

INTERNET²
2016
GLOBAL
SUMMIT
MAY 15-18
CHICAGO



END-TO-END TRUST & SECURITY INNOVATION WORKING GROUP

E2ET&S Innovation Working Group

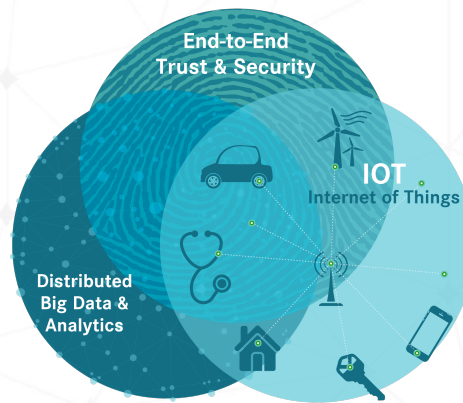
AGENDA

- **Evolution of the E2ET&S Innovation Working Group:** Florence Hudson, Internet2
- **Update on Recent E2ET&S Working Group Activities:** Scot Ransbottom, Va Tech
- **CSG Session on E2ET&S for IoT:** Scot Ransbottom, Va Tech
- **E2ET&S for Healthcare:** Mark Cather, UMBC
- **IoT Related Policy, Ethics and Education:** Mark Cather, UMBC
- **Introducing the Smart Campus Initiative:** Emily Nichols, Internet2
- **IoT Systems Risk Management Task Force:** Chuck Benson, University of Washington
- **Next Steps:** Florence Hudson, Internet2



Collaborative Innovation Program

**Established three new Collaborative Innovation Working Groups
During Global Summit 2015 based on March 2015 Member Survey**



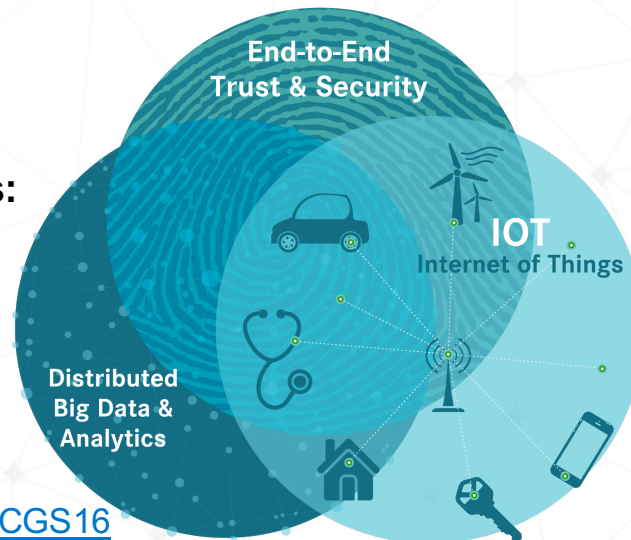
Collaborative Innovation Program Current Focus Areas

E2E Trust & Security:

- End to End Trust and Security for IoT
- TIPPSS – Trust, Identity, Privacy, Protection, Safety, Security
- SDP (Software Defined Perimeter), Network Segmentation

Distributed Big Data & Analytics:

- Genomics
- Smart Campus/Smart Cities
- Digital Humanities

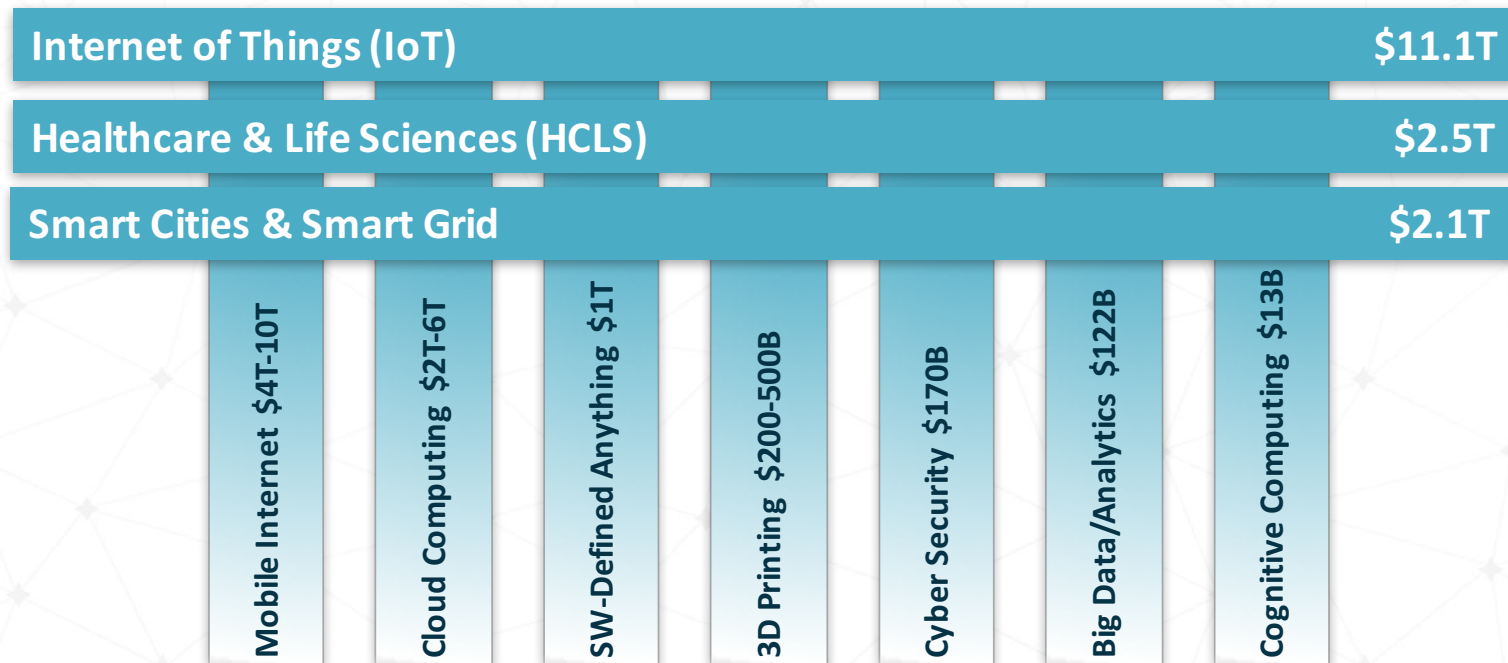


Internet of Things:

- IoT Sandbox
- Smart Campus/Smart Cities
- Smart Grid Testbed

Join a working group: <http://bit.ly/CINCGS16>

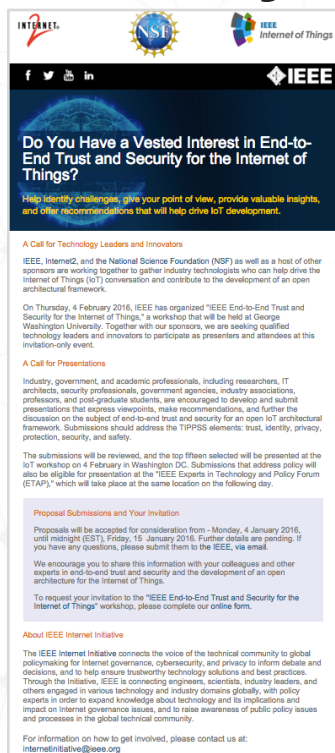
The Internet of Things, Healthcare & Life Sciences, and Smart Cities could represent \$15T in global economic value in 2025



Economic value includes revenues, cost reductions & service improvements achieved

Sources: Internet2 CINO analysis; BizTech; Deloitte; Consultantcy.uk; Forbes; Markets and Markets; McKinsey; US Department of Agriculture, Economic Research Services.

Recent E2ET&S Activities: E2ET&S for IoT Workshop, February 4, 2016



Event at the George Washington University Marvin Center in Washington, DC in co-sponsored by Internet2, IEEE, NSF, and George Washington University

- Followed by IEEE Experts in Technology & Policy (ETAP) event. Final ETAP report available on our CINO Wiki (<http://bit.ly/1rpQN6u>)

150+ participants, 35+ papers presented

Agenda:

- Opening panel with participants from the US DoE, IEEE, IIC, NSF, and M2Mi
- Afternoon break outs on Access Control & Identity Management; Architectural Framework; Policy & Standards; and Scenarios & Use Cases
- Focus on **TIPSS: Trust, Identity, Privacy, Protection, Safety & Security**

Next Steps:

- Opportunity for IoT-related education a key theme (E2ET&S, educating future leaders)
- Internet2 on panel at IEEE conference on Connected Health: Applications, Systems & Engineering Technology (CHASE) event, June 27-29 in Washington, DC (<http://bit.ly/1W6x1Wt>)

Recent E2ET&S Activities: Webinars

- Software Defined Perimeter: September 1, 2015
 - Cloud Security Alliance’s Junaid Islam outlines how Software Defined Perimeter (SDP) can secure open networks and fend off cyberattacks
 - Developing the specs for V2. Want to get involved? Contact Junaid Islam jislam@vidder.com
 - Recording and slides available: <http://bit.ly/1phYI3M>
- Network Segmentation for IoT: February 2, 2016
 - Cisco’s Paul Forbes Bigbee outlines the use of network segmentation to ensure additional IoT connected devices don’t undermine overall network security
 - Based on a blog post by Scott Harrell, Cisco Vice President Product Management, Security Business Group in *The Security Ledger* <http://bit.ly/1A1acwl>
 - Recording and slides available: <http://bit.ly/1Q2eDcl>

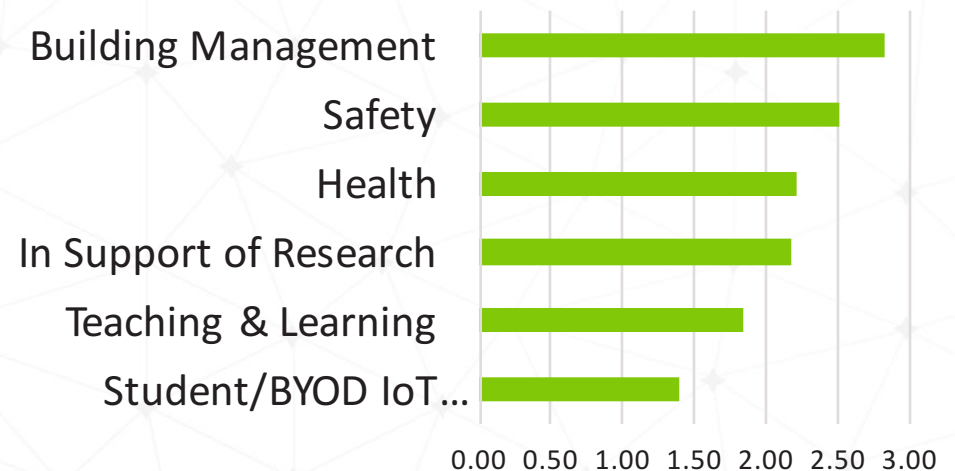
CSG Session on E2ET&S for IoT: IoT is becoming a campus reality in Smart Buildings, Research, & Healthcare

Participation in IoT use cases on or off campus

	On Campus	Off Campus
Smart buildings	6	0
Research projects	5	3
Connected healthcare	3	3
Smart stadiums	3	1
Connected vehicles	2	2
Smart museums	1	0

N = 6

Rank importance of IoT use cases on your campus



E2ET&S for Healthcare

- Big Data in HCLS Innovations
 - Much of the research is done with anonymized data but value comes from personalization of the data
 - Narrowing results to a Zip code, industry employees, personal activities, etc...
 - Balance risks to privacy, security, and ethics against benefits of personalization within data sets.
- Movement of HCLS data between trusted and untrusted systems. Ex. Hospital & Academic
- Innovation vs. HIPAA, FISMA, FDA, and state regulations.
- Privacy and Security for huge HCLS data flows across a global compute infrastructure.
- Ethics, Privacy, and Security training resources are needed for a growing research community.
- Health data is being spread to computer scientists and other disciplines.
- Global HCLS: How to collaborate around HCLS in a global privacy and legal environment.
- How do we overlay HCLS regulations, security, and privacy onto a Science DMZ concept.
- How can Shibboleth and InCommon Play a Role in IDM for HCLS?
- IoT of HCLS Devices - Pacemakers, FitBits, Insulin Pumps, etc.
- IEEE Conference on Connected Health: Applications, Systems and Engineering Technologies, June 27-29 in Washington, D.C.: <http://bit.ly/1W6x1Wt>

IoT Related Policy & Ethics

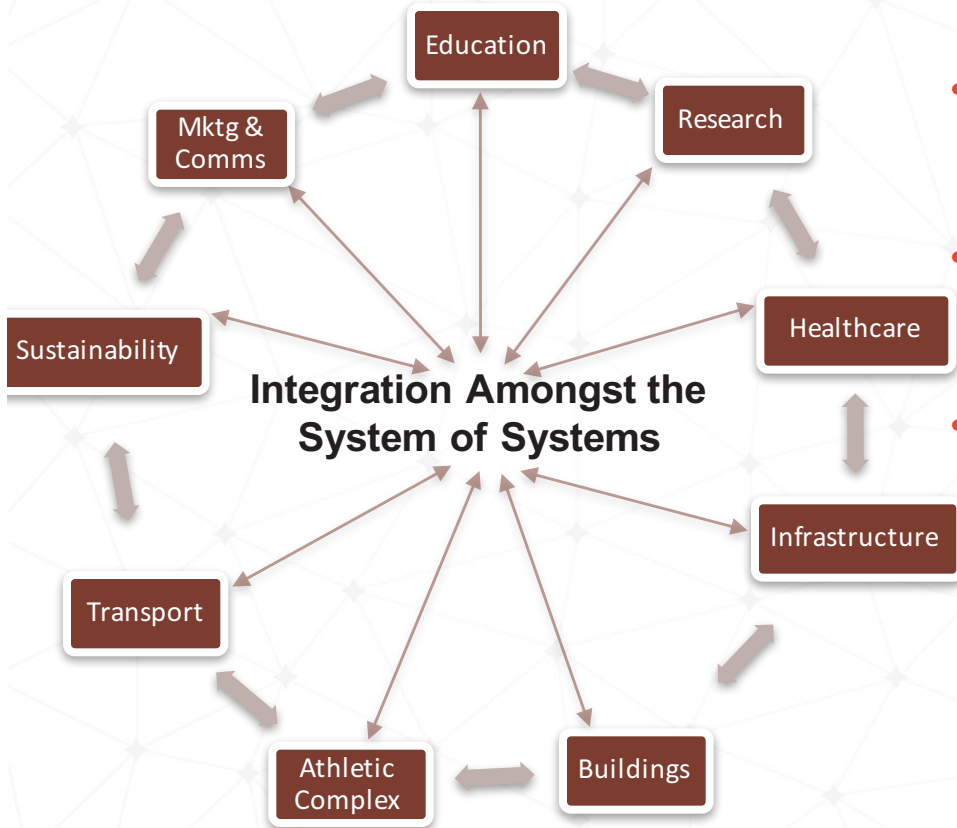
- An initial group has formed including Berkeley, UMBC, Virginia Tech, University of Pennsylvania, and Princeton.
- Starting Points of the Group
 - Explore how the law, policy, and ethics around technology need to evolve to try and keep up with technology and enable innovation rather than restrict it.
 - Explore how to educate the community at large about proper ethics and risk taking related to technology.
- Examples Topics
 - How do we train society on privacy and the ethical use of data?
 - How do we train new technologists to develop secure, open technical solutions?
 - How do we support consent to use data in a dynamic environment like the IOT?
 - Can a framework be developed to allow machines to understand and negotiate privacy and security policies on-the-fly?
 - How can we support HCLS data flows and innovation while maintaining regulatory compliance, privacy, and security?

Welcome to the Smart Campus Initiative

- Forum to share learnings and develop new insights and practical recommendations
- Create focused task forces to support collaborative development of practical recommendations
- Guided by a Smart Campus CIO Advisory Council



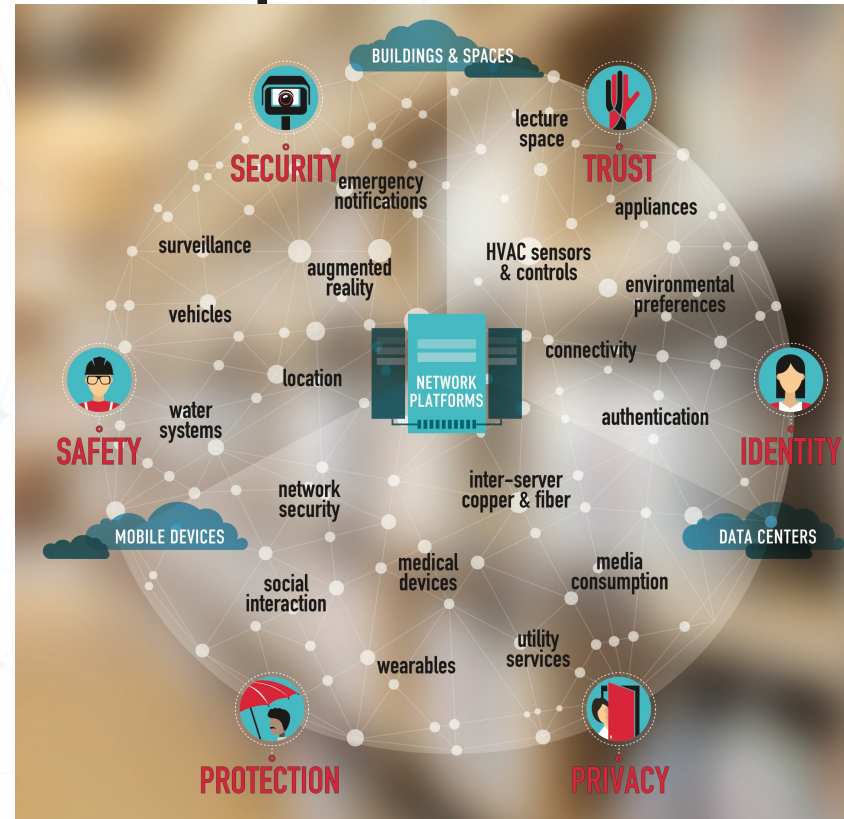
Defining a Smart Campus



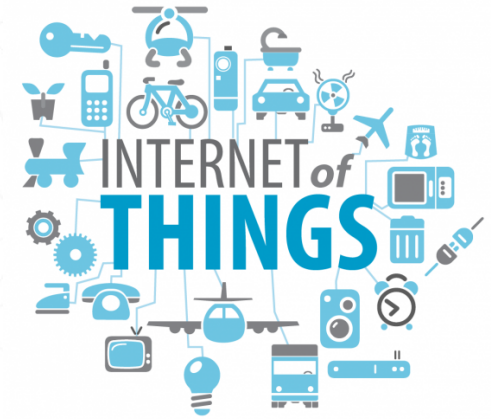
- A Smart Campus leverages data to **improve student success, experience and campus operations**
- Requires integration of Information Technology and Operational Technology to **better inform decision making** in each domain and across the campus
- Achieving a Smart Campus will involve cross-campus collaboration with multiple stakeholder partnerships. These partnerships will include, but not be limited to:
 - Facilities
 - Administration
 - Central IT
 - Research Community
 - Campus Security
 - Faculty & Students

Addressing TIPPSS is essential to achieving safe, secure, scalable future smart city and campus architectures

Trust
Intity
Privacy
Protection
Safety
Security



Smart Campus Initiative: IoT Systems Risk Management Task Force



Great potential in IoT Systems in Higher Ed institutions --
Energy management, sustainability, building access control,
research automation & environmental control, building
automation, safety systems, academic learning systems ...

IoT Systems

Implementation & Management

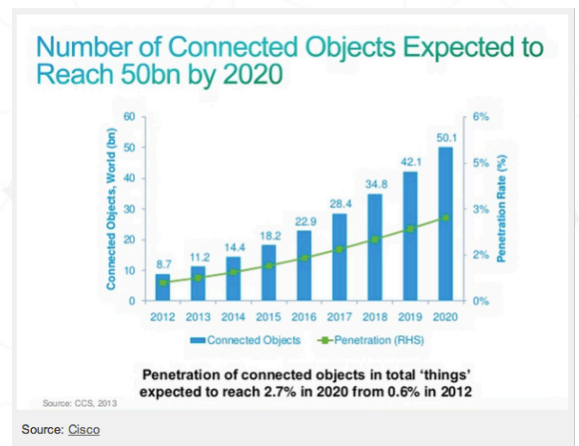
The Real World – e.g. Campus, City, ...

But potential not realized if IoT System is not implemented & managed well. Topics include:

- Vendor management – articulating & raising expectations
- Vendor management – multiple proprietary systems
- System ownership
- IoT System selection, procurement, installation
- Costing models & approaches
- System risk identification & management
- Network segmentation & portfolio management
- Organizational/Culture change
- Others

Smart Campus Initiative: IoT Systems Risk Management Task Force

- IoT Systems are different from traditional enterprise systems
 - Large numbers of networked, computing devices
 - High variability within device types
 - Little language/conceptual framework for system planning & managing risk
 - Out of sight, out of mind – Systems embedded in the environment around us
 - IoT Systems tend to span multiple organizations within an institution



Smart Campus Initiative: IoT Systems Risk Management Task Force

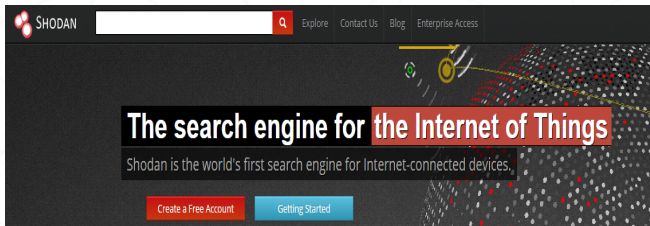
Some participating schools/networks:

- Clemson
- Cornell
- Indiana University
- MIT
- Princeton
- Rice
- Virginia Tech
- University of Pittsburgh
- University of Washington
- University of Wisconsin-Madison
- Yale
- HEA-Net (Ireland)

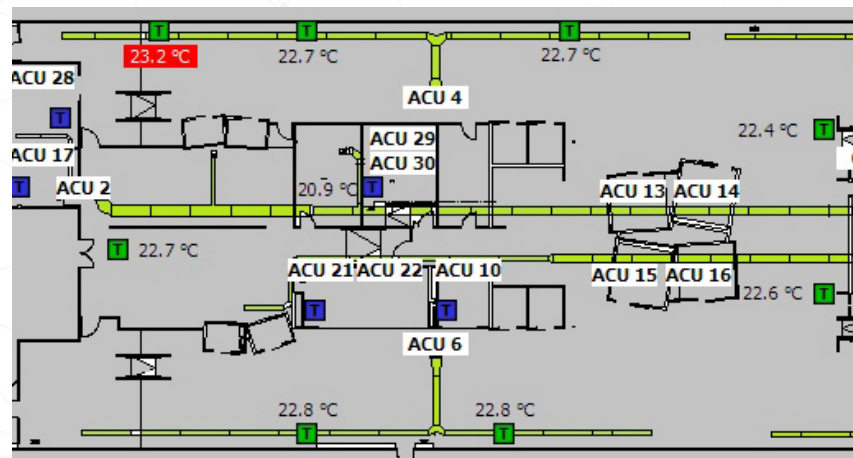
Some roles/titles of participants:

- AVC Operations & Maintenance
- AVP & Chief Facilities Officer
- Associate CIO
- Chief Technology Officer
- Deputy CIO/Chief of Staff
- Enterprise Architect
- Infrastructure Director
- IT Service Owner for Research
- Network Development Manager
- Research Cyber Infrastructure Liaison
- Security Manager
- Senior Applications Systems Engineer

Smart Campus Initiative: IoT Systems Risk Management Task Force



- The search engine for **Power Plants**
- The search engine for **Buildings**
- The search engine for **Refrigerators**
- The search engine for **Webcams**



Smart Campus Initiative: IoT Systems Risk Management Task Force

Proposed topics for Quarterly Report Outs to Smart Campus CIO Advisory Council:

Quarter 1 – Sept 2016: Ability to profile IoT Systems exposure w/public tool (e.g., Shodan.io or Censys.io)

Quarter 2 – Dec 2016: Vendor management – Standards doc for IoT Systems vendors (process, checklist, etc.)

Quarter 3 – March 2017: Cost model for IoT Systems selection, procurement, & management

Quarter 4 – May 2017: Recommendations for further work in 3 – 5 areas

- network segmentation management ?
- organizational/culture change ?
- development of IoT Systems risk language/taxonomies ?
- dependence on non-interoperable proprietary IoT Systems ?
- other ?

Next Steps

- Let us know if you're interested in participating in the IoT Related Policy & Ethics discussion: Email CINO@internet2.edu
- Let Chuck Benson know if you're interested in participating in the IoT Systems Risk Management Task Force: Email iotsys-tf@internet2.edu
- Save the date! CINC Up Call for entire Collaborative Innovation Community on Monday, June 6 at 2PM ET. Topic: OpenFog Consortium presented by Mung Chiang, Princeton University and OpenFog Consortium Board Member
- Let us know if you'd like to participate in the E2ET&S Working Group, or any of the other Collaborative Innovation Community Working Groups, or the Collaborative Innovation Community at large (CINC Up): Email CINO@internet2.edu

Join us for other Collaborative Innovation Community Meetings during Global Summit

- **Sunday, May 15**
 - Healthcare and Life Sciences Working Meeting: 10:30AM-12PM, Cook Room, 3rd Floor
 - Smart Campus Initiative & Innovations: 4-5:30PM, Kane Room, 3rd Floor
- **Monday, May 16**
 - Internet of Things (IoT) Innovation Working Group Meeting: 8-9:30AM, Kane Room, 3rd Floor
 - End-to-End Trust & Security Innovation Working Group Meeting: 10-11:30AM, Kane Room, 3rd Floor
- **Tuesday, May 17**
 - Distributed Big Data and Analytics Innovation Working Group Meeting: 7:30-8:45AM, Kane Room, 3rd Floor
- **Wednesday, May 18**
 - Gender Diversity in the Internet2 Community: 7:15-8:45AM, Addison Room, 4th Floor
 - Innovation Development and Management – Think Local, Act Global: 12-1:15PM, Kane Room, 3rd Floor



INTERNET[®]



2016
GLOBAL
SUMMIT
MAY 15-18

CHICAGO



END-TO-END TRUST & SECURITY INNOVATION WORKING GROUP