**SLIDE 1**

**Until Jim Kurose starts talking then move to SLIDE 2**

**SLIDE 2**

JIM KUROSE:

* Good afternoon! Who I am, and who is here from NSF (go around room)
* We are also very pleased to have from VMWare: David Tennenhouse, Chris Ramming, Bruce Davie, Dennis Moreau, Jianqing Zhang (pronounced Jun-Ching Zhang), and Tom Corn, joining by phone.  I’m sure many of you recognize a number of our VMWare colleagues as networking researchers, as folks who have worked here in DC (e.g., at DARPA) and as leaders in industry R&D, so in all of these different dimensions, they are well connected to our computing research community.
* Welcome to my colleagues from VMware.
* And welcome to all of you out there for this webinar to learn about our joint NSF/VMware partnership on Software Defined Infrastructure as a Foundation for Clean-Slate Computing Security (SDI-CSCS).

Technical Talking points:

* NSF CISE funds projects exploring or using virtualization through our Networking Technology and Systems (NeTS), Computer Systems Research (CSR) and other programs.  CISE also leads a vital and extensive investment focused on cybersecurity – the Secure and Trustworthy Cyberspace (SaTC) Program (indeed, SaTC is largest single research program in NSF’s portfolio, foundation-wide, and involves four other directorates in addition to CISE).
* The new NSF/VMware solicitation that we are discussing today brings together research in these and other programs to focus on the question:  *Can we use virtualization to build systems that are inherently secure because of the properties of virtualization and the composition of virtualized components?* David Tennenhouse will discuss VMWare’s vision for this joint program, and the associated opportunities and excitement for the advances that we hope it will enable.
* This partnership provides for important interaction among NSF, VMWare, and the awarded principal investigators to understand real-world contexts and problems faced by industry.  Even though the research is pre-competitive, direct interaction with VMWare program directors on the jointly-funded projects provides a venue for understanding and enabling tech transfer. (As a researcher, I’ve always found these kinds of interactions with industry particularly valuable, because it’s something we can’t do in the academic research community alone).
* This kind of partnership is important to our researchers, to NSF, to industry and indeed to our Nation. The NSF Act of 1950 established NSF to fund basic research, but also to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes. There is a recent report from AAAS (called “Restoring the Foundation” (restoring the foundation for basic science and engineering research in this country) that calls for thinking about new partnerships between academia, industry and the federal govt – and that’s exactly who we have engaged in this joint effort. So, we are particularly excited about this opportunity.
* Through the SDI-CSCS solicitation, we aim to foster a multi-disciplinary research community at the confluence of networking, computer systems, and security.  We also aim to transition research results from funded projects into engineering practice.  The partnership begins a strong collaboration between NSF and VMWare, which will combine NSF’s experience of developing and managing successful large, diverse portfolios with VMWare’s strong capability in the area of virtualization and security.
* I am very excited to kick off this meeting that marks the beginning of our partnership between NSF and VMWare.
* Let me now turn things over to David Tennenhouse, Chief Research Officer at VMware. You know David for his work with PlanetLab and Active Networks, two of the many pre-cursors to Software Defined Infrastructure. Dave, I can tell you I remember how exciting it was to read your CCR paper in 1995/6 that really laid the foundation for active networking.

DAVID TENNENHOUSE: Thank you, Jim. It is an honor for VMware to partner with you, the National Science Foundation and the CISE research community in this effort to reinvent our collective approach to securing cyberspace. In addition to thanking all the VMware folks who have been helping with this, I’d like to express my appreciation the talented NSF team including Erwin Gianchandani, Ken Calvert, Nina Amla, Jack Brassil, Darleen Fisher, Mimi McClure, and Gurdip Singh.

Now I’d like to briefly provide some historical context for the connection between virtualization and security, and a few thoughts on what the emergence of software defined infrastructure brings to the research table.

The connection between virtualization and security has been recognized since at least the late 1960s when IBM’s CP/CMS isolated users in completely separate operating system instances. Since those early days, many security benefits beyond sandboxing have been identified and exploited. For example, virtual machine introspection can provide new hooks for monitoring and enforcement; VMs can be used as an ingredient of honeypot-based attack containment and forensics; virtual hardware can be altered and simplified to reduce attack surfaces; and VMs can be reconfigured, replicated, and rolled back as an aspect of defense.

In recent years, virtualization as a concept has been extended beyond processors to storage and networking, leading to a world in which a broad and complete range of service infrastructure can be defined and secured in entirely novel ways. For example, micro-segmentation is increasingly viewed as a key element of “cyber hygiene” for industry and government. It is a datacenter security practice that enforces isolation, containment, monitoring, and recovery around specific application services. In one implementation approach, network virtualization is used to achieve a degree of isolation that would otherwise be implemented with complex combinations of hardware-based firewalls, subnets, and ACLs. *Virtual networks therefore significantly reduce the hardware required and the opportunities for configuration problems and human errors* that are the root cause of so many security vulnerabilities.

**SLIDE 3: SDI-CSCS Vision**

Software defined infrastructure, or SDI for short, builds on the foundation of virtualization by specifying applications at a higher layer of abstraction. SDI as an architectural approach opens the door to additional security opportunities, such as using dynamic reconfiguration to sustain a high “work factor” deterrent for attackers. At a yet higher level, SDI can be used to enable secure multi-tenancy, through the dynamic instantiation of virtual data centers.

In addition to opening the door to new approaches to security, SDI can also be the enabler of security-related research and of its rapid translation to practice. This is the key to the “clean slate” aspect of this program. Today, researchers who hope to do pioneering work are discouraged by the difficulty of bringing disruptive new ideas into a world with so much legacy infrastructure. For example, networking researchers privately bemoan the “ossification” of the Internet as an obstacle to experimenting with, let alone deploying, novel network and security technologies. SDI can reduce these barriers to research by hiding the dependencies on legacy physical infrastructure and/or enabling the virtualized deployment of whole new classes of infrastructure. In effect, it allows radically new hardware and software to co-exist with legacy artifacts.

In summary, the premise of this program is that virtualization and SDI offer a realistic entry point to truly groundbreaking security research. Although VMware is an enterprise software company today, our roots trace back to government-supported university research. We feel that we have a special obligation to give back to this community and look forward to partnering with CISE to help researchers create a secure cyberspace for the nation and the world. Thank you for joining us on this journey!

I would like to introduce Ken Calvert, who joined CISE in May 2016 as Director for the Computer and Networking Systems (CNS) Division in CISE. Ken will talk about the Vision behind the solicitation and the research challenges NSF and VMware would like to see addressed.

**SLIDE 4: Motivation**

KEN CALVERT: We all know the problem: we hear every day about cyber threats and attacks on our information systems. As the solicitation notes, many of our critical systems have been developed with security as an "add-on", rather than a basic design consideration. As a result, the mechanisms we rely on to make our systems trustworthy are fragmented, hard to configure, and hard to reason about. This makes it difficult, for example, to detect the spread of attacks. Policies have to be specified in terms of low-level artifacts like processes, IP addresses and port numbers; this leads to configuration errors and hard-to-debug gaps and conflicts up and down the stack. Applications have, and will continue to have, faults that provide entranceways for malicious payloads.

It's no exaggeration to say that the security and trustworthiness of our infrastructure is one of the most challenging issues of our time. We still have a long way to go toward a solution, and the problem is not going away. Indeed, as our modern society becomes increasingly dependent on cyberinfrastructure in **all** areas, it's only going to grow in importance.

**SLIDE 5 SDI-CSCS Challenge**

This solicitation challenges teams of researchers in security, networking, computer systems, and other areas to investigate the advantages of software-defined infrastructure (SDI) in building a more secure foundation for our information infrastructure. We are interested in supporting a research community working at the confluence of SDI and clean-slate computer security, and in transitioning the research findings to practice quickly.

**SLIDE 6 Example Research topics**

David Tennenhouse has given some history about how virtualization has been used in the past to make components of computer and network systems, including legacy systems, more secure. We want to extend the research underpinning these advances in virtualization, integrate them into an innovative systems perspective, and focus on new ways to make them more secure than our current systems. At NSF we know that the most innovative ideas are ones that we do not anticipate. Nevertheless the solicitation provides some examples of possible research directions, to give the flavor of what we are looking for. In that light, consider:

* SDI can offer "wide-angle" visibility into the normal (and abnormal) behavior of highly distributed applications. This capability could be used to detect and isolate malicious activity.
* SDI supports least-privilege execution, for example by limiting access to virtual resource pools to those needed by a particular application and/or principal.
* SDI may enhance resilience through adaptive response and flexible mitigation strategies, adapted to classes of applications.
* SDI can act as a trust measurement interface between software and the underlying hosting platforms (processing, network, storage), and provide mutual attestation between a virtual platform and application software.

I want to stress, again, that these are illustrative examples, and not intended to be limiting.

**SLIDE 7 Other Desiderata**

Also, as you think through your proposals, please note that the review criteria emphasize a **systems perspective**, and focus on the creation, deployment, and evaluation of demonstration or prototype solutions at the component and eventually the system levels. We are especially interested in approaches that take into account multiple heterogeneous administrative domains, at various levels. Although a well-defined threat model is crucial, **we are looking for teams working toward solutions, as opposed to finding new vulnerabilities**.

We invite truly innovative proposals and look forward to working with VMWare as we fund and enable teams as they take up our challenge that could have wide-reaching technical and eventually, if successful, social impacts.

Now I'd like to introduce Darleen Fisher, Director for the Networking Technology and Systems (NeTS) program, who will talk about the solicitation, who can submit, required proposal components, and the review and award selection process.

DARLEEN FISHER

Thank you all for your interest in this exciting research opportunity and for attending the webinar today.

**SLIDE 8**

I will start by noting information that you should have immediately.

First the program solicitation is NSF 16-582 which you can easily find with a web search. It is also posted on the CISE website and on the CNS webpage.

Second the proposal deadline is 5:00 your local time on October 5, 2016.

NSF and VMWare together expect to award approximately 2 projects. Each project may request up to 3 million dollars over 3 years.

We expect the awards to be made early spring 2017.

**SLIDE 9**

I am next going to talk about the solicitation, its requirements, thoughts about team composition, and key proposal sections and what we expect to see in each section. I will then talk about the review and award selection process and we will end the webinar with Questions and Answers.

**SLIDE 10**

Who can submit? This solicitation restricts submissions to US academic institutions. US universities and 2- and 4- year colleges including community colleges may submit one or more proposals. A US institution, in this case, is one that is accredited within the US and has a campus in the US that acts on behalf of its faculty members.

Sub-awardee institutions have the same restrictions.

**SLIDE 11**

An individual may participate as PI, co-PI, or senior personnel in **no more than one proposal** submitted in response to this solicitation.

If any individual is found to be on two proposals, the proposal with the earliest submission date will be accepted and all others will be returned without review. Make sure that individuals on your team have consented to participate on a project and are not listed on another proposal.

We are looking for manageable-sized teams with individuals with demonstrable expertise that is needed to successfully conduct the research.

The solicitation requires that the inclusion of each team member be justified and show how he or she will contribute to the overall vision of the program and the specific goals of the proposal.

**SLIDE 12**

I am first going to talk about the Project Description section of the proposal. You have up to 20 pages for this section. There are very specific topics that should be addressed in the Project Description section of the proposal. The purpose of listing these topics is to make sure you clearly describe the proposed research and how it addresses the goals of the solicitation, how you plan to validate your research, how you will manage the project, and the education and outreach activities you will as part of your project, and how you might move this research into practice beyond publishing academic papers. We want these projects to have real-world impact.

Most importantly we want to see a clear statement about how the outcomes of your proposed work, focusing on virtualization and SDI, will fundamentally improve security for future computer systems, networks, and networked systems.

We expect that you might divide the proposed research into topics or component. We would like to see how the components synergistically work together to advance the goals of the solicitation.

We would like to see a validation plan that includes the development of prototype systems and experimentation using the prototypes.

The solicitation further calls for a Gantt chart that lays out the major tasks, milestones and interdependencies among the tasks. Please note the solicitation also calls for a management plan as a supplementary document, which I will discuss later in the webinar. I mention it now because you should consider including in the Gantt chart as a way to indicate which team member or members are responsible for each task.

**SLIDE 13**

You should also discuss in the Project Description the following topics.

If your project involves more than one institution, you should provide the rationale for including them and describe how you will ensure effective collaboration. These awards are meant to be projects in which team members actively and synergistically collaborate to build upon concepts of Software-Defined Infrastructure and virtualization to design and prototype secure systems.

These projects should not be special purpose or single application systems, but to have outcomes that can be generalized to other areas of application. Thus you should show how your work can be generalized.

Broader Impact and the education of the next generation of researchers, scientists, and information technology workers are always of key value to the National Science Foundation. In your proposal you should show how your work will advance the field and discuss your plans to integrate this research into education. This section should be “actionable” in the future not just include past achievements or vague aspirations.

**SLIDE 14**

A Collaboration Plan is expected for all proposals that include more than one PI, which given the nature of the call, we expect will be all submitted proposals.

I have listed the following topics to be discussed in the proposal. You should include a description of the roles of all of the participants, how the project will be managed across all investigators, institutions, and disciplines, and includes coordination mechanisms. The budget should include support for collaboration and project management.

**SLIDE 15**

If a project includes funding for a postdoc, then a postdoc mentoring plan is required and is uploaded as a separate document. CRA has a resource page, hot linked on the slide, with best mentoring practices for you to consider.

**SLIDE 16**

This program will operate under a public dedication intellectual property model. Importantly, the solicitation specifies which open source licenses meet the program objectives, and the solicitation states a requirement that research results be publicly disseminated through an access-compliant repository in accordance with the NSF’s public access policy.

NSF also requires a Data Management Plan for all projects. This is where you should indicate the planned policy for licensing software. Please read the solicitation and visit the URL on the slide for more guidance on this topic.

**SLIDE 17**

All NSF research proposals require a Broader Impact section both in the Project Summary and in the Project Description.

I have already talked about this topic. You should note that you may request REU (Research Experience for Undergraduates) funds in the budget for up to $16K for the first year. REU funds do not count against the $3M budget limit.

**SLIDE 18**

You may include letters of collaboration pledging, for example, data or access to resources or facilities. You may NOT include letters of general support for the project or its expected outcomes.

**SLIDE 19**

We expect to see support for graduate students. You may also request support for software engineers or other necessary technical personnel, as well as for postdocs.

**SLIDE 20**

The review process for proposals received to this solicitation is as follows. Proposals will be reviewed by a merit review pane and the program director may request additional ad hoc reviews for a project as appropriate. The proposals will be reviewed according to the NSF standard Intellectual Merit and Broader Impact review criteria. In addition the reviewers will be asked to consider the solicitation-specific review criteria found in the solicitation. NSF will conduct the panels; VMWare team members will attend the panels as observers. NSF and VMWare will meet to discuss the proposals and decide whether to have a reverse site visit for the top rated projects, whereby individual teams are called upon to answer concerns raised by the reviews, NSF program directors or VMWare partners.

NSF and VMWare jointly makes final funding decisions.

**SLIDE 21**

The solicitation-specific review criteria include the following: The extent to which projects:

* have a systems perspective and result in a coherent whole that is more than the sum of its parts We do not want to see individual research topics “stapled together”.
* include evaluation through demonstrations and prototypes of components and an overall system; and
* feature lean, well integrated team of researchers with expertise in security, networking, computer systems and other critical areas necessary to conduct the proposed research

**SLIDE 22**

FUNDING Models.

Projects will be funded jointly by NSF and VMWare through separate NSF and VMWare funding instruments.

* NSF will make grants.
* VMWare will use VMWare agreements.

Projects may receive supplements from either NSF or VMWare.

**SLIDE 23**

NSF and VMWare will work together to jointly manage the NSF/VMware Partnership projects while following the guidelines and regulations governing each party.

NSF and VMware will each designate a Program Director for each NSF/VMware Partnership award. The Program Directors will jointly oversee the execution of the project. VMWare will work with NSF to be active participants, such as advising researchers on technical issues and industry context; with NSF conducting Annual on-site reviews, inviting awardees to site visits at VMWare, accepting invitations to attend site visits at the awardees’ institutions, and potentially hosting student interns. VMware may separately fund its own personnel to directly support the NSF/VMware Partnership research, part-time or full-time, with the institutions awarded projects.

We will add an FAQ with more information about how VMWare might participate in the awarded projects and how they might help awardees identify promising directions for increased industrial and societal impact.

**SLIDE 24**

The SDI-CSCS solicitation aligns nicely with National Priorities as designated by the White House by supporting high-risk, potentially high payoff research and education. We hope that projects will be transform how we think about and design secure, complex engineered systems.

The solicitation outlines potential new capabilities that might result from these systems. Some are listed on the slides and others are included in the solicitation. These are included as examples.

**SLIDE 25**

Note that there are requirements for the Project title. I have also listed the expected supplementary documents.

Please READ the solicitation carefully and take a look at NSF PAPPG 2016 for overall guidance on writing NSF proposals.

**SLIDE 26**

Let me repeat the deadline date. The proposals are due on October 5th. We hope that many of you are already working with high-powered teams to create new secure systems building on the potential power of virtualization and Software-Defined Infrastructure.

**SLIDE 27**

We are open for questions.

We will compile the questions and answers into a Frequently Asked Questions or FAQ list and post it on the webpage for this webinar.