IoT Security Foundation Executive Steering Board
Follow-Up Notes and Actions From
Wednesday 14th May 2025, Virtual Meeting

0 Agenda

1. Minutes from last meeting
2. Operations Update
    a. WG's
    b. Townhall/Plenary
    c. Projects
    d. Funding
    e. Membership and Engagement
    f. Relations
    g. All Roads: CONFERENCE
3. Roundtable
4. 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), Richard Marshall (RM),

Observer: Chris Bennison (CB)

0.2 Non-attendance for the ESB meeting

Anna Maria Mandalari (AMM), Tim Snape (TS), Carsten Maple (CM), Ken Munro (KM)

These notes are to be read in conjunction with slides '52 ESB Virtual Meeting May 2025.pdf' available on Basecamp: IoTSF ESB Communications > Docs & Files

1 Minutes from last meeting

Reiterated the interest of IoTSF is beyond regulatory affairs ('the position of last resort') and there is more value to our members in commercial matters – including the Procurement theme and taking every opportunity to further develop/leverage the Assurance Framework.

Once again, we discussed the utility of using the term 'IoT' as it is regarded by some as a sub-category with 'connected devices' and AI being more fashionable. We asked (once again) 'is the IoTSF name still cutting it?' We concluded that the name is good but our messaging, as well as our activities, need to (continue to) adapt. As an outcome we agreed to 'do some work on this in between meetings' to save future agenda time – i.e. identify more prevalent themes/activities and messaging to be synonymous with the IoTSF brand.

ACTION: SP/DA/JWM/PD to share thoughts on the most noteworthy themes and messaging.

ACTIONS to rolled forward:

Producing policy papers to demonstrate thought leadership and value for members.

1.1 SBoM's

There is a long-standing issue with SBoMs as the UK is out of sync with the EU and US - CRA cites SBoMs as necessary for compliance, and the US is mandates them in government procurement

NA mentioned 2 specific points to separate out:

1. Technical: How they can be used – Useful? Needs a conclusion
2. Commercial: Problem on the international stage

We asked *'should we write a paper and circulate?'* to help raise awareness and share our concerns w.r.t UK position.

We also explored making a formal approach to NCSC to set out our concerns/views and clarify NCSC's position as a simpler option.

PD: Asked "what is most useful to our members" and suggested drafting a paper titled (candidate title) "CE marking on your product - what does it mean?".

This was supported by others as being useful.

ACTION: Write a formal letter to Ollie Whitehouse - setting out our points and asking for clarity on SBoMs - SP/JWM/NA
ACTION: CE marking paper: draft - PD/RM AND pre-publish review by NA / JWM / SP

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

It was also stated that memory safety is a significant source of failure within the realm of the top 5 big electrical suppliers (ABB, Siemens, Honeywell, Schneider etc.) but 80% of attendees at the Embedded World show were largely ignorant of the problem.

It was stated that memory safety is a top 5 DSIT focus area with £15 million funding being allocated to CHERI adoption.

We asked *'How does IoTSF add its voice and where - what's our position - can we leverage the Framework?'*

Should we focus on an educational piece for the embedded sector and ask *'memory safety: what's the problem?'*

Due to time constraints, we concluded the discussion needed to continue outside of the ESB meeting.

ACTION: JWM, HP, SP and PD to further develop ideas as to how to appropriately utilise IoTSF's position in the theme of memory safety.

2 Operations Update

2.1 Regulation / Standards update

JWM noted a discussion with Plexal/NCSC on their forth-coming policy-based assurance scheme – little is known about the motivations and intent behind the scheme hence a call has been arranged to learn more.

DSIT has approached IoTSF asking for assistance with a Call for Views on the Cyber Security of Enterprise Connected Devices.

The Regulatory Watch WG will be invited to formulate an official response – comments made during the discussion include:

- This could add confusion and may not add much (at first glance)
- Enterprise device security is differentiated from consumer however, is this simply an awareness issue?
- The legal liability in the Enterprise is different (see PD comments below), and so is device provisioning – however, it may not add much.

We discussed how regulations and compliance interact with laws.

A concern expressed was that regulations can be regarded as a legal defence, regardless of whether they work - this is a bad situation to be in as it transfers responsibility away - e.g. Garmin device is not medical equipment. Instead, regulation needs to be setup for the outcomes wanted and what Executive Boards' should be concerned about.

This has been seen in the RED discussions with attempts to wriggle out of regulation, and a 'wireless tech alliance' trying to sidestep security with fragmentation issues.

Two laws were mentioned of specifc note:

- 1967 Misrepresentation Act (*English contract law, designed to protect parties who enter into contracts based on false or misleading statements*) w.r.t contractual liability and the company Board
- Computer Misuse Act (*primary UK legislation criminalising unauthorised access to computer systems and data, as well as the damaging or destroying of such systems and data*) 3ZA section (*Section 3ZA was introduced by the Serious Crime Act 2015 to address the most serious cyber attacks—those that could cause or risk causing significant harm to critical infrastructure or society at large*)

We have also been invited by the ICO to help raise awareness of new draft guidance for consumer Internet of Things (IoT) products and services looking at how data protection law applies when processing personal information.

Comment: It is good that DSIT and the ICO recognise IoTSF's expertise in these areas and are looking to collaborate with us and our members.

ACTION: JWM to invite the Regulatory Watch WG to gain consensus on feedback to DSIT's Call for Views on Enterprise Connected Devices

2.2 SBE Working Group

The SBE WG is close to having a procurement paper ready for publication – it just requires graphics.
ACTION: SS to work with IoTSF digital team to produce the required graphics necessary for publication.

2.3 Chapters

JWM outlined progress with the IoTSF Chapters Programme and that attention was needed to meet the expectations of membership growth.
DA: Noted that the Bangalore Chapter, which he has staff involved in, has significant vendors and tech resources - it's seen as a good thing for IoTSF and has a good nucleus of people.

ACTION: CB and JWM to liaise with Chapter leaders and ask how we can grow membership in the Chapters

2.4 Conference

The 2025 conference was launched in late April – it is promoted as IoT Resilience and Trustable AI – a co-located conference with the newly established TechWorks-AI: website is iotsf-ai.org

We are working on the content agenda and a UK Minister has been invited to provide an opening talk – response is pending.

A major challenge each year is covering the operating costs which exceed £50k and we look to cover these with exhibitor space and sponsorships – the sales process takes effort away from front-line activities but is essential.

AI and defence are seen as a hot areas hence good to include in the agenda to help sponsorship.

ACTION: DA to make an introduction to Grace Cassy – CyLOn co-founder and ex-government advisor
ACTION: PD: to help with ideas for defence defence-related section of the conference as necessary.

3 Roundtable

General viewpoints were invited from attendant ESB members:

PD: emphasised the commercial and operational value to members in aspects of what we do - e.g. IoT to be more viable and reliable - compliance is good but what is driving adoption?
HP: echoes PD's view – adding we must differentiate – help show how to implement systems
HP also commented newsletters and webinars are good; however there is room for improvement on the website - it should be more dynamic where it is easier to find resources, find ideas, find guidance, how to acquire knowledge – show why we exist? We should further leverage the Framework as the embedded industry struggles with regulation and 'how to' meet it.

JWM added a note of gratitude to all ESB members as their insight and guidance is valuable in guiding the prioritisation and selection of activities we undertake as we are always challenged by resources.

SP summarised and emphasised the value of what we do and that we must not lose sight of the industry we are serving. We need to be more ambitious with attempts to attract the blue-chip companies however, there is plenty to be optimistic/enthusiastic about.

4 AOB / Next Meeting

4.1 Next Meeting

The next meeting will be a physical meeting in London on Sept 11th – details t.b.c
ACTION: JWM to send calendar invite