University of the District of Columbia
Institute of Public Safety and Justice
Department of Criminal Justice, Sociology, and Social Work
4200 Connecticut Ave., NW
Washington, DC 20008
202-274-5687

STATEMENT OF PURPOSE:

The University of the District of Columbia's Institute of Public Safety and Justice (UDC-IPSJ), part of the University's Department of Criminal Justice, Sociology, and Social Work, appreciates this opportunity to make comment and to be of service to the U.S. Department of Commerce's National Institute of Standards and Technology as it seeks input from industry sectors on the development, promulgation, and implementation of national cybersecurity standards (RFI Docket: 130208119-3119-01). With this submission, the Institute addresses academia as a sector subject to imminent regulation. The academy has a cross-cutting mission-set, public-private partnerships, differently-facing stakeholders, multi-Agency dependencies, and a not-insignificant focus on civil liberties; each requiring, singly and in combination, additional address. Simply put, we believe that NIST must acknowledge that successful regulation and promulgation schema includes 1) explaining the most basic tenets of cybersecurity to include fundamental digital literacy and digital hygiene; 2) being broadly-inclusive; 3) including child-protective and vulnerable-citizen protective modalities at all levels of regulation and programming; and 4) including cybersecurity *and* digital media operations in emergency management operations. Our observation from multiple conversations with academic, public, and private stakeholders around the NIST is that there is tremendous focus, energy, and resources at the top tier of technology, and the most sophisticated stakeholders. We suggest that NIST also must consider and include those most likely to be left in the pixel-pile.

About UDC-IPSJ, Its Mission, and Successful Performance as a DHS Grantee

The Institute for Public Safety and Justice at the University of the District of Columbia has a tripartite mission of research, training, and evaluation; coupled with an aggressive service and outreach thrust to government agencies, community-based organizations, faith-based organizations, and other non-profit entities. The Institute seeks to address the University's urban land grant mission by strengthening communities to better resist crime, disorder, and social decay. This mission is directed towards addressing the issues of crime, its related causal factors, community capacity building, as well as broader issues of justice and inequity. The Institute is an integral component of the Administration of Justice and Homeland Security Programs at the University of the District of Columbia and has the responsibility for implementation of the Program's contribution to the University's urban land grant mission. This Comment is comprised of four parts: 1) Executive Summary; 2) Body of Comment; 3) UDC Capabilities; 4) Suggested next-steps and Summary. It works in concert with the NSF funded Assurance in Research Center for Trusted Information Computing in cybersecurity education and research activities.

1) EXECUTIVE SUMMARY:

With this submission, the Institute addresses academia as a sector subject to imminent regulation. The academy has a cross-cutting mission-set, public-private partnerships, differently-facing stakeholders, multi-Agency dependencies in differently-specialized departments that receive Federal research grants, and a not-insignificant focus on civil liberties; each requiring, singly and in combination, additional address. Of particular note and interest are the starkly different levels of digital literacy between faculty and students; the lack of basic digital hygiene in different modes by both faculty and students; and the lack of a self-replicating mechanism to drive understanding through the most broadly-inclusive spectrum of colleges and Universities at the state, junior, and community levels. Each of these three drives critical security vulnerabilities for which redress must be more comprehensive than issuing norms. Holistic address, systemic education that pairs online and offline components, and concrete measures of program effectiveness must be an essential part of regulatory schema for the academy. We elaborate in the body of comment, below.

2) BODY OF COMMENT:
Academia is a critical intersection-point between two differing cohorts of usage for cybersecurity; an institution capable of positive teaching, innovation, and influence in cybersecurity and STEM-supportive disciplines; and an institution, itself, in great need of functional support to address known and emergent vulnerabilities. This is a persistent tension-area of usage between two major cohorts, and it cuts both ways, with implications for cybersecurity, as follows:

- "Digital Immigrants"[1], eg, those who "migrated" from analog world to a digital world. There are three important factors to understand about this cohort's use case:
  a) They frequently do not make the best use of *existing* technology due to lack of skills;
  b) They frequently do not make the best use of *emergent* technology due to an *inherent distrust* of the technology; and
  c) The "Digital Immigrants" may also have a more robustly-developed sense of personal privacy grounded in an analog experience of what is, and is not, supposed to be publicly-available information.
- "Digital Natives"[2], eg, those who were "born digital". The "Natives" have always experienced life using, intaking information from, and exchanging information, digitally. There are several important factors to understand about this cohort's use case:
  a) "Natives" make adept use of extant *and* emergent technology due to an adaptive skillset promulgated from early childhood education onward;
  b) They *trust* extant and emergent technology for delivery of services and communication, without critically examining it; and
  c) The "Digital Natives" have a less-robustly developed sense of personal privacy, and private personal identity, making volumes of personal data, location, preferences, opinions, publicly available in a persistent digital timeline.

Academia is a critical intersection-point for these two cohorts. Academia is also a critical intersection-point across every important functional domain affected by cybersecurity. On the positive/functional side, the academic infrastructure is uniquely positioned to provide essential instruction to both "Immigrants" and to "Natives" about cybersecurity at the institutional, and the personal, levels. Academia also drives innovation in the space. On the vulnerability side, academia itself is at risk for major institutional cybersecurity breaches, as well as liability to individual user behaviors (see **Table 1**). Because "cyber" is a complex domain, it can drive security vulnerabilities in any physical-security, functional, or behavioral realm.

[1] Palfrey, J & Gasser, U. Born Digital: Understanding the first generation of digital natives. New York: Perseus Books, 2008.
[2] Ibid.

University of the District of Columbia
Institute of Public Safety and Justice
Department of Criminal Justice, Sociology, and Social Work
4200 Connecticut Ave., NW
Washington, DC 20008
202-274-5687

Cybersecurity Vulnerabilities in Academia	•Poor security hygiene can create critical infrastructure vulnerabilities to outside attackers and insider threat actors •Individual user-error can compromise Federal / Defense security under USG grant programs •"Digital Immigrants" at the Administration level may fail to recognize or act upon disruptive technology or usage •SM usage by students and faculty can create physical, business, and legal vulnerabilities to the institution •Poor cybersecurity infrastructure, or poor cybersecurity hygiene by faculty, can create institutional vulnerability to international cyberespionage efforts that are pervasive, ongoing, and frequently undetected •Lack of understanding of cyber/SM usage by students and faculty can lead to serious physical security vulnerabilities (active shooter scenario [Blacksburg], dorm harassment scenario [Rutgers])
Positive/Functional Influence of Academia in Cybersecurity	•Can provide essential instruction on: - cybersecurity hygiene and best-practices - forms and types of cybersecurity threats, how to spot and how to report them (eg, DHS "Stop. Think. Connect.") •Broad reach and influence to: - faculty via institutional training - students via training/curricula - communities via local community outreach - vendors to the institution and local businesses - grantees - secondary academic institutions such as community colleges and local technical schools •Academic teaching and research in STEM-supportive subjects, including cybersecurity, drives innovation. - The Internet, itself, came out of University usage of DARPA's ARPANET in the late 1980's. - Facebook was created in a dorm room at Harvard.

University of the District of Columbia
Institute of Public Safety and Justice
Department of Criminal Justice, Sociology, and Social Work
4200 Connecticut Ave., NW
Washington, DC 20008
202-274-5687

3) UDC CAPABILITIES:

UDC can lever its successful performance as a DHS and National Science Foundation grantee to design, develop and promulgate train-the-trainer curricula that will be used to teach other academic institutions, particularly urban land-grant Universities, a functional/cognitive framework of cybersecurity, with four specific content units that address:

1) physical cybersecurity hygiene best practices,
2) social media best practices policy,
3) child protective and vulnerable-citizen-protective practices, including cyber-incident reporting,
4) emergency incident mitigation and response.

Each of the four specific content areas should have a Senior Federal Mentor from relevant sectors for compliance and quality assurance, as well as an Industry Mentor to ensure leading-edge content. To drive measures of program effectiveness, the overall curricula and the four specific content units will be held online, and then made available to other Universities once they have completed the training and provided the requisite documentation and metrics reporting to UDC-IPSJ. The curricula then is provided to the trained Universities to be used as a teaching modality to their own Faculty, Students, and as a practicum / outreach to be used by Faculty and student-teachers to train other academic institutions such as community colleges, University annexes, and urban trade/technical schools. UDC can lever its NSF-funded Hadoop ARCTIC cloud to will design, and create, a “wiki” and an online conversation forum, in which NIST, UDC-IPSJ, and the participating Academic institutions who successfully complete training, can continue to communicate, share important developments, success stories, practices, and lessons-learned. This also creates a collaborative environment for future STEM-supportive academic collaborations under DHS programming, and for shared data-repositories for use by researchers who have previously been inhibited by a lack of scalable computing power. By doing this we intend to break down “silos” of knowledge and to be broadly inclusive to bring some of the most vulnerable communities, into the mainstream of regulatory compliance and the cybersecurity conversation. A Homeland Security - Computer Science faculty collaboration already has one article on Cybersecurity published in the IEEE Digital Library, another article accepted for publication in the Journal of Homeland Security and Emergency Management and is working on a third research publication in this important area.

4) SUGGESTED NEXT-STEPS AND SUMMARY

UDC-IPSJ respectfully offers that it would like to participate in workshops, seminars, committees, or other volunteer bodies during the preparatory period. We also respectfully offer our services to provide this type of programming upon promulgation of regulation. Again, we truly appreciate this opportunity to make comment and to be of service to NIST.

Respectfully Submitted,
Dr. Sylvia Hill, PhD, Co-Director, UDC-IPSJ
Dr. Angelyn Flowers, JD, PhD, Co-Director, UDC-IPSJ
Drafted by Ms. Larisa Breton, MPS, adjunct faculty