in 2013 by MOD, other government departments (OGDs) and Defence Suppliers working together to increase the resilience of the sector.

4. Who's involved? DCPP currently consists of two Trade Associations, ADS (Aerospace, Defence, Security) and techUK, 13 Prime contractors[i], the MOD, the Department for Culture, Media and Sport, the CESG and the CPNI.

5. How does DCPP take into account the interests of SMEs? The majority of Defence Suppliers are SMEs and therefore they have a critical role to play in protecting the supply chain. Within DCPP, SMEs are represented by the Trade Associations. It is in no one's interest for SMEs to become excluded from the defence sector; hence a guiding principle of DCPP has been to develop an approach that is proportionate, effective, pragmatic, and only requires smaller companies to invest where necessary.

6. What are the DCPP's objectives? DCPP's overall objective is to improve the resilience of the defence sector in the face of increasing volume and sophistication of cyber-attack. It has three strands of work: Information Sharing, Measurements and Standards, and Supply Chain Awareness. Information Sharing seeks to reduce adversaries' window of opportunity by timely sharing of threat and vulnerability information across Industry and Government. Measurements & Standards is about defining a risk-based set of cyber security standards that will be applied to all future MoD contracts and flowed down each project's supply chain in a way that is both proportionate and practical. Lastly, Supply Chain Awareness is focussed on raising awareness of cyber security by briefing a common message and surveying readiness.

7. What progress has been made?

i) **Information sharing.** DCPP chose to utilise CiSP (Cyber security information Sharing Partnership, now part of CERT-UK) which enables the real time and secure sharing of cyber threat and vulnerability information. DCPP has encouraged organisations and individuals to join and actively

participate in CiSP. CiSP is delivering tangible benefits, enabling members to share information and discuss developments within a trusted online community. When one company in a sector is hit, it leaves others in the same sector vulnerable too. Encouragingly we have seen cases where the sharing of information by one supplier has enabled others to put in place the necessary measures to mitigate the threat. Membership of the CiSP is available to both organisations and individuals, of which between 10 and 15% currently come from DCPP members (see https://www.cert.gov.uk/cisp/ for more information).

ii) **Measurements and standards.** A primary objective of the measurements and standards work stream was agreeing the definition of a set of proportionate cyber security controls to be implemented as part of all MOD contracts. These are embodied in the Cyber Security Model which is comprised of three stages: a risk assessment process, a set of cyber risk profiles, and a supplier assurance questionnaire. All three elements have been developed by a joint Government-Industry group and piloted with DCPP partners. This process of collaboration and review will continue as we move through implementation phases.

The risk assessment process sets the level of cyber risk on the basis of the contract. The cyber risk profile sets out – proportionate to that risk – the measures that will need to be taken by the supplier to mitigate those risks. The requirements are progressive so as the risk levels rise, each profile builds on the one before. The cyber risk profiles have been published as a new Defence Standard and are also available on www.gov.uk.

The final part of the Cyber Security Model is a Supplier Assurance Questionnaire (SAQ) which enables a supplier to demonstrate, via (an auditable) self-assessment, their ability to meet the requirements for the level of risk that their contract attracts.

iii) **Supply chain awareness.** There is an ongoing programme of engagement at cyber related events – conferences, seminars and others. This has been augmented by tailored and targeted communications in relevant publications. There is a dedicated Communications Working Group managing all this activity and developing further ideas to reach the target audience across Defence.

8. What are the timescales? Formal rollout of these cyber-security measures in all new Defence contracts during 2016. It is likely that these measures will be applied to some existing contracts where they are considered particularly vulnerable to cyber threats. In advance of such consideration, three things must be completed: further pen-testing of the risk assessment and supplier assurance questionnaire; the development and testing of an automated tool to gather and store data; and the agreement of a supporting commercial framework.

9. The Cyber Security Model and cross-government alignment. In 2014 the Department for Business, Innovation and Skills (BIS) on behalf of the government published the Cyber Essentials Scheme (CES): a set of five technical controls that all businesses were recommended to achieve. GCHQ has estimated that the Cyber Essentials Scheme would prevent up to 80% of currently successful attacks. The DCPP recognises Cyber Essentials as the basis for good cyber security practice and has incorporated it as the foundation of the Cyber Security Model. The lowest DCPP requirement ('Very Low') requires only that the supplier achieves Cyber Essentials, with all other levels requiring Cyber Essentials Plus in addition to the DCPP specific controls. It is recommended that all suppliers achieve compliance with Cyber Essentials in preparation for the implementation of the Cyber Security Model for Defence. DCPP's Cyber Risk Profiles have been mapped to other current industry standards, thereby protecting companies' existing investments in achieving cyber security measures. It is recognised. All credible studies and predictions point to the nature of the cyber threat evolving over time and therefore all elements of the Cyber Security Model will be subject to an ongoing process of review and periodic revision.

10. DCPP membership. The Partnership as it currently stands is a collective of like-minded organisations and companies, who met three criteria: they delivered a significant value of contracts to MOD; had both expertise and commitment to maintaining an ongoing contribution to the DCPP; and were willing to do so without seeking to pursue business development opportunities. However,

wide engagement is critical to meeting DCPP's objective and we remain keen to have other interested parties participate in our work.

11. Alignment with other approaches. In defence internationally, DCPP has been a guiding influence on the development of the NATO Industry Cyber Partnership (NICP) and is closely aligned with the US defence sector, with the intention of establishing reciprocal recognition and hence minimizing duplication of effort for suppliers operating globally. In addition, DCPP has ongoing conversations with representatives involved with cyber assurance approaches being developed in other sectors with a view to sharing best practice.

12. Where do I go for more information? Keep visiting the information found at www.gov.uk (please use the search function for 'DCPP'), where further details on the Cyber Security Model will be published in due course. Contact your defence Prime[ii] or Trade Association, join the DCPP Linkedin group or contact the MOD DCPP team at issdes-dcpp@mod.uk.

[i & ii] Airbus, BAE Systems, BT, CGI, General Dynamics, HP, Lockheed Martin, Qinetiq, Raytheon UK, Rolls-Royce, Selex ES, Thales and Ultra