IoT Security Foundation Executive Steering Board Follow-Up Notes and Actions From Wednesday 11th September 2025, Virtual Meeting

0 Agenda

1. Minutes and Actions Review
2. Strategy and Positioning
    2.1. Major themes inc.,
        2.1.1. Memory Safety
        2.1.2. SBoMs
        2.1.3. Defence/CNI
    2.2. Member Value and Recruitment
        2.2.1. Large and small
3. Operations Update
4. AOB and Next Meeting

0.1 Attendees

Stephen Pattison (SP), John Moor (JWM), Darron Antill (DA), Tim Snape (TS), Carsten Maple (CM), Sarb Sembhi (SS), Nick Allott (NA), Peter Davies (PD), Richard Marshall (RM)

Observer: Chris Bennison (CB)

0.2 Non-attendance

Anna Maria Mandalari (AMM), Haydn Povey (HP), Ken Munro (KM)

These notes are to be read in conjunction with slides '53 ESB Virtual Meeting September 2025.pdf' available on Basecamp: IoTSF ESB Communications > Docs & Files

1 Minutes from last meeting

IoTSF Messaging:
JWM outlined the revised messaging and navigation on the IoTSF website following comments from the last meeting.

In general, 'IoT' is increasingly being mixed with other contemporary terms such as 'connected devices' and 'AI'.

A discussion followed about regulatory affairs and that we should not lose sight of the fact that it is still a significant topic of interest – and will continue to be – for current and future members.

ACTION: make sure messaging shows that IoTSF is influencing regulation and maintain the right balance with other messages.

1.1 Review position/activity w.r.t Memory Safety

We have several talks lined up for the conference to continue to support the need for memory safety in embedded/connected systems.

It was noted that recent announcements from Apple on a major new memory safety architecture - Memory Integrity Enforcement (MIE) – is a significant development.

"We believe Memory Integrity Enforcement represents the most significant upgrade to memory safety in the history of consumer operating systems."
"…we believe MIE will make exploit chains significantly more expensive and difficult to develop and maintain, disrupt many of the most effective exploitation techniques from the last 25 years, and completely redefine the landscape of memory safety for Apple products"

See here: https://security.apple.com/blog/memory-integrity-enforcement/

It is not clear at this point how it may affect the industry/UK's plans for CHERI.

Our position remains that we will be technology neutral whilst continuing to support awareness and members interests.

1.2 SBoM's

An update was provided on the actions:
ACTION from May: *CE marking paper: draft - PD/RM AND pre-publish review by NA / JWM / SP*
This action has not made progress largely due to competing priorities and availability of the personnel over the summer period (i.e. PD and RM) – status: hold for review.

ACTION from May: *Write a formal letter to Ollie Whitehouse - setting out our points and asking for clarity on SBoMs - SP/JWM/NA*

There has been several exchanges between IoTSF and NCSC and we are concerned that the UK's position is at odds with much of the world – especially the 5 eyes (e.g. see https://tinyurl.com/ESB-CISA-SBOM-SEPT25).

A discussion followed where we once again asked ourselves (1) do companies have to provide SBoMs? and (2) are they useful?

We confirmed that they are necessary to satisfy regulation – particularly the EU CRA and are aligned with the needs of the Product Liability Directive and US Executive Order(s) (although there is some recent bureaucratic roll-back noted from the Trump Administration is noted).

We also asked whether we can help members with how to use SBoMS? E.g. by producing a practical guide?

ACTION: SP/JWM Respond further to NCSC and be firm - we accept their position cannot be prescriptive but equally they should not be resistive to SBoM's even though the tools and practices are immature – it is the direction of travel and working against this will not be helpful.

ACTION: JWM to solicit views/appetite from the membership as to the need/desire to produce a practical guide.

2 Strategy and Positioning

2.1 Memory Safety

See 1.1 above

2.2 SBoM's

See 1.2 above

2.3 Defence / CNI

ESB members shared perspectives on these themes and explored whether IoTSF could have a proposition to the defence sector and our members.

NA had attended the DSEI UK 2027 event (https://www.dsei.co.uk) and gave his perspective. The following points and discussion summarised as:

- There is an appetite to engage SME's – the Strategic Defence Review (SDR) noted that this is of strategic significance to the UK as part of an integrated plan for defence and CNI resilience together with the role of dual use technologies.
- There is a challenge in the monolithic nature of procurement practice and the evolving need to modularise components without losing overall integrity and compromising the assurance levels. How would it be possible to plug systems together without losing overall quality assurance?
- The defence industry may be able to frame the problem but may not know how to solve it.
- This could be a key opportunity as the defence primes are gatekeepers (read 'in the way') yet also know they need to innovate faster.
- The bigger challenge is likely to be changing the incumbent culture - can we help? And even if we could, would they accept it?
- Could/should we try to broker high level conversations on the supply chain side – it appears to be a big problem.

DA had previously made introductions to the MissionLink organisation and a conversation was had for awareness/opportunity purposes yet no follow-on activity has happened to date as nothing specific was identified.

NA queried the possible purchasing utility of the Assurance Framework - can it be taken in current form as a starting point to talk to vendors?

SP has a good relationship with Alex Creswell from Mission Link and agreed to explore possible avenues for a partnership.

ACTION: SP to contact Alex Creswell, confirm our perceptions and explore whether there could be a useful role for the IoTSF and the Security Assurance Framework in the procurement process – especially for SME's.

2.4 Member Value and Recruitment

Board members discussed the IoTSF value proposition, the importance of our constituent members and how we might improve our recruitment.

NA noted that large companies are difficult to recruit but are important – especially for networking with our SME's.

TS reiterated that regulatory affairs are important – he also noted that IoTSF is mostly positioned to attract technical and engineering staff. Can we have a stronger offering to satisfy company concerns in defending their claims on compliance? This requires further thought/investigation including the legal implications.

NA also felt there was more value to help the procurement process of larger companies if we can be seen to save them time and effort.

We also discussed the challenges of giving the IoT Security Assurance Framework away for free (a decision made in the early days of IoTSF). We asked ourselves whether it would be possible to change the T's & C's of the Framework such that it could be used as reference material for free but a license would be required for real-world use – such a license would effectively be automatically issued to members. Or perhaps we could ask for recognition as a condition of use?

JWM mentioned that we had an idea to provide some member-only tooling to accompany the Framework (better than the member-only spreadsheet) however NA suggested that this may not be as useful for member recruitment as desired – needs more thought.

ESB members also made suggestions as to how to approach membership sales.
JWM outlined that member recruitment is largely carried out through marketing and bespoke biz-dev activities – i.e. no explicit sales function. This generates a steady, yet small, steady stream of membership interest calls where the value proposition is tailored as part of the call.

It was suggested a "sales deck" (as opposed to our introduction to IoTSF "marketing deck) could be a helpful progression exercise – it should be compact.

ACTION: JWM to produce a concise sales deck to pitch to prospective members.

3 Operations Update

See slides.

3.1 SBE

SS gave a short update on the SBE group; the document just waiting on graphic, there will also be a call with SBE group w/c Sept 15 to discuss what next.

3.2 AI

DA asked how the TW-AI initiative is going.
Both NA and CM felt it could do with having a steering function similar to ESB
ACTION: JWM to ensure TW-AI has a steering board by end of 2025

3.3 Conference

The agenda is almost complete – it is more advanced than in prior years which has been driven by the TechWorks team.

Unfortunately, the Minister we had lined up (Minister Feryal Clark) has "stepped back" and is no longer in office. JWM has reached out via contacts at DSIT to try and find an alternative – no response as yet.

ESB members regularly participate in the conference, and several are already on the agenda.

In addition -
PD has agreed to be a session host (defence/CNI related)
CM will also be a session host also and work with NA and JWM to put the final panel (on what the future holds) together.

Thank you to Device Authority and SCI Semiconductor for their loyal sponsorship, and to SP for helping persuade Arm to sponsor (currently in play).

4 AOB / Next Meeting

4.1 AOB

None

4.2 Next Meeting

This meeting was planned to be a face meeting however a strike affected travel in London hence it was switched to virtual to avoid disruption. It is considered important to have a physical meeting before the end of the year, so we agreed to have an ESB meeting prior to the TechWorks Annual Dinner in London with a compact agenda.

The next meeting will therefore be a physical meeting in London, at the Royal Lancaster Hotel on December 3rd – details t.b.c

ACTION: ALL - save the DECEMBER 3rd date - JWM to send calendar invite