

**AGREEMENT FOR PUBLICATION AND MARKETING OF**  
***IEEE Computing in Science and Engineering***

**For Technical Sponsor**

**IEEE Signal Processing Society**

**9 September 2016**

## MEMORANDUM OF UNDERSTANDING FOR TECHNICAL CO-SPONSORSHIP

The IEEE Signal Processing Society (hereafter SPS) agrees to be a technical co-sponsor of the periodical known as *IEEE Computing in Science and Engineering* (hereafter the Publication).

### RESPONSIBILITIES & COLLABORATION IN EDITORIAL POLICY:

Editorial selection and review shall be consistent with the policies and procedures of IEEE, including but not limited to the IEEE PSPB Operations Manual and as expressed below. One Editor from the SPS shall be appointed by the SPS's President to serve as a non-voting member of the Publication's Editorial Board for a term of two years with a maximum of two consecutive terms. Any travel expense for this appointed Editor will be funded by the Technical Partner at its discretion. Typically this travel will be to the Publication's Editorial Board meeting.

The function of the Editorial Board shall be to review and offer guidance to the technical content of the periodical. The function of the Editor(s) shall be to implement the policies established by the Editorial Board and EIC, as well as the following:

- A. As a matter of principle, the Financial Sponsor(s) and the SPS shall direct the Editors of their other publications to forward suitable material to the Publication. The Committee shall develop procedures (a) for IEEE and IEEE Computer Society and IEEE Reliability Society to request, prepare, and publish special issues of the Publication, and (b) for directing papers not within the scope of the Publication to other IEEE and IEEE Computer Society and IEEE Reliability Society publications for consideration.
- B. Authors of the Financial Sponsor's and SPS's conference, symposium, or workshop papers are encouraged to update and greatly extend their papers and submit them to the Publication for consideration to be published as original papers.
- C. The SPS's appointed Editor will keep the SPS President and Vice President of Publications apprised of activities related to the Publication via a written status report on this partnership successes and/or challenges a month prior to each Administrative Committee meeting of the SPS. This clause is included to ensure information flow to the Technical Partner and assumes standard information flow with the Financial Sponsor is already in place via the publication's Editorial Board's activities.

### PERIODICAL SCOPE:

The current scope of the Publication is as follows:

CS&E magazine emphasizes articles that help define the field as the interface among the applications (in science and engineering), algorithms (numerical and symbolic), system software, and computer architecture. Such articles should also be readable by specialists from various disciplines; i.e., such articles should overcome the barriers usually created by discipline oriented vocabularies. Articles on topics across this spectrum are welcomed. Example topics include: Role of symbolic computing in computation; Survey of fast multipole methods; A revolution in computational electromagnetic field theory; Grid generation: State-of-the-art; Algorithms to overcome critical slowing down; Building the infrastructure for communications & networking & how to use it; Random number generation; Cellular automata & at-scale problems; Mathematical software: Future needs; Ab initio calculations (chemistry vs. physics approaches); Opinion pieces on trends; Protein polymer simulations & their use in other disciplines; Large-scope computation (combine simulation of fluid flow and structures, ... ); Continuing surveys of computational biology, chemistry, physics, etc.; Computer science surveys/tutorials for computational scientists, e.g., what does RISC architecture mean to me?; Does computation complexity theory

provide useful information: Now or ever?; Scientific computing in C; University programs in computational science & engineering; Industrial programs & approaches to computational science engineering; Computational plasma-aided manufacturing; Computational approaches to lithography; Software tools such as debuggers, profilers, and performance evaluation tools; Standardization issues as they affect CS&E, e.g. FORTRAN and POSIX. CS&E magazine emphasizes articles that help define the field as the interface among the applications (in science and engineering), algorithms (numerical and symbolic), system software, and computer architecture. Such articles should also be readable by specialists from various disciplines; i.e., such articles should overcome the barriers usually created by discipline-oriented vocabularies. Articles on topics across this spectrum are welcomed. Example topics include: Role of symbolic computing in computation; Survey of fast multipole methods; A revolution in computational electromagnetic field theory; Grid generation: State-of-the-art; Algorithms to overcome critical slowing down; Building the infrastructure for communications & networking & how to use it; Random number generation; Cellular automata & at scale problems; Mathematical software: Future needs; Ab initio calculations (chemistry vs. physics approaches); Opinion pieces on trends; Protein polymer simulations & their use in other disciplines; Large scope computation (combine simulation of fluid flow and structures, ...); Continuing surveys of computational biology, chemistry, physics, etc.; Computer science surveys/tutorials for computational scientists, e.g., what does RISC architecture mean to me?; Does computation complexity theory provide useful information: Now or ever?; Scientific computing in C; University programs in computational science & engineering; Industrial programs & approaches to computational science engineering; Computational plasma-aided manufacturing; Computational approaches to lithography; Software tools such as debuggers, profilers, and performance evaluation tools; Standardization issues as they affect CS&E, e.g. FORTRAN and POSIX.

“Examples of topics appropriate for IEEE Security & Privacy include, but are not limited to, the topics below. Networks: Securing legacy networks, Rapid intrusion detection, Rapid intrusion containment, Post-intrusion recovery and re-validation, Strategies for continuing operations during an ongoing attack, Automated, dynamic reconfigurations of network and software topologies, Self-regulating service strategies (automated denial of service defenses), Strategies for effective use of certificates, Recognition of and response to network attack patterns. Software: Evaluating legacy software, Securing legacy software, Evaluating commercial software, Protecting commercial software, Subsystem-level security techniques, Systems-level security techniques, Enterprise-level security techniques, Automated security evaluation techniques. Operating systems and security: Techniques for making existing operating systems more secure, Common security problems of operating systems. Hardware: Techniques for preventing undetected physical subversion of systems, Usability and security of hardware to hardware interfaces, Usability and security of hardware to human interfaces. Tools: User evaluations of tools, Techniques for effective use of tools, Avoiding misuse of tools. Decoys and misdirection: Building and instrumenting decoy targets, Multilevel decoy strategies, Acceptable loss strategies, Misdirection strategies. Preemptive defense strategies: Rapid automated responses to attacks, Scouting and remote instrumentation of hostile sites. Physical security: Role of physical security in protecting complex systems, Usability and security of physical security methods. Human security: Human fallibility and its implications for secure system design, How to allocate security roles between people and automated systems, Minimizing the impact of internal human threats, Monitoring and analysis of usage patterns. Security Usability: Overall security impacts of failing to make security “user friendly”, Techniques for making security easier to use, Techniques for making security inconspicuous, Risks and benefits of single-login strategies. Security policies: Recognizing self-defeating security policies, Making security policies work. Security Designer Topics — Networks: Integrated approaches to evaluating and designing network security, Distributed network security architectures, Multilevel network security architectures. Software: Recursive and multilevel (from enterprise down to code) security design, Code-level security techniques. Computer languages and security: Security implications of computer languages (such as overflows in C/C++), Evaluating and selecting secure computer languages — Designing secure computer languages, Computer languages for expressing and enforcing security policies. Security policies: Automated policies and policy (rule) languages, Scalability of automated policy-based methods, Computer-assisted creation of automated policy rule sets, Testing of policy rule-based systems, including risks of adding new rules. Hardware: Designing security first computer and network hardware, Security and the design of real (e.g., Intel) and virtual (e.g., Java) instruction sets. Wireless security: Strategies for increasing wireless security, Evaluations of off-the-shelf wireless technologies, Techniques for hardening off-the-shelf wireless technologies for secure use, Comparisons of the security features of multiple wireless technologies, Designing architectures to minimize security risks from the wireless components. Integrated security design methods: Physical, procedural, electronic, and software limitations and tradeoffs, Implications of human limitations for technical system design, Training versus system tradeoffs — Designing hardware to support software security, Common-sense rules for good hardware and software design. Developer training: Academic strategies to increase awareness of security issues, Integrated approaches to security training (security as a fundamental constraint), Commonsense approaches to security (avoiding the obvious holes). Security Theory:

~~Security evaluation models, Cross-disciplinary security evaluation models, Mathematical representations of trust and trustability, Mathematical representations of attack and response spaces, Probabilistic models of system behaviors under attack, “Hydraulic pressure” enterprise-wide models of security intrusion threats, Fallback theory (estimating level of protection provided by multiple layers), Integrating models of physical, human, and electronic security, Payoff maximization approaches (e.g., using kernel call patterns vs. code patterns), Scalability analysis and theory as applied to security. Security economics: Estimating potential losses due to security flaws, Validity of example-based arguments for security investment, Cost of implementing security, Designing to maximize benefits of security investments, Cost impact of using or reusing validated secure components, Cost tradeoffs between security and other system attributes (e.g., usability), Synergies between security and other system attributes (e.g., reliability). User training: Exploring security implications of inadequate training, Techniques for effective training of users, Exploring security implications of difficult, cumbersome, and stressful policies, Training systems that show users the security consequences of their actions. Infrastructure Security Telecommunications, Financial, Energy/utilities, Emergency response, Health care and vital human services, Commerce, Transportation.~~

NEED: TAB approval date Approved by TAB on 21-Jun-2014.

This scope can be changed after approval by the Publication’s management committee as well as each of its sponsoring partners. Formal scope change approval and implementation processes in existence within the Financial Sponsor(s) at the time of the change consideration shall also be followed.

## **PERIODICAL COVER, PUBLICATION INFORMATION PAGE, AND MARKETING MATERIALS TREATMENT:**

The Financial Sponsor and Technical Sponsor logos will appear together on the Publication as soon after the starting point of this signed MOU as possible. Typically logos will appear on the periodical’s cover or Publication Information page.

The cover or publication information page of the Publication shall have a statement that the SPS is a Technical Sponsor, or alternatively, all financial and technical co-sponsors can be listed together simply as “sponsors.” This mention should coincide with the appearance of the Technical Partner’s logo.

In addition, all marketing information solely focused on the Publication shall also have a statement that the SPS is a Technical Sponsor. This can begin as soon after the starting point of this signed MOU as possible, but the application of a sponsor price for subscriptions must be done only at specific times of the year to avoid disruption of the IEEE’s renewal handling. Communication with Technical Activities staff is important to coordinate this pricing change, and [periodical@ieee.org](mailto:periodical@ieee.org) is the alias for the staff whom will assist in the setup of this price level for the Technical Partner’s members.

Catalog product detail pages and website pages dedicated to the Publication for authors, readers, subscribers or other audiences will mention both Financial and Technical Partners. The Technical Partner list the publication on their website(s) and areas of promotion of technical content.

## **AGREEMENTS & DURATIONS:**

The term of this agreement shall begin January 1, 2017 and continue through December 31, 2021, unless terminated in accordance with this agreement prior. While the start of cooperative activities can occur any time of year, sponsor-level subscription pricing for the new Technical Sponsor can only be implemented during the renewal preparation period (May/June before the subscription year the lower price should apply) and in the March to July timeframe for immediate shift to the sponsor price level.

The agreement may be terminated by either the Financial Sponsor(s) or Technical Partner upon written notification supplied at least one year in advance of the effective publication year. For example, to end technical sponsorship at the end of the 2016 publication year, the Financial Sponsor or Technical Partner must have provided notice of the intended agreement end by late December 2015. Notification of intended termination of an

agreement should be sent to all of the following:

- President of the Financial Sponsor
- Editor-in-Chief of the Publication
- Chair of the Steering Committee for the Publication, if one exists
- Vice President, Publications of the Financial Sponsor
- Executive Director (staff) of the Financial Sponsor, if one exists
- Technical Activities staff at [periodical@ieee.org](mailto:periodical@ieee.org)

This agreement will automatically be renewed every five years unless the agreement is terminated upon written one-year notification as described in the preceding paragraph. The termination notification will trigger planning regarding the end of the agreement, sponsor-pricing for the Technical Partner's members, and adjustments to remove marketing/editorial references of the partnership.

All modifications to this agreement must be approved by the Administrative Committees all Financial Sponsors of the Publication. All modifications to this agreement must be in writing and signed by the Presidents of the Financial Sponsor and Technical Partner.

Upon termination of this agreement or the termination of the Publication, the Financial Sponsor(s) and the SPS agree to the following terms:


- A. All indications of joint sponsorship with SPS shall be removed from all future issues of the Publication, and this removal is timed with the end of a publication year. However, an indication that the Publication is a continuation of the previously jointly cosponsored Publication with SPS is permitted through one complete calendar year from the date of termination.
- B. Those papers accepted for the Publication or under review and subsequently accepted shall remain committed to the Publication.

## MISCELLANEOUS

- A. The relationship between the parties shall be that of independent contractors, and nothing in this agreement shall be construed to constitute either party as an employee, agent or member of the other. Without limiting the foregoing, neither party shall have authority to act for or to bind the other in any way, to make representations or warranties or to execute agreements on behalf of the other, or to represent that it is in any way responsible for the acts or omissions of the other.
- B. Neither Party may assign this MOU or any of its rights, obligations or duties hereunder, without the prior written consent of the other Party.
- C. This agreement represents the full and complete understanding of the parties.

## AGREEMENT ACCEPTANCE BY THE PRESIDENT OF THE SPS AND IEEE COMPUTER SOCIETY AND IEEE RELIABILITY SOCIETY:

Technical Sponsor

Signature		
-----------	-------------------------------------------------------------------------------------	--

Name	Rabab Ward	
Title	President	
Organization	IEEE Signal Processing Society	
Date	Sept 13.2016	

## Financial Partner(s)

Signature		
Name		
Title		
Organization	IEEE Computer Society	
Date		

Signature		
Name		
Title		
Organization	IEEE Reliability Society	
Date		