From: Souppaya, Murugiah (Fed)
To: Stine, Kevin M. (Fed); Scholl, Matthew A. (Fed); Dodson, Donna F. (Fed)
Subject: Re: Catch-up on Thursday to discuss RSAC plan
Date: Thursday, January 31, 2019 8:00:05 AM

Here is the info I have collected so far with respect to the activities we are coordinating for RSAC. It is not well organized or formatted but I would like to share it so you can refer to for our meeting.

Thanks

Murugiah

Walt's calendar and meetings with Industry partners at RSAC (include Chuck and Elham?)
- McAfee requested a meeting

Four NIST sessions (Privacy, NICE, Crypto and PQC, and AI)

- Privacy
  - Two rooms available (400 attendees or 75 attendees)
  - Marriott Marquis (can hold up to 400) will be setup theater style with Full AV/Audio (from our previous Public Sector Day event)
  - Learn from NIST representatives about the NIST Privacy Framework: A Tool for Enterprise Risk Management. NIST leadership on the framework effort will hold a panel discussion on development of the framework to date, tackling topics such as: the stakeholder engagement process since kick-off of this effort, the comments received on NIST's Request for Information (issued 11/13/18), the draft outline of the framework, and what was discussed at Workshop #2 in Atlanta, Georgia in February 2019. Attendees will learn how this framework could facilitate their privacy risk management efforts in government, and will have an opportunity to ask questions.NICE - slot, #1 at 1:30 pm - 3:30 pm on Wednesday, March 6
  - Having a call with Ellen, Kevin, and Naomi at 1 today

- NICE
  - slot, #1 at 8:00 am - 10:00 am on Wednesday, March 6
  - Title
    - Employer Use of the NICE Cybersecurity Workforce Framework: Practical Applications and Tools
  - Description
    - The NICE Cybersecurity Workforce Framework (NICE Framework) provides a common taxonomy and lexicon for describing cybersecurity work. The NICE Framework can be used by employers for workforce planning including the identification of cybersecurity human resource needs, development of position descriptions, discovery of skills gaps, and design of education and training curricula to develop and demonstrate employee competencies. This interactive session will engage NICE Program Office staff with employers from the IT sector and others that are looking for standards-based approaches and scalable solutions for growing and sustaining their cybersecurity workforce.
  - Rodney's plan for RSAC
    - NICE Team: Marian and I briefly discussed this morning three possible initiatives to make the most of our presence at the RSA Conference: 1) Some type of employer engagement – either individually or collectively - about the NICE Framework (capitalizing on Murugiah's offer above); 2) Industry engagement and support of creative efforts to increase the discovery and awareness of cybersecurity careers; and 3) NICE participation (and ideally a role!) as part of "College Day" during the RSA Conference. We can discuss these ideas at our next staff meeting.

- AI
  - slot, #2 at 10:30 am - 12:30 pm on Wednesday, March 6
  - Title
    - Trustworthy AI (we can think if a better/cuter title).

- Short paragraph describing the session
    - AI is increasingly taking a central and critical role on monitoring, controlling, and enhancing the services provided by systems that are widely-deployed throughout society. The first version of NIST's Framework and Roadmap for Trustworthy AI Systems is under development and aims to provide a deep investigation into how AI technologies can augment, enhance, or possibly diminish, trustworthiness in ubiquitous computing systems.
    - The session will discuss characteristics and attributes of Trustworthy AI and focuses on identifying the highest-priority issues and on establishing the order in which issues should be addressed.
- Possible questions:
    - How can we understand, or control, propagation of possibly-sensitive information within an AI system?
    - How can we ensure that AI systems don't corrupt high-integrity information?
    - How can AI systems be trained to produce trustworthy results, even in the presence of tainted training data?
    - How can AI systems be trusted given that limitations of their models could be exploited by adversaries?
    - How can AI systems prevent intentional miscategorization caused by adversaries?
    - How robust are AI algorithms?
    - How might AI benefit traditional software practices such as: design, implementation, testing, deployment, intrusion-detection, incident handling, recovery?
    - Should existing software development/deployment/operation practices be updated to account for important AI characteristics and capabilities?
    - How might AI enable more sophisticated, and damaging, attacks?
- Discussion of Trustworthiness in AI
    - Layers of trust
    - Trustworthiness in software
    - Risks associated with AI
    - Performance risks: errors, biases, explainability, generalizability
    - Security risks: Adversarial attacks (data poisoning, inference, stealing model), privacy risks
    - Economic risks: job displacement
    - Societal risks: risk of `intelligence divide'
    - Ethical risks: `lack of value', goal/value alignment
    - Risk of AI going `rouge'
    - Risk management approach to AI?
    - Others?
    - What is Secure AI
    - How to define robustness / resilience / security
    - ISO: ability of a system to resist virtual or physical, internal or external attacks
    - ML community use robust as generalizable
    - What is Reliable AI?
    - How to measure and eliminate bias? In Training data and in algorithms.
    - How to protect privacy? Do models contain PII?
    - What is Explainable AI
    - How to define explainability. Levels of explainability.
    - ISO: ensuring that important factors informing any algorithmic decision can be communicated in humanlike language to users.
    - Relation to transparency. Explainability does not equate to technical transparency

- Crypto and PQC
    - slot, #3 at 1:30 pm - 3:30 pm on Wednesday, March 6
    - Title (proposed):
        - NIST Crypto Update with a Post Quantum Crypto panel discussion targeting IT industry and enterprise
    - Description:
        - (Work in progress)
    - Panelists:
        - Zully (RSA CTO) - confirmed
        - David Ott or Dennis Moreau (VMware) - confirmed
        - Janet Jones (Microsoft) - confirmed
        - Tim Hollebeek (Verisign) - tbd
        - ???

_____
From: Stine, Kevin (Fed)
Sent: Wednesday, January 30, 2019 10:10 AM
To: Souppaya, Murugiah (Fed); Scholl, Matthew (Fed); Dodson, Donna F. (Fed)
Subject: Re: Catch-up on Thursday to discuss RSAC plan

Thanks Murugiah.

_____
On: 30 January 2019 09:03,
"Souppaya, Murugiah (Fed)" <murugiah.souppaya@nist.gov<mailto:murugiah.souppaya@nist.gov>> wrote:

I will send a meeting invite to discuss the RSAC plan.

Walt's presentation at RSA Public sector day. He met with RSA CEO and I was able to catch-up with Tim Shea to share what I have learned.
Walt's calendar and meetings with Industry partners at RSAC.
Four NIST lead sessions (Privacy, NICE, Crypto and PQC, and AI)
Other topics ???

Thanks

Murugiah