SLIDE 1:

FARNAM JAHANIAN:

Good afternoon! I'm Farnam Jahanian, Assistant Director of the National Science Foundation for Computer and Information Science and Engineering. With me here are Angelos Keromytis and David Corman. It's also my pleasure to have Chris Ramming, John Manferdelli, and Wen-Hann Wang of Intel joining by phone.

On behalf of all of us, it is my great pleasure to welcome you to this webinar to learn about our joint partnership on the Cyber-Physical Systems Security and Privacy solicitation.

As automation and information technology pervade new platforms, cyber-physical systems have become ubiquitous in our everyday lives.

CPS technology is transforming the way people interact with engineered systems -- just as the Internet has transformed the way people interact with information.

These systems grow increasingly complex each year. They fly our planes, control our power grids, run our medical devices, and as the 'Internet of Things' become more pervasive, they also control our household appliances – controlling our thermostats, lights, and even the locks on our doors.

Advances in cyber-physical systems hold the potential to reshape our world with more responsive, precise, reliable, efficient, and secure systems.

These advances are closely intertwined with, and will have

pervasive impact upon, many of our societal priorities, including:

Smart systems for manufacturing and robotics;
Emergency response;
Healthcare; and
Transportation and energy networks and infrastructure.

Since its inception in 2009, the NSF CPS program has sought to deeply integrate computation, communication, and control into physical systems, enabling "smart" systems with cyber technologies – both hardware and software –

That are deeply embedded in, and interact with, physical components; and
That sense AND change the state of the real world.

Within NSF, we recognize that achieving next-generation cyber-physical systems requires bringing together experts from many different sectors and disciplines.

For example, the 2014 CPS solicitation for the first time constituted a multi-agency effort. It involves NSF as well as our partners at the Department of Homeland Security's Science and Technology Directorate and two parts of the Department of Transportation – the Federal Highway Administration and the Intelligent Transportation Systems Joint Program Office.

And to fortify the adoption of CPS across sectors, we know that we must address "How can we build and verify systems upon which people can – and will – bet their lives?"

– which is why we have worked closely over the last several months to build a partnership with Intel to advance the security of

CPS, particularly in the context of sociotechnical aspects.

We are pleased to introduce you to the Cyber-Physical Systems Security and Privacy solicitation through today's webinar.

We all recognize that a key challenge for current and emerging cyber-physical systems is to ensure the security of these systems, the infrastructures they form, and those integrated with them.

Through the CPS-Security solicitation, we aim to foster a multi-disciplinary research community at the confluence of cybersecurity, privacy, and cyber-physical systems. We also aim to transition research findings into engineering practice.

This partnership builds on a strong collaboration between NSF and Intel. It will combine NSF's experience of developing and managing successful large, diverse portfolios with Intel's long history of building research communities in emerging technology areas.

Let me take just a moment to thank Keith Marzullo, Fen Zhao, Angelos, and David of NSF and Wen-Hann, Chris, and John of Intel for their leadership and facilitating this effort.

Let me now turn things our Wen-Hann.

WEN-HANN WANG:

Thank you, Farnam.

I'd just like to speak briefly at a higher level about the importance of CPS and the security of current and emerging cyber-physical systems.

At Intel we have embraced a mission to “create and extend computing technology to connect and enrich the lives of every person on earth”. As the lines between embedded, mobile, personal, and cloud computing become ever-more blurred we find ourselves on the verge of realizing a vision where it is natural to think about the remarkable benefits in terms of new function, efficiency, and convenience that could accrue if we are able to develop reliable computing systems that both deeply sense and interact with the real world. In some ways the trend toward CPS has already emerged and is becoming more of a reality with every passing day on the strength of the opportunities. But because of the fact that these systems interact with the real world – the power grid, transportation, healthcare – the opportunity to do good is balanced almost equally by the potential for accidental or even intentional harm if the uses run ahead of our ability to secure and protect these systems and their users. What we’d like to do now with the NSF community is pause and think deeply with the community’s thought leaders about new ways to protect these systems, and build security and privacy into the foundations of cyber physical systems going forward.

This collaboration is designed to combine NSF’s strengths with Intel’s capabilities. What we hope to contribute to the amazing NSF community includes both insight into current industry trends and capabilities, as well as a partnership for bringing big insights and ideas into practice.

However this program is designed to do more than just combine academia and industry to increase the odds that discoveries will become innovations. We believe that security and privacy, especially for cyber physical systems, are not just technical issues that will admit of purely technical solutions. Therefore we have

designed this solicitation to create research partnerships that will span technology, social, policy, and economic disciplines in order to increase the odds of developing a holistic perspective and solutions that will truly comprehend the full range of opportunities and challenges.

What we hope and expect is that the CPS-Security community will be bold, and that it will swing for the fences with game-changing ideas. In the same way that our grandparents saw the introduction of an aviation industry so safe it can be taken for nearly for granted, we'd like cyberphysical systems to have a profound impact that is equally taken for granted by our grandchildren. To make that possible we'll need a few people willing to step back and look at some non-incremental, non-linear new directions in security and privacy. We're hoping that is why all of you are on this call and we really look forward to learning more about your perspectives and then working together to make a difference. Thanks for joining us on this adventure!

Let me now turn things over to Dr. Angelos Keromytis from NSF, who will continue the webinar and offer more detail about the program.

SLIDE 2:

ANGELOS KEROMYTIS:

We will begin with a discussion of this partnership and the motivations behind it.

We will then discuss the security challenges behind Cyber-Physical Systems and the need for this program.

Because Intel will be an active participant in this process, we will carefully highlight the special aspects of the program administration and proposal selection. We will focus In particular on how it differs from proposal administration for the nominal SaTC and CPS programs, the different types of proposals, and the Ideas Lab.

We will close out our prepared remarks on questions that we think the community might ask about the program and then open the discussion to anyone on the Webinar.

As a reminder, these slides will be posted to the NSF website after the conclusion of this webinar. We are going to try to keep this to an hour, but can stay longer if needed for Q&A.

SLIDE 3:

NSF and Intel have come together to fund and support research in the intersection area of Cyber-Physical Systems and Security.

By bringing together their resources and expertise, NSF and Intel hope to both fund fundamental research in making Cyber-Physical Systems more trustworthy and secure, but also to help develop a community of researchers interested in this area. From NSF's perspective, our partnership with Intel can provide researchers with greater insight and access to industry needs, capabilities and resources, and will facilitate transition of research outcomes to practice.

SLIDE 4:

Since we are trying to bring together two different communities, it is worthwhile clarifying the intersection space. One of its key

components, Cyber-Physical Systems, describes sociotechnical systems in which cyber and physical elements are tightly integrated at all scales and levels. Cyber refers to computation, communication, and control elements that are discrete, logical and switched. Physical refers to natural and human-made systems governed by the laws of physical and operating in continuous time.

SLIDE 5:

Cyber-Physical Systems have characteristics that make them a challenging domain, especially from a security point of view. These include the close integration of cyber capabilities in every physical component; the scale at which many CPS-enabled infrastructures are designed and operate; and the complex interactions that are highly, and sometimes fully, automated. An additional complexity arises from the sometimes unconventional computation and physical substrates in which such systems operate. All these factors make the design, analysis and operation of such systems challenging, even absent security and privacy concerns. Cyber-Physical Systems are fundamental elements of real systems that we interact with every day, including transportation, energy, medical, and others. This means that their operation must be significantly more dependable than the state of affairs with general computing. In some cases, such systems must be certified for use, due to policy or legal reasons.

SLIDE 6:

Through its CPS program, NSF has been supporting the development of the core system science needed to engineer complex cyber-physical systems upon which people can depend with high confidence. The program aims to foster a

research community committed to advancing research and education in CPS and to transitioning CPS science and technology into engineering practice. By abstracting from the particulars of specific systems and application domains, the CPS program aims to reveal cross-cutting fundamental scientific and engineering principles that underpin the integration of cyber and physical elements across all application sectors. Security has long being identified by NSF as a key cross-cutting fundamental research interest in CPS.

SLIDE 7:

There is good reason for this interest. Starting from the fact that CPS inherits the security and privacy concerns inherent in “cyber” systems, there are a number of additional issues that make securing Cyber-Physical Systems both challenging and important.

Cyber-Physical Systems sense and collect information related to a large spectrum of everyday human activities. Similarly, they control infrastructure that we, as humans, interact with on a daily basis; such interaction often has life-critical implications, especially when actions taken by Cyber-Physical Systems are non-reverseble

Cyber-Physical Systems are often federated into networks of extremely large size and complexity, and at the same time are deeply embedded (almost hidden) in our infrastructures. Their fully-automated interactions often lead to emergent behaviors, which are almost invariably undesirable from a security and privacy perspective.

Such systems often rely on subtle and brittle assumptions at the interface boundaries among hardware and software components,

and with human operators and maintainers. This also brings to the fore the fact that Cyber-Physical Systems typically operate in multi-stakeholder environments, where the participants have varying degrees of expertise and control over these systems. Despite this, there is limited scope for interaction with humans (who could otherwise act as arbitrators in security decisions).

Finally, Cyber-Physical Systems must operate under varying economic and policy constraints; any approach to securing such systems must take these into consideration, along with the social norms that organically emerge after such systems are fielded and operated.

All these factors complicate the design, analysis, understanding, and ultimately trustworthiness of the current generation of Cyber-Physical Systems.

SLIDE 8:

With these challenges, the question that we pose is how can we enable secure and private Cyber-Physical Systems without sacrificing the benefits that come from this integration of automated sensing and actuating with the physical environment?

SLIDE 9:

The goal of the CPS-Security program is to foster transformative, multi-disciplinary approaches that address the problem of securing current and emerging cyber-physical systems, the infrastructures they form, and those infrastructures integrated with them.

Specific objectives include:

understanding the range of technical issues affecting hardware and software in infrastructure components, and their integration in sociotechnical systems; and

developing an understanding of the interplay between key technical, social, and policy aspects.

CPS-Security is interested in receiving proposals on any idea that addresses these Goals & Objectives.

SLIDE 10:

Some topics of interest to the CPS-Security program include, but are not limited to:

Security Architectures for CPS

Tools and Methodologies for Secure CPS Development, Verification and Analysis

Current and Future Threat Assessment and Countermeasures

Balance of technical solutions, regulation, and policy incentives to enhance privacy and security

Effective, Secure, Reliable Control in Centralized and Decentralized Systems

SLIDE 11:

We will now discuss some of the important details in the solicitation. The main topics here revolve around the Ideas Lab,

and the two types of full proposals invited by the solicitation.

I will remind everyone that only US Universities and Colleges are eligible to submit proposals.

SLIDE 12:

We view the Ideas Lab as a precursor to the submission of full proposals. However, participation in the Ideas Lab is NOT required for submission of full proposals.

The goal of the Ideas Lab is to identify and develop novel ideas at the intersection of CPS and Cybersecurity, and to assist in the establishment of research partnerships.

Participation will be by invitation. Invitations will be based on preliminary proposals that must be submitted prior to the Ideas Lab.

SLIDE 13:

Submission of Preliminary Proposals is required for participation in the Ideas Lab. The deadline for Preliminary Proposals is July 29, and submission may only be made via Fastlane. Preliminary proposals may have only individual PIs, and are limited to 2 pages of Project Description, Biographical Sketch, and Current & Pending Support. All other elements of regular NSF proposals (such as Summary or Budget) are waived. Proposers must follow specific guidelines for the content of the 2 pages of project description; see the solicitation for details.

Responses to the Preliminary Proposals (including invitations to the Ideas Lab) will be sent out by August 5.

SLIDE 14:

The Ideas Lab itself is an intensive 5-day residential workshop that will use a real-time, iterative review process to develop research ideas. The participants will be assisted by a team of professional facilitators, and a group of mentors. The mentors will be senior researchers with relevant expertise, who will help guide the technical discussions.

We expect 20 to 30 participants. The date has been fixed to August 12 through 16, in the Washington DC metropolitan area. NSF will cover the travel expenses of participants.

Note that submission of a Preliminary Proposal implies a commitment by the PI to attend the full 5-day Ideas Lab, if invited.

SLIDE 15:

Following the Ideas Lab, the mentor team will provide recommendations to NSF about specific ideas developed in the Lab. Within 2 weeks from the conclusion of the Ideas Lab, NSF will determine which participant teams will be invited to submit full proposals, and will notify the participants. Note that such an invitation does not imply a guarantee to fund. Also note that non-invited ideas can still be submitted as full proposal. I will also repeat that participation in the Ideas Lab is not required for submitting a full proposal to this solicitation.

SLIDE 16:

Let’s move now into the logistics of the program.

Proposals to this joint program will be submitted to NSF with the following requirements:

All proposals will be up to 3 years with a total award value of $500K for Breakthrough and $3,000,000 for Synergy proposals.

The submission deadline is 5pm proposers local time 28 October 2014.

The title should start with the prefix “Breakthrough:” or “Synergy:”, as appropriate.

Only two proposals per PI/co-PI to CPS-Security is allowed.

This limit is separate and distinct from the SaTC and CPS programs.

No proposal containing or referencing classified material will be accepted.

Proposals must follow all the usual NSF policies, including inclusion of biographical sketches, budgets and budget justifications, lists of references, data management plans, etc. Proposals are submitted through Fastlane or grants.gov, as with any NSF proposal.

One requirement that is different from the usual submission to NSF is a statement of consent that gives NSF permission to share the proposal, reviews and any other related information with Intel. This statement of consent needs to be uploaded into Fastlane or grants.gov as a supplementary document. There is no particular format for this statement, but we expect it will be no more than about a page.

Intel will treat your proposal as proprietary.

SLIDE 17:

The proposal review process will be conducted by NSF, according to the standard rules and procedures in place for NSF proposals.

The review and award recommendations will be coordinated by a Joint NSF and Intel Working Group of program officers from both NSF and Intel.

Projects that are selected for joint funding by both NSF and Intel will be funded under two funding instruments. That is, NSF support will be provided via an NSF grant, and Intel support will be provided via an Intel contract.

Note that not all projects will necessarily be jointly funded, NSF or Intel may decide to fund certain projects separately.

The budget submitted with the proposal should include all necessary project funds without regard to the two funding organizations. The budget will be divided subsequent to selection.

SLIDE 18:

NSF and Intel expect to jointly fund 2 Synergy proposals.

Such proposals are expected to take a holistic view of the challenges in protecting Cyber-Physical Systems. In particular, we expect such proposals to account for technical, human/social, policy, and economics factors.

Due to their multi-disciplinary nature, Synergy proposals must have a separate 2-page collaboration plan.

In addition to the standard NSF Intellectual Merit and Broader Impact review criteria, Synergy proposals will be evaluated using two solicitation-specific review criteria. First, the degree of integration of the technical research with the broader security context in CPS. Second, how well the proposal pursues the development of a Systems perspective and drive toward demonstrations of interrelated component research ideas.

SLIDE 19:

Breakthrough proposals will be funded exclusively by NSF. We expect to fund 4 such projects.

Our goal with Breakthrough proposals is to bring together the CPS and SaTC communities. Thus, we expect such proposals to involve at least two PIs, representing the respective communities. A separate 2-page collaboration plan is required.

SLIDE 20:

NSF and Intel will manage their respective awards according to their own procedures and guidelines. Specifically for Synergy proposals, this means that Intel funds will be made available under a contract with specific conditions relating to Intel access to Intellectual Property developed through research supported by these funds.

Synergy projects agree to distribute all source code that has been authored while working on an NSF/Intel Synergy award under a

BSD, Apache or other equivalent open source license, but not GNU's General Public License (GPL) or Lesser/Library GPL, the Artistic License, or the Mozilla Public License. See the solicitation for specific guidelines.

SLIDE 21:

Synergy projects that generate data or software agree not to incorporate into this data or software any third-party code or background intellectual property, except by separate prearrangement with NSF and Intel if this incorporation would limit or restrict its ability to be distributed under an open source license.

Awardees may file patent applications, providing that they grant to Intel a non-exclusive, worldwide, royalty-free, sub-licensable license to all intellectual property rights in any inventions or works of authorship resulting from research conducted under the joint award.

Note that these three conditions relating to Intellectual Property do not apply to Breakthrough awards.

SLIDE 22:

Intel may separately fund its own personnel to directly participate in NSF/Intel Partnership research, part-time or full-time, with the universities awarded Synergy awards. These Intel researchers will work alongside the academic researchers, identifying opportunities for tech transfer, and being involved with the projects as advisors or as fellow researchers. Such deployment of Intel Researchers in Residence (RinR) on campuses will require mutual consent by the Parties and respective awardees in the

Project Management Plan for each Synergy award.

Further, Intel may designate one of its more senior, separately funded researchers to work alongside Synergy PIs. This senior researcher would help manage the project as a member of the Project Management Team. He/she would inject a perspective on commercial aspects and help with the day-to-day leadership of the center. He/she would also be responsible for working with the Intel Program Director to oversee the engagement of all other Intel researchers.

SLIDE 23:

All awardees must submit annual reports to the respective funding agency. If a project is co-funded by NSF and Intel, then the PI must submit reports to both NSF and Intel, which are similar in content.

One or more project representatives from an awarded CPS-Security project must attend the next NSF/SaTC PI meeting after the award is made.

For Synergy awards, Intel will also conduct annual retreats, and may conduct on-site annual reviews jointly with NSF. Intel may also lead the organization of phone calls with project teams; NSF may participate in these calls at its discretion.

SLIDE 24:

In summary, the CPS-Security Solicitation is an exciting new opportunity for NSF-funded researchers to work closely with industry and to explore an increasingly important area domain. CPS-Security researchers will help provide assurance that Cyber-

Physical Systems will be secure and trustworthy into the future.

Proposals are due to NSF on October 28, 2014.

If you have any questions after the end of this webinar, please contact an NSF and/or Intel program officer. Our contact information is on the next slide.
As a reminder, these slides will be posted to the NSF website after the conclusion of this webinar.

At this point, we will open the line for questions.

QUESTION & ANSWER PERIOD.

BACK TO SLIDE 24:

Again, the CPS-Security Solicitation is an exciting new opportunity for NSF-funded researchers to work closely with industry and to explore an increasingly important area domain. CPS-Security researchers will help provide assurance that Cyber-Physical Systems will be secure and trustworthy into the future.

Proposals are due to NSF on October 28, 2014.

If you have any questions after the end of this webinar, please contact an NSF and/or Intel program officer. Our contact information is on the next slide.
As a reminder, these slides will be posted to the NSF website after the conclusion of this webinar.

Thank you for your attention this afternoon. We look forward to receiving your proposals.