NCOIC Update to Members – July 2015

Heath Naquin Joins Advisory Council

Welcome to Heath Naquin of the University of Texas at Austin, who is the newest member of the NCOIC Advisory Council. He is Executive Director in the Office of the Vice President for Research and manages the National Science Foundation Southwest Innovation Corps Node, a consortium of more than 36 institutions focused on advancing commercial outcomes from fundamental research across sectors. Naquin also serves as the Managing Director of the multi-university Center for Next Generation Photovoltaics and is Principal Investigator for the U.S. Department of State Global Innovation in Science and Technology program.

"It is an honor to join the NCOIC Advisory Council as an active participant from academia. The work NCOIC is doing globally to address unstructured problems in interoperability across business, governments and research is a noble and important mission," said Naquin, who is involved in variety of international commercialization and country-building efforts.

NATO and NCOIC Working Together on Interoperability Verification

NCOIC continues to work with the NATO Communications and Information Agency to craft an interoperability verification capability. This exciting project has significant potential to NATO and other organizations in reducing the risk of acquisition and increasing interoperability assurance. The consortium also is working with the NATO Allied Command Transformation to finalize a Framework for Collaborative Interaction (FFCI) agreement that will enhance cooperative interaction; specific areas of interaction include interoperability verification, healthcare and the NCOIC Rapid Response Incubator. You can read more about the FFCI, which is designed to enable non-procurement, collaborative work between ACT and industry, at http://www.act.nato.int/ffci

Advisor John Grimes Steps Down

Longtime Advisory Council member John Grimes has stepped down after serving NCOIC for almost a decade. Grimes was Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer at the US Department of Defense from 2005 to 2009. He also was Vice President of Intelligence and Information Systems / Washington Operations for Raytheon Corporation. Prior to that, he had extensive technical and policy experience in the telecommunications and information fields with the White House staff and the Department of Defense following his service with the U.S Air Force.

Cybersecurity Workshop, Demos Held

NCOIC held its third Cybersecurity Symposium in the Washington DC area on June 30 and July 1. Day one featured five guest speakers from U.S. Northern Command, The Aerospace Corporation and San Diego State University (SDSU) as well as healthcare and cybersecurity companies. Then during the workshop, participants discussed solutions to barriers and security concerns related to secure interoperability for federated cloud environments for information exchange and coordination in disaster response and healthcare—with an emphasis on lessons learned from past government disaster response exercises and NCOIC participation in future exercises. The second day of the symposium consisted of demonstrations of two cybersecurity tools and an update on the NCOIC Rapid Response Incubator.

One highlight of the event was a presentation by Dr. Eric Frost on lessons learned from government disaster response exercises. Frost runs the SDSU Visualization Center and Homeland Security Graduate

Program and is involved in humanitarian disaster relief. His insights, along with the thoughts and observations of other symposium participants, will lead to an update of the NCOIC readout report of problems, solutions and opportunities associated with developing and maintaining a secure cloud environment for rapid response situations such as natural disaster, epidemics and other crises.

The first NCOIC Cybersecurity Workshop held in October 2014 identified 150 barriers, most of which fell into five major groups; results were published in a readout report. A second workshop in March identified 100 potential solutions to those barriers and security concerns; results were published in an updated readout report. The discussion at the third workshop will help refine those solutions and identify additional high-priority barriers and solutions. The overall goal of these workshops is to write a series of NCOIC technical pattern documents.

New Tech Team Leaders Announced

Three NCOIC technical teams recently held elections. Colleen Dealey is now Chair of the Cloud Computing Working Group, with John Quaderer elected to Vice-Chair; Dealey takes over from Mel Greer, who led the group this past year and will continue to participate in its activities. Paula Moss was re-elected Chair of the Services Working Group, which focuses on net-centric related services such as the Emergency Services Playbook and Net-Centric Services Framework. Andy Born was re-elected as Chair of the Cybersecurity Integrated Project Team, which works closely with the Cloud Computing WG on secure interoperability related technologies and governance. Election cycles for the other two teams and the Technical Council Chair position will begin soon.

Cloud Computing WG Activities Showcased

As part of the Cybersecurity Workshop, the Cloud Computing Working Group conducted a follow-on activity to address the identity and access management challenges of the NCOIC Rapid Response Incubator (RRI) environment. Dr. Craig Lee of The Aerospace Corporation gave an in-depth presentation of the virtual organization model and how it can be used to facilitate rapid access to tools, data and applications within the RRI. Dr. Alenka Brown of McClure Brown & Associates discussed how cognitive fingerprinting could play a key role in user authentication in a low-governance, low-user friction environment typical of RRI emergency response users and analyze their actions as part of a re-vetting capability.

These concepts will be further explored as the group focuses on interoperability among various methods of authentication. The RRI is designed to provide a basic level of trust in the development environment, with a more secure, robust transition environment where these types of tools will allow for the development of multiple, interoperable security solutions. The Cloud Computing WG will work to identify various participants from the first responder community, non-governmental organizations and others to assist in establishing basic requirements for identity and access management to drive solutions in the RRI.