Proposal Example 1

Information and Communications Technology (ICT) has taken a central role in modern society. Unfortunately, malicious hackers and cybercrime have become a stubborn and expensive part of the ICT landscape. This has made providing cybersecurity a defining challenge for our era. Many strategic plans and National Academies of Sciences (NAS) studies have been written, and billions of dollars have been spent on the development and deployment of innovative cybersecurity solutions, but our network infrastructure, devices and organizations are increasingly insecure against threats. Quite recently (in January 2016), the federal government released a new cybersecurity federal R&D strategic plan – this one mandated by Congress – that is novel in that it engages the socio-technical nature of the systems that we are securing. The plan also emphasizes the need for understanding the efficacy of different approaches, albeit empirically, economically, or mathematically. However, in order to make meaningful progress, using a socio-technical approach requires innovation driven by informational and experiential diversity.

A socio-technical approach to cybersecurity recognizes that the science and technology deployed to protect and defend our information and critical infrastructure must consider human, social, organizational, economic and technical factors, as well as the complex interaction among them, in the creation, maintenance, and operation of our systems and infrastructure. Furthermore, measuring the evidence of efficacy of different approaches is often a socio-technical issue.

There is ample evidence to suggest that socio-technical efforts could prove fruitful. Billions of dollars are spent each year securing network infrastructure, devices, and resources against threats, but often the very people that these systems are supposed to protect find ways around these cybersecurity mechanisms because they were designed with insufficient attention to the needs, capabilities and behaviors of the users. In 2014, the IBM Security Services 2014 Cyber Security Intelligence Index reported that over 95 percent of all incidents investigated recognize “human error” as a contributing factor. User error and misuse are responsible for 68% of security incidents and 29% of cybersecurity breaches are accomplished purely through social tactics, according to Verizon’s most recent cybersecurity report. Symantec’s 2015 *Internet Security Threat Report* (Volume 20), reported that attackers trick companies into infecting themselves by Trojanizing software updates to common programs and patiently waiting for their targets to download them. They also reported that attackers have increased highly-targeted spear phishing attacks by 8 percent in 2014. These attacks are quite precise, and used 20 percent fewer email messages to successfully reach their targets. In short, human behavior is the proverbial Achilles’ heel for our secure systems and critical infrastructure and organizational politics have not provided sufficient protection.

Previous efforts to build cybersecurity capability have not excluded the human element, but it has received insufficient attention. In 2002, the Computing Research Association (CRA) sponsored its first “Grand Research Challenges in Computer Science and Engineering” conference. This was the first in a series of highly non-traditional conferences to encourage thinking beyond incremental improvements. Because of the importance of information security and assurance, CRA’s second Grand Challenges Conference, held in 2003, was devoted to defining technical and social challenges in trustworthy computing.

Nearly fifty technology and policy experts in security, privacy and networking met in November 2003 in a Gordon-style conference, and produced four grand challenges in trustworthy computing. They were:

- Within the decade, eliminate the threat of all epidemic-style attacks such as viruses and worms, spam, and denial-of-service attacks

- As many new systems with great societal impact are currently planned or under development, develop tools and design principles that will allow these systems to be highly trustworthy
- Develop and validate quantitative models of risk and reward and deploy them to decision-makers so that progress can be made
- Setting one's sights on the dynamic, pervasive computing environments of the future, provide understandable security and privacy to tens of millions of new users

Each grand challenge was presented with an explanation of why progress was possible and a description of barriers to progress. In both sections, socio-technical aspects are only lightly touched upon. For example, the reluctance of organizations to release data was listed as a barrier for the third challenge, and a barrier for the fourth challenge was that "IT will be much more human-centered that it has been in the past, and it will be a significant challenge to bridge this gap between users and underlying mechanism".

Much has changed since the 2003 CRA workshop. The kinds of researchers working on cybersecurity has broadened in response to the clear need to understand the human aspects of cybersecurity. The National Science Foundation (NSF), for example, has issued a series of Dear Colleague Letters soliciting proposals for new collaborations between computer scientists and social, behavior and economic scientists: nearly 40 EAGER grants have been funded over the last three years. Psychologists, behaviorists, economists, cultural anthropologists, and those who research improved design techniques for inclusion are actively researching issues in cybersecurity. Workshops and conferences have been created that study the human sides of cybersecurity, such as the *Workshop on the Economics of Information Security (WEIS)*, the *Symposium on Usable Privacy and Security (SOUPS)*, and the by invitation only interdisciplinary *Workshop on Security and Human Behavior (SHB)*. Cybersecurity is being studied in the context of the individual, of groups such as management units, organizations, and societies.

This diversity of effort is encouraging, but creates new challenges for the field of cybersecurity. The disciplinary nature of academic institutions and pressures to publish in top outlets within one's home discipline has resulted in a literature that is fragmented and renders integration and dissemination of important findings difficult at best.

We propose a reprise of the 2003 CRA workshop, again with the goal of developing a small set of grand challenges to set direction for the field, but this time with the understanding that the systems requiring cybersecurity are socio-technical, and so the approaches must be firmly socio-technical as well. Attendees will be drawn from a broad set of disciplines in the social, behavioral and economic sciences as well as from computer science and data analytics. The workshop will also consider diverse cybersecurity contexts ranging from the individual to the organization and to the society.

We intend to advocate an evidence-based sociotechnical cybersecurity approach, integrating the best research evidence with diverse cybersecurity expertise and broadening the consideration of ICT user characteristics. Our intention is that the grand challenges will promote effective and appropriate consideration of the socio-technical factors and sound and effective principles of cybersecurity assessment, evaluation, and intervention. The resulting report will help illuminate the implications for cybersecurity researchers of taking a socio-technical approach identifying human, social, organizational, economic and technical factors that must be considered, techniques for understanding the interactions among them, and positive steps that can be taken to better protect and defend our information and critical infrastructure.

We will seek broad representation in the workshop participants across academics, industry, and the public sector, as well as across research disciplines. While we have not yet approached them, the following

people are examples of potential participants: ….

We expect that the organizing committee will need to solicit white papers across several different research communities. Drawing our attendees from such a broad set of disciplines will be essential for identifying and integrating the best research evidence with cybersecurity data to ensure that we have the highest probability of achieving the goals of the workshop.

To evaluate the results of the workshop, we will disseminate the results through channels such as workshop panels, birds of a feather sessions (BoF), symposia, and through publications such as in editorials and special issues, to promulgate and refine the concepts generated by the workshop. We will seek out organizations such as the Industrial Internet Consortium (IIC) and the Semiconductor Research Consortium (SRC) and other public private partnerships as appropriate to the grand challenge problems. The results will also be socialized with the relevant Federal agencies such as the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST), the Networking and Information Technology Research and Development (NITRD) program and the Office of Science and Technology Policy (OTSP), with the assistance of the Computing Research Association (CRA).

Structure
The workshop will have an organizing committee chosen from a broad set of research strengths and selected for their interest and vision for discovering challenge problems in cybersecurity that focus on the socio-technical. The following people have agreed to serve on the organizing committee:

……

Rather than following a Gordon Research Conference format, a pair of workshops will be held to create the time needed for ideation in a highly multidisciplinary endeavor.

A person who wishes to attend will be asked to submit a brief position statement (‘white paper”) that explains their interests in attending the workshop, suggests a challenge problem, and describes their experience and interests in interdisciplinary research. The organizing committee will select attendees based on these white papers, with the goal of assembling a diverse set of attendees who have the experience and interest to contribute to the effort.

Workshop Schedule and Milestones

Early April 2016 Pre-Workshop Virtual Meeting	Introductions and discussion on call for white papers (CFP)
Early April 2016	CFP issued with a one-month deadline and a three-week review period.
Late May 2016 – Early June 2016 Organizing Committee Program Review (virtual)	Discussion of white papers and of potential areas of interests; Decision on 10 people to invite for experience and expertise; Issue invitations with potential areas and covered expertise.
Early August 2016 First Workshop (2 days)	Lightening talks (4 hours @ 15 mins/person); Cybercafe to develop potential Grand Challenge Problem (GCP) areas; Refinement of GCP areas and selection of six GCP areas; Formation of working groups.
Interstice	Each GCP area chooses others to invite to the second workshop; Issue a second CFP if necessary; Expanded working groups develop potential GCPs in area and circulates a short report to second workshop attendees: What we know/What is the state of the art, What we still need to know/Desired outcome, and what are the barriers to achieving this.

Mid-January 2017 Second Workshop (2.5 days)	Icebreaker; Each GCP working group gives a 20-min presentation + 10-min discussion; Ideation to develop (cybercafé); Second day will be a cycle of presentations, comments, and refinement; Third day starts with a prioritized ordering of GCPs; Remainder of day will focus on drafting of report outline and writing assignments, plus discussion of other next steps.
March 2017 Dissemination	Organizing committee meets with NSF, NIST, and NITRD

Budget

For the First Workshop, to be held in early August 2016 at the University of Maryland, College Park, the budget should include lodging (2 days/3 nights), daily meals, a welcome dinner for 20 participants, and venue costs at the University of Maryland Marriott.

For the Second Workshop, to be held in mid-January 2017 at the University of California, San Diego, the budget should include lodging (3 days/2 nights), daily meals, a welcome dinner for 60 participants, and venue costs. The UCSD recommended venue incudes meeting rooms on the 15th Floor at the Village at Torrey Pines ($44k) and the recommended hotel is the Estancia Hotel, which is in easy walking distance to the venue.

For Dissemination, the budget should include travel and accommodation funds for the organizing committee to meet with NSF, NIST, and NITRD to report out to those agencies with the goal of supporting the 2016 strategic plan.

Organizing Committee Bios

…..