Can you briefly describe what the Joint Task Force on IoT Security is, and what are its objectives?
The Global Certification Forum (GCF) and the IoT M2M Council (IMC) have agreed to form a Joint Task Force on IoT Security. This Joint Task Force (JTF) will evaluate whether it is possible to create a set of global standards for the security of IoT deployments that truly adds value, and if so, what that standards set might look like, and how it might be certified. Key to this effort will be analyzing existing standards/certifications and assessing their efficacy, while identifying gaps where more work is needed.

Participation in the JTF is non-binding, and the following companies have agreed to participate in advance of the first meeting in early February 2025: **Aeris, Anritsu, AWS, Cisco Systems, DEKRA, Digi International, Element Material Technologies, Eurofins, filancore, Finite State, Giesecke + Devrient, Globalstar, Keyfactor, Keysight, MultiTech, Qualcomm, Quectel, Rohde & Schwarz, Samsung Eletronics, SGS, Somos, Tartabit, Tata Communications, Telefonica, Telit Cinterion, Thales, TUV, Verizon,** and **Vodafone**.

It seems like there are hundreds of initiatives for IoT-related security – what makes this one different?
Two things make this project different:
1) The JTF will attempt to address all layers of the IoT stack, not just devices, but also the cloud/app and network layers. We just don't see how IoT security can be improved significantly without taking this holistic approach. Most existing standards/certifications concentrate primarily on devices or "last mile" topography.
2) The JTF will attempt to be more prescriptive and practical in its approach than is currently common. Most standards/certifications today concentrate on outcomes – e.g., "you must be impervious to attack" – but they don't offer advice on how to get there. We will attempt to provide hands-on, practical approaches to achieving more secure IoT deployments.

It sounds like the scope of this project could be enormous – is what is being considered feasible?
There is no doubt that the scope of the JTF on IoT Security is ambitious, to say the least. Major questions remain about the ultimate recommendations of the group. How will all layers of the IoT stack be covered, and how might that be automated? How will this effort integrate with or supplement vertical-market initiatives, such as those for the medical device, automotive, or critical infrastructure? How will prescriptive standards be curated and not go out-of-date? It's clear that phased approaches that concentrate on certain vertical markets or technology layers may be necessary. It will be the task of the JTF to see that these questions are answered.

Why should the IMC and the GCF be the organizations to manage this initiative?
The GCF will bring to the project broad and deep knowledge of the landscape for

standards/certifications, including existing relationships with all of the pertinent standards development organizations (SDO's). We know of no other organization that certifies more devices currently (over 600 annually) than the GCF – IoT devices that it certifies now outnumber handsets – and the group is now branching out into the certification of networks with its Mission Critical Services Work Stream.

The IMC will bring the technical expertise of its Board of Governors, which include over 30 of the most influential companies providing IoT solutions in the form of hardware, software, and networked connectivity services. As the largest association dedicated to the global IoT sector, the IMC is comprised of 28,000 qualified IoT users covering 30 different vertical markets, with roughly 30% in North America, 20% in Europe, and 25% in Asia. Direct communications channels to these constituents will be key to market acceptance of JTF proposals.

Neither the GCF nor the IMC is a Standards Development Organization – how will this work?
Fine work has been completed by numerous SDOs on the subject of security for connected devices and the systems behind them. The core task of the JTF on IoT Security is to evaluate existing standards and recommend those that are determined to add intrinsic value, most likely in combination with other existing standards. It is a core tenant of the group that we will use existing standards that are in the public domain to the greatest extent possible (only with complete permission and attribution, of course).

What will be the JTF's relationship with regulations and regulatory bodies?
This remains unclear, though no direct relationships are expected. It is our hope that recommendations developed by the JTF will influence policy makers around the globe and we certainly encourage policy makers to participate In the group. Special consideration will be given to government or government-adjacent participants.

What is the expected schedule for the JTF look like – when can we expect tangible work product?
The very first meeting of the JTF on IoT Security will be on Thursday, 6 February 2025, with monthly online meetings occurring throughout the coming year. A hybrid (live and online) meeting will occur just prior to the **embedded world** exhibition in Nuernberg, Germany on Monday, 10 March 2025. A complete schedule is available on the IMC website landing page for the JTF. Realistically, we do not expect tangible work product from the JTF before Q1 2026

How can my company participate in the Joint Task Force on IoT Security?
All companies with an interest in the security of connected devices are encouraged to participate in the JTF. Simply fill out the form on the IMC website landing page dedicated to the JTF. Special consideration is given to member companies of the GCF or sustaining member companies of the IMC. The JTF on IoT Security requires no binding commitments (apart from non-disclosure) on the part of participating companies.