

IoT Security Foundation Executive Steering Board Follow-Up Notes and Actions From Wednesday 3rd December 2025, Physical Meeting

0 Agenda

1. Minutes and Actions Review
2. Updates
3. The Next 5 Years
4. AOB and Next Meeting

0.1 Attendees

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

0.2 Non-attendance

Stephen Pattison (SP), Tim Snape (TS), Carsten Maple (CM), Ken Munro (KM)

These notes are to be read in conjunction with slides ‘54 ESB Physical Meeting December 2025.pdf’ available on Basecamp: IoTSF ESB Communications > Docs & Files

Thank you to AMM for hosting us at UCL – greatly appreciated.

1 Minutes from last meeting

1.1 CE marking paper / SBoM's / NCSC

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 September 2025: 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.

Ref ‘CE marking paper’ – as this is an action carried over from May we asked ‘is this still useful?’

Following a discussion, we concluded it would still be useful to produce an educational paper, or a series of shorter pieces in relation to the CRA, UKCA, SBoM's and being "export ready". It will help us get across that SBoM's (and their utility/misgivings) in particular are not just about the utility with security, they are a trade essential.

Comments were made about the impact of the CRA on firms and how it may impact innovation and their willingness to place products on the EU market - notably due to the cyber management costs.

ACTION:

PD and RM to look to co-draft a paper in February timeframe.

NA to review.

Goal for (1st) publication within Q1 2026.

ACTION from September 2025: JWM to solicit views/appetite from the membership as to the need/desire to produce a practical guide [to SBoMs].

No progress due to competing priorities and evolving situation – hold for now.

1.2 Mission Link

ACTION carried forward from September 2025: 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.

Roll forward in SP's absence.

1.3 IoTSF Sales Deck

ACTION from September 2025: JWM to produce a concise sales deck to pitch to prospective members.

ESB members are invited to view and provide direct feedback: <https://tinyurl.com/IoTSF-PitchDeck-Dec2025>

1.4 TW-AI Steering Board

ACTION from September 2025: JWM to ensure TW-AI has a steering board by end of 2025

JWM noted that Gareth Richards' temporary contract would expire at the end of December 2025 and we have not been able to 'align TechWorks-AI with the UK AI zeitgeist' (i.e. membership recruitment is slow) and have not been successful in several public funding applications. This means that TechWorks is not in a position to extend his contract into 2026 unless/until we can find funding. The situation is on-going hence, despite some progress, this action remains incomplete.

2 Updates

Brief updates were given on the annual conference, website traffic and newly launched SIG activity.

The final event report for the conference is pending (due to a succession of follow-on events – including the TechWorks annual dinner) however it is considered a success on all fronts (see slides).

We discussed the importance of getting good/timely feedback from the conference as our response rate was poor - ESB felt capturing immediate feedback at the event is essential.

ACTION: JWM to pass the ‘get better feedback response rate’ challenge to the TW events team.

3 The Next 5 Years

There was an active discussion around the status of IoT, AI, regulation/compliance, secure by default, security by design, technology, applications etc., where IoTSF seeks to remain relevant or, preferably, lead.

Salient points emerged from the discussion that will help us fashion a vision, strategy and plan for the next 1, 3 and 5 years:

- Security through the lens of the sector (e.g. defence, CNI, medical), ecosystem (networks) and product/device assurance.
- The evolution of applications and markets – convergence of OT and AI. The inevitability of AI and IoT edge devices.
- Beyond secure-by-default and security by design, what does a business need? The utility/need for standardised and customised security: “Security by demand”.
- The role of the Assurance Framework as a foundational asset in evidence gathering, sharing of information (transparency) and procurement – throughout complex/overlapping system/product lifecycles.
- Utilising evidence in risk assessment and management. The emergence of the Digital Product Passport (DPP).
- IoTSF needs to help firms with compliance, but it also needs to be looking ahead and helping to shape the agenda.
- The possibility of changing our name to reflect the evolution (next phase) was, once again suggested; “The Security Foundation”.

Status

In synthesis/short summary, here is a strawman for our next meeting in January 2026:

5 years: ‘Security by Demand’ would be a good slogan to get behind (shows thought leadership) for the next phase.

3 years: We should consider how we help deliver ‘continuous assurance’ – based on evidence transportation and transparency – tailored to sector/ecosystem/devices.

1 year: How can we develop/enhance the utility of the Assurance Framework to support Security by Demand – especially in the procurement process? What role of standard profiles as a baseline?

Unfortunately, “The Security Foundation” has already been taken however “The AIOT Security Foundation” is available and would allow us evolutionary path.

Here is what my AI branding consultant saw as the benefits:

Self-explanatory: Instantly conveys "AI + IoT" security as a foundational resource—blending your original IoT focus with AI tech/business integration (e.g., secure edge AI deployments). Unique: Zero organizational matches; AIoT is an emerging term but not claimed. Recognition: Retains "Security Foundation" verbatim for seamless transition; acronym (AIoTSF) echoes IoTSF.

We should also ask: How should we evolve ESB to help us achieve our new vision?

4 AOB / Next Meeting

AOB: None

Next Meeting: Virtual, Jan 28th : 14:00 – 16:00

ACTION: JWM to issue calendar invite