RM3764.3 - Cyber Security Services 3 (CS3).

Summary of feedback from Customer and Supplier Engagement Sessions.

Engagement events took place during June and July 2019 as follows:
14th June - London Customer and Supplier workshops
27th June - Supplier Webinar
16th July - Manchester Supplier workshop
16th July - Customer Webinar

In addition to feedback at the events all those who registered were asked to complete an on-line survey. The same questions were covered at all events.

A total of 140 suppliers attended events, or completed surveys.
A total of 20 customer organisations attended events, or completed surveys.

1. **What route to market do you currently use to supply services to Public Sector?**

The most popular route is GCloud. Other CCS frameworks used include Technology Products 2 (TP2), Digital Outomes Speciaists (DOS) and Digital Applications Solutions (DAS). Non CCS routes were MoD's FATS framework, OJEU, direct contracting with customers via Tenders portal, or from customer approach.

Direct award is seen as important to customers, especially for more urgent requirements.

Cyber Security Services 2 (CS2) was mentioned, but said to be "not good". One supplier said that they were awarded a place on the framework, but only recently obtained NCSC certification. This meant they could not contract with customers via this route.

2. **What filters would you think would be helpful to differentiate the services offered on the DPS?**

A number of filters were mentioned: service types, clearance levels, location, accreditations, CNI sectors, previous experience, price levels, length of contract, nationality of operatives, sovereignty, turn-around times (e.g. for incident responses).
Concern was expressed that too many filters could have a negative impact on competition, especially for SMEs.

3. **What would discourage you from applying to get on Dynamic Purchasing System (DPS)?**

- High levels of competition could make the roles less desirable to work on.
- "It turns into a cattle market very quickly with all the agencies that receive the roles".
- "It makes your levels of work extremely high filtering through all."
- Turn around for the client slow and very likely they will be off the market by the time does come for an interview.

4. **What information / guidance would be helpful from CCS or NCSC?**

Responses show a clear steer for better guidance from CCS and NCSC.

- How CCS will advertise the DPS and drive buyers to use it.
- Supplier points of contact published.
- A detailed guide on becoming accredited.
- Details of the management information overheads in terms of reports and returns etc. and pricing information around the costs both up front and recurring to be certified by NCSC to trade on the DPS and then from CCS to administer the DPS (1% of revenues?)
- Joined up certification process and clarification on who does what.

".. significant improvement in the marketing to buyers and suppliers and guidance around Cyber 2 and Cyber3. This was not adequate for Cyber 2"
"Customers want more information about hoops suppliers have to jump through to get onto framework - ie.. what does NCSC assurance mean?"

5. **Regarding Call-offs, what would be effective for fulfilling cyber requirements?**

Responses covered a range of subjects: contract term, pricing, terms and conditions.
For contracting there is a steer for simpler and standardised approach, using plain English.
Customers want the Public Sector Contract to be flexible:
"Idea of a bolt on so that customers can choose appropriate T&Cs for their special requirements".

Both Customers and Suppliers are concerned about terms for I.P and limiting liability.
"..Public Sector clients have a track record of applying IP terms that preclude suppliers from any rights to project specific IP and foreground IP. The notable exception is MoD. Will CCS be recommending any changes in this regard?"

Pricing models should include fixed price, plus clarity about how maximum day rates will be set. Clarity about how expenses are covered. Suppliers want clear views of response times required and rates to be applied. Hourly rates for incident response requirements.

Call off terms should be flexible with option to extend. Minimum of twelve months mentioned. For the DPS term, 2 years mentioned with 1 + 1 extensions.

6. **Assurance**

A number of responses mentioned the time it takes to get accredited (several months) and the cost involved being a blocker. Will the volume and value of work make it worthwhile? Clarity is wanted on the assurance requirements: " good guidance required to help make process more seamless".

One concern was the difficulty for named individuals achieving certification. Another was concerned about having an overlap between CS2 and CS3.

Questions asked included:
- What is the mandation around assured services?
- Prime vs Sub - how does this work?