IoT Security Foundation Executive Steering Board
Follow-Up Notes and Actions From
Thursday 23rd January 2025, Virtual Meeting

0   Agenda

1. What do we want to achieve in 2025?
   a. Roundtable: Significant Themes
2. Specifics To include
   a. Leveraging Assets:
      i. Procurement Proposal / Assurance Framework
      ii. Policy Papers: e.g. BoM's
   b. Chapters
      i. Tamil Nadu
   c. Themes and Working Groups
      i. Development/evolution of existing WG's
      ii. New? Member-led / Physical plenary
      iii. DeviceID
      iv. DSbD/Memory Safety?
   d. Conference
3. AOB / Next Meeting

0.1   Attendees

Stephen Pattison (SP), John Moor (JWM), Darron Antill (DA), Haydn Povey (HP), Sarb Sembhi (SS), Nick Allott (NA), Peter Davies (PD), Anna Maria Mandalari (AMM), Richard Marshall (RM),

Observer: Chris Bennison (CB)

0.2   Non-attendance for ESB meeting
Tim Snape (TS), Carsten Maple (CM), Ken Munro (KM)

These notes are to be read in conjunction with slides '51 ESB Virtual Meeting Jan 2025.pdf' and supporting documents available on basecamp: IoTSF ESB Communications > Docs & Files

1   What do we want to achieve in 2025?

It was reaffirmed that AI, edge computing, data and standards are enduring/evolving themes.

AMM provided some useful links to the CEN standardisation process
- https://standards.iteh.ai/catalog/tc/cen/22ac58f4-646e-42fc-b2d4-86c57e0064eb/cen-clc-tc-13

and the Eu's Cyber Resilience Act
- https://standards.iteh.ai/catalog/tc/cen/79a73458-f0c9-4d87-823e-c1d80b647da8/cen-clc-jtc-13-wg-9

and ETSI
- https://www.etsi.org/technologies/consumer-iot-security

RM noted that matters could be described as 'getting turgid' in CRA as the Eu wants to move faster but there are vacancies for rapporteurs. He also noted that EN18031 was being suggested for a live date of Aug 1st 2025 (this year). He concluded that the regulation may come late or be sudden.

W.r.t regulation, it was noted that there are examples of the unintended consequences of existing regulation – including trade sanctions. PD gave an example of the area of health equipment and creating an environment for manufacturers that was unintended. He also noted the relationship of security to safety and that safety may override security concerns - especially in safety-critical systems - as illustrated in the conclusions of the RESauto (CHERI-based) project – where the acceptable outcome would be to fail-safe (not denial of service).

In the light of geo-political changes – notably the inauguration of the Trump administration - the question was asked: *"are we comfortable IoTSF is pro-regulation?"*

The sentiment across the group was that the 'tide has turned' on regulation and, at the political level, the emerging emphasis is on growth and de-regulation.

A discussion ensued that reaffirmed the value of IoTSF – despite our lack of significant engagement with 'the big 7' tech companies. We must remain independent and agile as companies are looking for best practices and guidance as the world continues to develop quickly in a confusing landscape.

1.1 Conclusion:
We should stay true to our founding spirit of providing expert guidance and thought leadership.

IoTSF is not just about regulatory compliance, the thrust of best practice is good, we should not be seen to push regulation (it's the position of last resort), we will maintain our activity with regulation but we should emphasise efforts on commercial considerations including security practice, innovation, guidance and applications (markets and growth).

2 Specifics

2.1 Procurement Paper
NA walked through the procurement strategy paper circulated before the meeting.
It was noted that
- IoTSF's highest value asset is the Assurance Framework and we should look at how we can leverage this further by positioning in the purchasing process.
- It has utility for buyers and vendors

- Sector specific product/service offerings are possible.
- Can we use it more specifically to overcome the bureaucracy of purchasing which can become a heavy burden in certain sectors – for both 'primes' and SME's?

The general consensus was that exploring the use of the Assurance Framework to help streamline the purchase of common/bespoke security requirements could be beneficial for our members and potential new members.

It was concluded that we should take the next step of producing a paper proposal to help socialise the idea with key stakeholders before firmly committing resource

ACTION: NA, PD, SP and JWM to form a sub-group to develop the proposal – essentially a 'next steps' paper and a 'strawman sales pack'.

In the process, it is essential that:
- Anti-trust aspects are covered (considered as 'a must').
- Ensure IoTSF does not become legally liable. This would be a service "to the benefit of the members".
- Resourcing (IT, legal) 'behind the scenes' requirements are defined/estimated
- Gain feedback from members and user archetypes

ACTION: Update to be given at next ESB.

2.2 Producing Policy Papers

The aspiration remains strong however it was noted that we lack a system for creating policy papers. Perhaps it starts with the ESB group?
No conclusion – roll forward.

2.3 Tamil Nadu State-wide Chapter Proposal

After a short discussion, it was agreed that we should accept the proposal and encourage the leaders of the Chennai Chapter to further develop the activity yet monitor progress carefully.

ACTION: JWM to notify the Chennai leadership their proposal has been accepted.
ACTION: CB to support the logistics of the change in status.

2.4 Themes and Working Groups

2.4.1 DeviceID

We discussed the importance of DeviceID's w.r.t cybersecurity as a foundational mechanism. There is member-driven appetite to explore the possibilities of bringing more focus to the topic within IoTSF.
This is a nascent activity and more skin is needed to be put on the bones, and more interested parties are recruited.
It was noted that this work could carry forward 'approx 70%' of the activity already established within the ManySecured WG.

DA noted that his team will participate.

ACTION: JWM / NA / DA to drive progress, test interest, develop the vision, mission and plan.

ACTION: Update to be given at next ESB.

2.4.2   DSbD/Memory Safety

It was noted that both the Secure Networking by Design (SNbD) project (from IoTSF) and the RESauto project (from AESIN) have been completed and the UK funded Digital Security by Design (DSbD) programme was nearing completion.

As part of the final delivery, we have published a 'Global Marketing Report' for the SNbD project, which outlines the opportunity for a CHERI-based / ManySecured router and the real/perceived barriers to deployment. See the IoTSF website: https://iotsecurityfoundation.org/time-to-fix-our-digital-foundations-a-new-report-on-memory-safety-and-secure-networking/

A discussion followed as to what IoTSF (and TechWorks) should do to maintain the awareness around 'memory safety'.

It is not clear what can be done longer term at this point as we do not know whether the programme will get follow-on funding from UK Government or not. The final determination will affect our plans.

In the meantime, IoTSF will exhibit at the DSbD showcase in London on Feb 11 and monitor the situation regarding programme funding. Note, both PD and JWM are on the DSbD Advisory Board.

ACTION: Update to be given at next ESB.

2.5   Conference

JWM noted that we have not yet booked the venue but aim to return to the IET on Oct 15. Due to time limitations, the discussion was limited.
ESB members were invited to make suggestions for invited keynote speakers.

3   AOB

AMM (UCL) has submitted an ad-hoc proposal to the UK Government (DSIT) for an IoT device testbed through the Digital Catapult. IoTSF has been included in the bid as a partner.

DA reminded JWM of the relevance of MissionLink UK – JWM to revisit.

3.1 Next Meeting

~~The next meeting will be virtual at **2 pm on April 23ʳᵈ 2025**~~
Due to the Chairman's availability, the meeting will now take place on 14ᵗʰ May, 2pm

ACTION: JWM to re-send calendar invite