OPEN EUROPEAN NETWORK FOR ENTERPRISE
INNOVATION IN HIGH VALUE MANUFACTURING
WWW.INNOVATION-WEB.EU

Version 3.0 issued on July 18th, 2020

Invitation to High Value Manufacturing Medium-, Small- and Micro-Sized Enterprises, Industrial Organizations and Digital Security Intelligence Providers to Participate as Associate Partners in our "eGoose" Horizon Europe Innovation Action Proposal on enabling

"Digital Security and Privacy for Small and Medium Enterprises (SMEs) and Micro Enterprises (MEs)"

with the aim

"to build communities of learning (supported by collaboration technologies) that democratically share knowledge of digital security incidents, risks and treatments among participants of extended SME and ME supply chain ecosystems in order to raise their individual and aggregated digital security resilience in a demonstrable and sustainable manner. Members of such ecosystems also include their industry customers and their digital security information and solution providers."

The Open European Network for Enterprise Innovation in High Value Manufacturing (ENTOV-HVM) in collaboration with the Innovation Value Institute at Maynooth University (Ireland) hereby invites High Value Manufacturing Medium-, Small- and Micro-Sized Enterprises, Industrial Companies and Digital Security Intelligence Providers to participate in our upcoming proposal to develop and implement an innovative digital security solution with a focus on building communities of learning (supported by collaboration technologies) that democratically share knowledge of individual digital security incidents, risks and treatments in order to raise the digital security resilience of their extended supply chain ecosystems in a demonstrable and sustainable manner. Proposal submission will be by August 27th, 2020. The proposal will apply for three year and up to €4M funding.

ENTOV-HVM aims at strengthening Europe's innovation capacity and at fostering innovation in higher education, business and the broader socio-economic environment of the European Union by identifying, developing, and sustainably implementing measures to disruptively accelerate the value creation of innovative ideas in high value manufacturing from inception to late adopters and laggards in markets at individual, organizational and ecosystem levels.

The Innovation Value Institute at Maynooth University (Ireland) is a globally leading research institute on technology adoption and diffusion with a dedicated group focused on Cyber Safety and relevant effectiveness frameworks.

The following definitions apply:

- Micro: Enterprises which employ fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.
- Small: Enterprises which employ fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million, excluding enterprises that qualify as micro-enterprises.
- Medium-sized: enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million, excluding enterprises that qualify as micro-enterprises and small enterprises.

Organizations not meeting the above criteria (i.e. being of industrial size or acting as associations or intermediaries or solution providers) are also welcomed to apply for joining the proposal as advisory knowledge contributors.

The challenge posed is sub-topic (b) of the call "Small and Medium-sized Enterprises and Micro Enterprises (SMEs & MEs): Defenders of Security, Privacy and Personal Data Protection" and specifies: "Most SMEs & MEs lack sufficient awareness and can only allocate limited resources - both technical and human - to counter cyber risks, hence they are an easier target (e.g. of ransomware attacks) compared to large organizations. Security professionals and experts working for SME s & MEs need to be in a constant learning process since cybersecurity is a significantly complex and fast-evolving field. Taking into account the significant economic role of SMEs & MEs in the EU, tailored research to innovation should support cybersecurity for SMEs & MEs."

The Innovation Action builds on existing technical solution frameworks (i.e. the German open source Corona warning app), refocuses these on digital security (i.e. MITRE ATT@CK and NIST CSF frameworks) and enables pro-active knowledge sharing behavior based on advanced research and practice in social engineering for ecosystem orchestration. The following key intangible and tangible outcomes will be generated:

- The aspired intangible outcome is the voluntary and non-commercial sharing of knowledge regarding actual and anticipated digital security compromises within the extended supply chain ecosystems of SMEs & MEs, the automatic and instant relevant notification of other network members of such compromises, and the action of notified members to mitigate the threat informed of through collaboration with relevant trusted experts from business and research who volunteer their capabilities. The key innovative contribution is the social engineering needed to drive high degrees of participation through the science of living systems and ecosystems, and which will be based on leading principles of game design and information dissemination techniques which lead to exponential adoption behavior ("going viral").
- The aspired tangible outcome will be a voluntarily self-registering, free, decentralized, open source collaboration platform as mobile application, enabling and accelerating the real time diffusion of digital security solutions related to Security, Privacy and Personal Data Protection, in and across SMEs & MEs and their ecosystems in the core expertise area of the proposal consortium which is High Value Manufacturing ecosystems, for continuously increasing and maintaining cyber resilience.

The proposed solution thus enables an autonomous self-orchestrating opt-in/-out Digital Security Ecosystem protecting existing (and future) extended supply network partners from actual and anticipated incidents based on evolving best practice in this and relevant cross-disciplinary sectors.

The proposed solution will apply the Maynooth Cyber Safety Effectiveness Framework to accelerate the increase in Cyber Safety maturity of participants of the extended supply networks of SMEs and MEs by democratizing access to and triggering use of tools and solutions of varied sophistication level, to enable them to rapidly benefit from innovative targeted solutions addressing their specific needs and available resources (currently reserved to larger organizations, due to their cost and availability of internal expertise). Furthermore, the proposal will develop targeted, user-friendly and cost-effective solutions enabling the participants to:

- dynamically monitor, forecast and assess their security, privacy and personal data protection risks,
- become more aware of vulnerabilities, attacks and risks that influence their business,
- manage and forecast their security, privacy and personal data protection risks in an easy and affordable way, and

- build on-line collaboration between them, thus enabling them to report any (anticipated) incident and trigger suitable treatment activities.

Business participants will receive deep insights into how cyber safety solutions are currently deployed effectively across ecosystems by their peers and receive early access to the solution as it develops. Business participants will be expected to contribute case studies, validate research findings and host at least one workshop in their spaces each year of the project. They will furthermore be expected to pilot the developing solution in their own supply chains. Piloting involves mapping their supply network partners, supporting the distributing of the solution among their supply network partners, regularly (re-) assessing the digital security effectiveness of their supply network, helping to coordinate use case simulations, and committing to pro-active use of the solution at least during the implementation and validation period of the project. Business sponsors are expected to be CISOs (where present), business owners and senior business leadership as relevant. Business participants are not required to contribute funding, nor will they receive funding. The minimum effort involved is expected to be 80 work hours for each year of the project at minimum. A Letter of Intent confirming participation and resource allocation will be required in the format of the relevant template included in this invitation on the last page. Business participants may also join after formal start of the project subject to project budget and resource availability.

Further proposal participants from higher education and research include the Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University (Israel), Riga Technical University (Latvia), the Technical University of Berlin (Germany), UniSmart (Italy), the University of Lisbon (Portugal), Vidzeme University (Latvia) and the VTT Research Institute (Finland). The list of business and intermediary participants is growing and will be released in due time.

We look forward to hearing from you.

Dr. Oliver Schwabe, Principal Web Weaver ENTOV-HVM

On behalf of the eGoose consortium

More information on the Open European Network for Enterprise Innovation in High Value Manufacturing (ENTOV-HVM) is available at www.innovation-web.eu, our LinkedIn Group at https://www.linkedin.com/groups/8779542/, our blog at https://www.innovation-web.eu/entov-hvm-blog, our Researchgate project page at https://www.researchgate.net/project/Open-European-Network-for-Enterprise-Innovation-in-High-Value-Manufacturing-ENTOV-HVM, our Sourceforge page at https://sourceforge.net/projects/entov-hvm/ and our Facebook page at https://www.facebook.com/groups/2014779865300180/. You can also follow us via Twitter: @owschwabe (#innovationweb) and the LinkedIn Group page https://www.linkedin.com/company/entov.

** Please complete and email to Markus.Helfert@mu.ie and oliver.schwabe@innovation-web.eu **

[On letter head with organisation address]

To

Prof. Markus Helfert
Director Innovation Value Institute
Maynooth University
Ireland

<Date>

Letter of Support for "eGoose"

H2020 Call: Innovation Action SU-DS03-2019-2020 - Providing "Digital Security and Privacy for Small and Medium Enterprises (SMEs) and Micro Enterprises (MEs)"

[organization] is a [medium size]/[small]/[micro]/[industry]/[association] and [manufacturing]/ [digital security provider] enterprise and expresses its strong interest to participate in activities that are offered by the eGoose Project within the framework of the Horizon 2020 Call Innovation Action SU-DS03-2019-2020 - Providing "Digital Security and Privacy for Small and Medium Enterprises (SMEs) and Micro Enterprises (MEs)".

The eGoose project aims to build communities of learning (supported by collaboration technologies) that democratically share knowledge of digital security incidents, risks and treatments among participants of extended SME and ME supply chain ecosystems in order to raise their individual and aggregated digital security resilience in a demonstrable and sustainable manner. Members of such ecosystems also include their industry customers and their digital security information and solution providers.

[organization] wishes to support research and the knowledge transfer, capacity building activities and exchange opportunities within the eGoose project in order to contribute to not only the research and development activities in this project, but also the implementation of a system prototype demonstration in operational environment (Technical Readiness Level 7). Specifically, we wish to state our interest to participate in:

- contributing case studies as part of Work Package 2: Mapping Ecosystems,
- sharing in-depth needs as part of Work Package 3: In-Depth Needs Analysis,
- inputting to and validating the impact evaluation as part of Work Package 4: Impact Evaluation,
- reviewing and validating the knowledge sharing simulation as part of Work Package 5: Simulate and Assess Knowledge Sharing and Work Package 6: Accelerate Knowledge Sharing,
- inputting to and testing the collaboration technology solution as part of Work Package 7: Technology Support,
- implementing the collaboration technology solution in our extended supply chain ecosystem as part of Work Package 8: Implement Solution, and
- supporting dissemination and exploitation efforts as part of Work Package 9.

Participation will also involve hosting at least one workshop annually at our facilities in each year of the project. We commit to contributing at least 80 work hours for each year of the project at minimum.

We look forward to a successful application and the granting of the project, which will allow us to contribute to the success of the eGoose project.

[Date: DD MM YYY]

____

[name, position, stamp]