IEEE SA STANDARDS ASSOCIATION

Meta Issues in Cybersecurity

Industry Connections Activity Initiation Document (ICAID)

Version 1.0, 12 November 2020

IC20-021-01 Approved by IESS SMDC 18 December 2020

Instructions

- Instructions on how to fill out this form are shown in red. It is recommended to leave the instructions in the final document and simply add the requested information where indicated.
- Shaded Text indicates a placeholder that should be replaced with information specific to this ICAID, and the shading removed.
- Completed forms, in Word format, or any questions should be sent to the IEEE Standards Association (IEEE SA) Industry Connections Committee (ICCom) Administrator at the following address: industryconnections@ieee.org.
- The version number above, along with the date, may be used by the submitter to distinguish successive updates of this document. A separate, unique Industry Connections (IC) Activity Number will be assigned when the document is submitted to the ICCom Administrator.

1. Contact

Provide the name and contact information of the primary contact person for this IC activity. Affiliation is any entity that provides the person financial or other substantive support, for which the person may feel an obligation. If necessary, a second/alternate contact person's information may also be provided.

Name: Greg Adamson
Email Address: G.Adamson@IEEE.Org
Employer: Digital Risk Innovation
Affiliation: University of Melbourne

IEEE collects personal data on this form, which is made publicly available, to allow communication by materially interested parties and with Activity Oversight Committee and Activity officers who are responsible for IEEE work items.

2. Participation and Voting Model

Specify whether this activity will be entity-based (participants are entities, which may have multiple representatives, one-entity-one-vote), or individual-based (participants represent themselves, one-person-one-vote).

"Individual-Based".

3. Purpose

3.1 Motivation and Goal

Briefly explain the context and motivation for starting this IC activity, and the overall purpose or goal to be accomplished.

Describe the motivation and goal.

IEEE is a leader in some aspects of cybersecurity, but it is not in general a leader in the field (among cybersecurity practitioners it is widely respected, but not for its cybersecurity work). This is unfortunate for at least two reasons: 1. IEEE uniquely sits across the cyber-physical domains, and the future of cybersecurity, in healthcare, critical infrastructure, and elsewhere is cyberphysical. 2. Cybersecurity, particularly in the age of Covid-19 which has seen a step-change increase in engagement with cyberspace, is one of the most important fields of technology consideration in the coming decade. The purpose of this Industry Connection is to examine the opportunity for IEEE to draw on its strengths and influence to advance the field of cybersecurity for the benefit of humanity.

Current opportunities to coordinate expertise in this field include:

- The increasingly technical and social character of cyber threats. Examples include AI-Systems enabling DeepFakes (for now - vocally, visually, auditorily); but as we consider social heuristics as continuously one of the leading paths to compromised outcomes, behavioral nudging technologies will increase in their risk levels applied to cyber-physical systems.

- The increasingly pervasive character of cyber threats. Defensive ("prepare for and respond to attacks") approaches to cybersecurity alone are no longer enough - if they ever were. Rather, a dual pronged approach of proactive and ongoing management coupled with defensive strategies will be critical to the future of successful cybersecurity systems. Technology approaches such as Zero Trust Architecture, security in IoT, fog and edge computing, personal data stores reflect the limitations of the "firewall" solution.

- The increasing stakes, as poorly planned or careless cyber attacks on health infrastructure result in the loss of life.

The outcomes will be useful to practitioners, policymakers and the general public in contributing to making cyberspace safe and trusted, and in addressing cyber-physical security threats.

The first stage will be to focus on the development of a committed and diverse community of experts with practical experience in the field, who are looking for a platform for addressing current limitations in cybersecurity approaches .

The program will contribute to IEEE SA's efforts to advance technology for humanity through the appropriate development of standards, and to broader IEEE and external programs to enable human flourishing in cyberspace.

3.2 Related Work

Provide a brief comparison of this activity to existing, related efforts or standards of which you are aware (industry associations, consortia, standardization activities, etc.).

Describe the related work.
https://cybersecurity.ieee.org/

https://www.ieee-security.org/, including IEEE Security and Privacy Magazine.

3.3 Previously Published Material

Provide a list of any known previously published material intended for inclusion in the proposed deliverables of this activity.

We will be inviting participants with a history of expertise in the field to contribute relevant pieces of their work to the program deliverables.

3.4 Potential Markets Served

Indicate the main beneficiaries of this work, and what the potential impact might be.

Describe the potential markets.
Cybersecurity touches every facet of our digital lives, even more given the enormous increase in remote working, learning, and social engagement during the Covid-19 pandemic, an increase that is not expected to disappear. The focus of this work will be to work with practitioners in the field to identify necessary and implementable approaches with respect to existing and emerging technologies; and to better enable current and future professionals in increasing their likelihood of success across all applicable fields.

3.5 How will the activity benefit the IEEE?

The activity will seek to position IEEE centrally within one of the most important fields of technology endeavor in the coming decade. The IEEE is known for many things; but its cybersecurity contributions are fragmented, and IEEE is not a universally recognized name in the cybersecurity field. Yet IEEE draws together a unique community of cybersecurity experts, and is the foremost technology professional organization addressing cyberphysical practice and theory, the basis of IoT (the intersection of information technology and operational technology, which underpins critical infrastructure resilience). Success here provides an opportunity for IEEE to leverage the successful work products to create a committed and engaged community (ies) dedicated to the space meaningfully.

Further, it will provide options for new assets that the IEEE could explore for Conferences, Standards, Education, etc.

4. Estimated Timeframe

Indicate approximately how long you expect this activity to operate to achieve its proposed results (e.g., time to completion of all deliverables).

Expected Completion Date: 12/2022 for the establishment phase.

IC activities are chartered for two years at a time. Activities are eligible for extension upon request and review by ICCom and the responsible committee of the IEEE SA Board of Governors. Should an extension be required, please notify the ICCom Administrator prior to the two-year mark.

5. Proposed Deliverables

Outline the anticipated deliverables and output from this IC activity, such as documents (e.g., white papers, reports), proposals for standards, conferences and workshops, databases, computer code, etc., and indicate the expected timeframe for each.

Specify the deliverables for this IC activity, please be specific.

- Webinars /Workshops
- New Project Proposals for developing Best Practices Guides & Standards
- Sandbox
- Toolkits

5.1 Open Source Software Development

Indicate whether this IC Activity will develop or incorporate open source software in the deliverables. All contributions of open source software for use in Industry Connections activities shall be accompanied by an approved IEEE Contributor License Agreement (CLA) appropriate for the open source license under which the Work Product will be made available. CLAs, once accepted, are irrevocable.

Will the activity develop or incorporate open source software (either normatively or informatively) in the deliverables? Yes/No

Not immediately. However, we do see it being a possible option.

6. Funding Requirements

Outline any contracted services or other expenses that are currently anticipated, beyond the basic support services provided to all IC activities. Indicate how those funds are expected to be obtained (e.g., through participant fees, sponsorships, government or other grants, etc.). Activities needing substantial funding may require additional reviews and approvals beyond ICCom.

Specify funding requirements and sources, if any.

N/A

7. Management and Procedures

7.1 Activity Oversight Committee

Indicate whether an IEEE committee of some form (e.g., a Standards committee) has agreed to oversee this activity and its procedures.

Has an IEEE committee agreed to oversee this activity?: No

If yes, indicate the IEEE committee's name and its chair's contact information.

IEEE Committee Name: Committee Name
Chair's Name: Full Name
Chair's Email Address: who@where

IEEE has a wide range of fragmented cybersecurity activity. During the first year of the IC, engagement will be undertaken with relevant Technical Societies and Technical Councils to engage them in the activity. At that point sponsorship from one or more of these OUs will be sought. This will both provide an opportunity to show the

validity of the IC's approach to the potential OU, and indicate to the IC the level of interest by the OU in the approach taken by the IC, maximizing the opportunity for alignment.

Additional IEEE committee information, if any. Please indicate if you are including a letter of support from the IEEE Committee that will oversee this activity.

IEEE collects personal data on this form, which is made publicly available, to allow communication by materially interested parties and with Activity Oversight Committee and Activity officers who are responsible for IEEE work items.

7.2 Activity Management

If no Activity Oversight Committee has been identified in 7.1 above, indicate how this activity will manage itself on a day-to-day basis (e.g., executive committee, officers, etc.)

Briefly outline activity management structure.

IC Chair and SA staff to identify initial interested participants, through IEEE and in the cybersecurity community beyond IEEE. Within the initial 6 months officers will be appointed and a program of work (ExeCom meetings, working meetings) established.

7.3 Procedures

Indicate what documented procedures will be used to guide the operations of this activity; either (a) modified baseline *Industry Connections Activity Policies and Procedures,* (b) Standards Committee policies and procedures accepted by the IEEE SA Standards Board, or (c) Working Group policies and procedures accepted by the Working Group's Standards Committee. If option (a) is chosen, then ICCom review and approval of the P&P is required. If option (b) or (c) is chosen, then ICCom approval of the use of the P&P is required.

Specify the policies and procedures document to be used. Attach a copy of chosen policies and procedures.

The IC will adopt option (a).

8. Participants

8.1 Stakeholder Communities

Indicate the stakeholder communities (the types of companies or other entities, or the different groups of individuals) that are expected to be interested in this IC activity, and will be invited to participate.

Specify types of entities or groups of individuals.
Leaders in the field, e.g. Bruce Schneier
Leaders in current and past IEEE cybersecurity initiatives.
Standards experts familiar with NIST Maturity Model and other approaches, interested in providing a future-facing approach.
Academics familiar with the limitations of current approaches.

Representatives of companies interested in addressing current gaps in security standards approaches, e.g. Thales (interested in a trust-based approach), companies focused on the under-developed machine to machine security field.
Government representatives interested in addressing the information technology--operational technology culture gap for resilience of critical infrastructure.
Defense cybersecurity specialists interested in overcoming the traditional misunderstanding of cybersecurity within the Defense community.
Specialists in the psychology of consumer cybercrime familiar with limitations of current cybersecurity training approaches.

8.2 Expected Number of Participants

Indicate the approximate number of entities (if entity-based) or individuals (if individual-based) expected to be actively involved in this activity.

12 individuals during the initiation period.

8.3 Initial Participants

Provide a number of the entities or individuals that will be participating from the outset. It is recommended there be at least three initial participants for an entity-based activity, or five initial participants (each with a different affiliation) for an individual-based activity.

Use the following table for an entity-based activity:

Entity	Primary Contact	Additional Representatives
Entity Name	Contact Name	Name

Use the following table for an individual-based activity [Note these individuals have worked with the chair on other projects in the past but have not yet been approached to participate]:

Individual		Employer	Affiliation
Bruce Schneier	Cryptographer	Harvard University	Independent researcher
Aloysius Joseph	Digital Identity & Security	Thales	Industry practitioner
Vignesh Saxena	Information Security	ANZ Bank	Industry practitioner
Ben Rubenstein	Data Privacy	University of Melbourne	University
RE Burnett	Dean	National Defense University	University
Monica Whitty	Professor, psychologist	University of NSW	University
Vishal Salvi	CISO	Infosys	Industry practitioner