APPG ON CYBER SECURITY MEETING ON CYBER SECURITY MINUTES

Title: The Cybersecurity Maturity Model Certification (CMMC), an examination of what the programme is, how it works and whether it should be adopted in the UK?

Chairman's welcome – The meeting chairman, Lord Arbuthnot of Edrom, opened the meeting by thanking everyone and in particular those from the US. The meeting will cover the US Dept of Defense's cyber security programme for their suppliers. It will examine what the programme is, how it works and whether it should be adopted in the UK? It will also look at the effects of the programme on UK firms who sell to the US Dept of Defense.

Present: Lord Arbuthnot of Edrom (Acting Chair), Tony Lloyd MP

Apologies: Simon Fell MP (Chair), Baroness Pauline Neville-Jones**,** Lord Mackenzie of Framwellgate, Lord West of Spithead, Rt Hon Sir George Howarth, MP

Speakers:

1. Rear Admiral (RDML) William Chase
Deputy Principal Cyber Advisor, OSD

Recently transferred from Joint Staff J6 as Deputy for C4/Cyber, comes with deep appreciation for importance of allies and partners and the need for interoperability. This is certainly true in cybersecurity and those partnerships must include industry. It is not enough for DoD to harden our own systems; our Nation's adversaries will always keep trying and will look for the most insecure part which could be anywhere in the supply chain. In that respect, we share risk with and depend on commercial industry, the defense industrial base and our international partners to also safeguard our data. As we look at the challenges surrounding the loss of the intellectual property, the cyber security maturity model certification (CMMC) offers a means to raise the bar for cybersecurity across the defense industrial base.

Welcomed the opportunity to discuss with APPG as it addresses two of lines of effort in DoD's Cyber Strategy: looking at protecting and advancing competitive advantage through private partnership (including critical infrastructure and the defense industrial base) and strengthening our international partnerships.

This is the beginning of a journey on maturing cybersecurity culture, not the end. As we come to terms with this, we must look at how to assess the industrial base. Self-attestation alone has not worked so looking to do this through a 3rd party certification. We have begun a pilot at CMMC Level One which is the lowest bar (of Five). CMMC is at the beginning of the journey which will finish in 2026. We are looking at reciprocity, other certifying bodies, how to synchronize across all of DoD acquisition, and how to harmonize the process when it involves partner nations. There are lots of opportunities to be had as we set out on this journey. I'll pause for a deeper discussion on CMMC and remain online for questions.

2. **John A. Weiler**
Chairman, CMMC Center of Excellence (CMMC-COE.org)

Thanked the APPG for the opportunity to collaborate. Admiral Chase is spot on in talking about partners and allies. JW talked to slides 3 and 4, talking about the CMMC programme. Main aim of CMMC is to ensure that a contractor can manage the information relating to a global weapon systems programme. Cyber Standard 800 - 171 was commissioned by NIST and the DoD CIO. It recognised that other standards did not sufficiently protect the cyber side of an enterprise esp. with smaller sub-contractors

Critical research and R&D investment have been stolen by enemies without any remediation. It allows our enemies to gain an equal footing with the US and its allies. Future wars will be cyber intensive. Cyber security will therefore be crucial in future wars. CMMC moves the self-attestation process on as this was not working. JW is putting together the structure, guides and co-operation with the DoD funded institutions such as Johns Hopkins. Objective of CMMC is to create a level based system (1 to 5) that allows suppliers to transition from the current self-attestation approach to an audited framework. Recognising that a 3rd party needs to verify a supplier's ability to meet the standards.

Also working on a training system to educate suppliers. Aim is to have better protection against theft. CMMC is not a do all, fill all concept. It needs to be more than compliance but resilience and understanding how to apply standards to better protect against a threat. Today the Office of the Under Secretary of Acquisition and Sustainment has issued an Interim Final Rule to DFARS that from 1st December the self-attestation will be backed by a more rigorous audit programme. This is forward looking not backward looking. Rules will be more rigorously enforced though. There is an appeals process and DCMA will adjudicate on this. The defense industry has a number of voices to represent it (e.g. Professional services council, Defense ISACS). Need to apply globally and to have a shared view going forward.

US Congress shares a view that something must be done about cyber security. Cyber Space Solarium Commission[1] was instituted to look beyond the CMMC framework. Supply chain risk management is a great challenge. The US has found foreign technology that it was not aware of. Has founded the National Information Assurance Partnership to assist with this. Important to set where each party as regards levels and ensure that the good work is shared and understood to secure the supply chain.

Slide 6 - Come Jan 2021 the DoD will start to deploy the CMMC framework, initially there are likely to be around are 15 programmes identified, which will have CMMC cyber security maturity levels applied to them. Contractors and subcontractors will require an independent CMMC certificate if they are to be awarded a contract. Certificates which can only be awarded

[1] https://www.solarium.gov/report

by accredited individuals from accredited third-party Assessment Organizations. Organizations and individuals which can only be accredited by the CMMC Accreditation Bod.

3. Andy Watkin-Child CSyP, MSyI, CEng, MIMechE, AMAE
Chartered Cyber security professional, risk advisor, CISO
Has been working the CMMC working group in the US for 6 months to help develop standards. CMMC will have an impact on the UK defence industry.
Slide 7 shows that the US takes cyber seriously. In 2017 cyber security was embedded into procurement standards as shown on the slide. The challenge over the last two years has been that not everyone abided by the rules and IP was stolen. This led to the DFARS case 2019-DO41 to come up with a new way forward.
Slide 8 On the 29th Sept the Interim Final Ruling was issued by the Department of Defense and will come into force on the 30th November. The Interim Final Ruling is a 2 part ruling. Part 1 requires organisations to assess their compliance to NIST SP 800–171 110 security practices using the DOD Assessment Methodology and input their result into the DoD's risk system (SPRS). This is the basic net assessment for where an organisation is. The DoD can complete a desk top assessment at a medium level or on site visit at a high-level . That will have an impact on the global defense industrial base.
The 2nd part is CMMC which creates 1 – 5 levels of cyber security maturity. Most organisations will start at LEVEL 1 or LEVEL 3. These include the 110 NIST security practices and as maturity levels increase so does the complexity. The DoD has made it clear that compliance must be proved prior to award. You must prove that your sub-contractors have input results into the DOD SPRS System as well. The IFR is clear that results must be put in by a contractor in order to be awarded a contract.
Part 2 stipulates that the audit must be done by a 3rd party assessor, accredited by the CMMC Accreditation Body, who work for an accredited 3rd party assessment organizations.
Slide 9 This is the legal wrap around the standard. AW-C talked through the slide in detail.
DFARS clause 2019 requires contractors to complete a NIST SP 800 – 171 assessment.
7020 puts the onus on contractors to allow the DoD to access their facilities to complete medium and high level assessments and contractors to ensure their subcontracts have input their results into SPRS prior to subcontract award.
7021 mandates CMMC compliance that contractors and sub-contractors have certification in place.
Slide 10 – CMMC will have a significant impact on the global defence industry. This requirement has been in place since 2017 and the costs are on the contractor. This will therefore create a financial challenge for compliance to the 110 security practices. If you have self-attested in the past that you comply, the assumption is that you do.
JW – the DoD has projected an allowable cost to help companies move up to the standard.
The rules imply that contractors understand contract information flow and understand where it is so that they can apply the relevant controls. This implies an overhead. CMMC can only be carried out by US citizens or US owned accreditation companies. Sure that the MOD will have issues with this. It will create some challenges.

NIST sets high standard, 110 security practices which may be higher than those adopted in the UK. It could create a 2 tier system.
Lincoln law -litigation tool used and taken seriously by the Federal Govt who took £3bn in fines in 2019.
Slide 11 – CMMC presents a number of challenges. The decision is economic one and has to be made at Board level.
The DoD is just taking international standards and applying them over its supply chain as a contractual obligation. Have to work together on this. Need reciprocity in cyber standards. Could have an economic impact.
RDML Chase - commented that he agreed that we should not apologize for the setting of a higher level of standard—it is needed. We can argue about the implementation, and now is the time for a transparent process to get the comments in to get it right. We welcome the feedback and we need all partners to collaborate in fully—both the Defence Industrial Base (DIB) partners and partner nations.
JW – almost 30 days left for the commentary period. CMMC welcomes input from the House of Lords and the UK in general, thoughts on how to embrace reciprocity would be welcome.

Open questions and discussion

Lord Arbuthnot cited *Ghost Fleet*[2] and thinks that this is an important step and hopes that like-minded allies can take similar steps.

Tony Lloyd MP - fascinating conversation. The recent debate in the UK around Huawei was interesting as it divided opinion. Either it was a US / China trade dispute or was a real problem around cyber security. Some experts thought that Huawei could be part of the UK system and others disagreed. If we are handed a standard it will lead to doubt about political influence. How objective is the intellectual authorship of the standard so that there is buy-in by US Allies as well as the DoD. The process is in everyone's interest.

Secondly, how do we ensure that UK industry is properly informed about CMMC?

John Weiler (JW) – the integrity of the standard and absence of bias – having worked with National Institute of Standards and Technology (NIST)[3] on 800-53 about computer controls, it is not specific to any source of technology but around a wide range of threats and dis-functions. CMMC's intention was not to call out any bad actors or participate in a trade dispute but to be part of an auditable system.

Huawei issue is a good point. Driven by Section 889. Those in the know, through testing and other mechanisms, the US has been able to identify problems with the supply chain. Supports the view that there might be unknown vulnerabilities. Supply chain risk management is outside of

[2] https://www.amazon.co.uk/Ghost-Fleet-Novel-Next-World/dp/0544142845
[3] https://www.nist.gov/

CMMC. Other agencies are also adopting CMMC, including GSA, NASA, DHS and DOE. We are integrating them into the CMMC-COE.org efforts

Andy Watkin-Child (AW-C) – what differentiates CMMC is that it is based on NIST which is used by lots of industries globally. The controls regime is similar ISO 27001 You could argue that the standards can be influenced but lots of people are looking at it. Personally quite comfortable with it.

It is a commercial decision by suppliers to participate in CMMC or not. If they do not comply, the DoD will not buy.

Finally, nothing here that is not good practice. Keen to work with APPG members and the Government to influence and engage with the right people in the UK.

RDML Chase – With regard to the NIST standard, I have not heard complaints. CMMC has not been challenged foundationally. I have heard concerns from industry about implementation and that what the open comment period is for-- to have transparent way for all partners to participate and get it right. It's about getting our contracts designed to combat IP theft. We welcome the chance to be educated on the concerns.

Lord A – huge cost in not doing something like this. The more IP is stolen form the US, the more likely that we are to face weapons created with US technology.

Tony Lloyd - very comprehensive, UK would want to respond to this.
JW – encouraged APPG participants to respond to consultation.

Lord A – advised people to join the APPG.

Graham Mann – totally agrees that such a standard is necessary. Concerned that once you start to go down the sub-contractor chain, you will get into organisations that will struggle significantly to meet the standards. How will they meet standards?

AW-C – generally speaking, in the UK if we want a cyber-robust economy we will need the requisite number of trained individuals. This comes down to Govt. policy. There are around 2 or 3m people shortfall globally. In my view, companies will have to comply so people will need to be trained. Why would you not do this anyway? Cyber is a significant problem

Kevin Borley (KB) – single biggest challenge is to get executive management to understand the detail and the risk. Major concern is that the balance sheet and short-term returns outweigh support for technical fixes.

Lord A – are things changing?

KB – risk and the scale is changing faster than Boards can cope with. Insurance is happy to facilitate the payment when a cyber attack takes place.

JW – great perspective, please send your comments to us?

KB – has sat at the Board table of City institutions who are happy to pay the money out on the risk.

AW-C – cyber insurance market is coming to the conclusion that they do not have the money to cover the risk. The insurance industry needs a set of standards and CMMC is perfect for this.

Boards generally do not get it. CMMC has got teeth.

KB – the way that this is coming together, taking in to account reciprocity is a transformational moment.

Curt Parkinson (CP) – heard cost coming up a few times. You do not need to break the bank to be compliant. Using multi-factor authentication as an example: you can spend millions of dollars on this and no-one will tell you that you are wrong. Some companies off free licenses below a certain number, the result is the same. Are you achieving the controls is the key question, do not let cost be a barrier? A lot of CMMC controls are paper driven ones.

Lord A – all too often Boards will think which piece of equipment do I need to buy not what sort of understanding do I need.

JW – spot on. Cited some vendors who sell themselves as CMMC level compliant but are not, they use the fear of compliance as a motivator to get companies to invest in new technology. JW is working on sorting this out.

CP – SMEs try to meet compliance with the Cadillac version no the Yugo which achieves the same result.

Conclusions –

AW-C – this is coming and will have an impact on the UK Defence industry base. We have a choice to comply, looking for help to support the UK defence industry. Standard is a fit for purpose one and there is an economic cost to not complying. If not careful, we will have a two tier system, UK standards are not as high. Issues faced are the same as are threat actors.

JW – Reiterate that this is a global market for IT and weapons systems, here to collaborate for the common good. Let’s bring together experience and take advantage of collaboration.

RDML Chase – really appreciated the discussion on risk. Cyber risk is becoming more understood at executive / Board level, but we need to make sure we understand that we go the last step and understand risk in context as risk-to-mission or risk to the company/product. That's really what CMMC is about—protecting competitive advantage in DOD missions. Thanked the APPG for engagement.

Lord A – thanked the speakers and the audience. Please sell the concept of joining the APPG.

Next meeting – 25th November at 11.00 Matt Warman, Parliamentary Under Secretary of State (Minister for Digital Infrastructure**)**