FASHION
INNOVATION
ALLIANCE ™

September 9, 2016

Via Electronic Mail: cybercommission@nist.gov

Nakia Grayson
National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Input to the Commission on Enhancing National Cybersecurity

Dear Ms. Grayson:

The Fashion Innovation Alliance (FIA) submits these comments to the Department of Commerce, National Institute of Standards and Technology (NIST) in response to the notice for public comment on *Information on Current and Future States of Cybersecurity in the Digital Economy*, published in the *Federal Register* on August 10, 2016. *See* 81 Fed. Reg. 52,827 (August 10, 2016).

The Fashion Innovation Alliance is a nonprofit trade association representing leaders in fashion and technology committed to shaping the future of fashion tech, including smart textiles, wearables, e-commerce, and mobile apps. The social and economic value of fashion tech continues to expand and is revolutionizing how we live our lives. The U.S. Census Bureau of the Department of Commerce announced in August that the e-commerce retail sales estimate for the second quarter of 2016 increased 15.8 percent from the same period in 2015.[1] Additionally, apparel e-commerce sales in the United States are expected to reach $50.4 billion in 2018.[2] The future of fashion tech continues to grow for the wearables market too, which is estimated to be worth $25 billion by 2019.[3]

[1] Quarterly E-Commerce Retail Sales, Second Quarter 2016, U.S. Census Bureau, U.S. Department of Commerce, August 16, 2016, *available at* https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

[2] E-commerce Apparel Sales to Reach $50.4 Billion, Women's Wear Daily, Oct. 15, 2015.

[3] Wearables Market to Be Worth $25 Billion by 2019, CCS Insight, Aug. 2015, *available at* http://www.ccsinsight.com/press/company-news/2332-wearables-market-to-be-worth-25-billion-by-2019-reveals-ccs-insight.

The Alliance welcomes the opportunity to share with NIST the state of cybersecurity for fashion tech, especially given the emerging technology trends and innovation in e-commerce, mobile, and smart accessories and apparel.

## EXECUTIVE SUMMARY

The digital age has transformed how companies in fashion tech—fueled by strategic partnerships and collaborations among technology companies, fashion brands, and startups—deliver products and services and help shape customers' overall shopping experiences. Customers are now able to use innovative fashion tech products and digital services to engage with their favorite brands and retailers in ways that improve their quality of life. FIA values the security and trust of the consumers using fashion tech products and services, and we recommend that government and industry continue to work together to strengthen cybersecurity efforts. The Alliance has identified below key issues toward encouraging a collaborative approach that will advance cybersecurity efforts while also furthering American innovation.

**Internet of Things.** The federal government should take a public-private collaborative approach in supporting efforts to increase the security of IoT networks and interoperability, while taking into account global innovation, industry standards, and best practices.

**Innovative and Inclusive Cybersecurity Workforce for Government and Industry.** Cyber talent is key to ensuring that both the public and private sectors are not only able to advance effective cybersecurity practices, but also make adjustments as technologies and cyber challenges evolve. FIA recommends that the public and private sectors continue to work together to build an innovative and inclusive cybersecurity workforce through educational and training programs.

**The Role of Government in Enhancing Cybersecurity for the Private Sector.** The public and private sectors should continue to collaborate and work together, building upon the progress of the NIST Cybersecurity Framework and other programs. FIA recommends that before implementing new rules or regulations, the government should collaborate with the innovators developing these technologies in working to address cyber challenges.

**Cybersecurity Resources for Startups.** The Alliance recommends that the government expand upon its efforts to provide cybersecurity training and business resources for the growing startups and entrepreneurs designing fashion tech products and services. The Alliance welcomes NIST's SMB Outreach program and the Federal Trade Commission's (FTC) *Start with Security* initiative offering guidance for business.

## DISCUSSION

### Internet of Things (IoT)

Many fashion tech products are connected devices that fall within the category of Internet of Things: smart apparel and accessories are connected to sensors detecting heart rate, breathing, and other body functions; rings and bracelets are able to link text messages and consumer data directly to users' smartphones and apps. These products are generating significant interest among consumers—not only for their ability to track lifestyle activities and ensure connectivity to consumers' smart devices—but also for their sophisticated aesthetics and design. Thus, we must continue to advance cybersecurity best practices to keep consumer data safe and secure, while building consumer trust and confidence.

As creative entrepreneurs in fashion tech continue to design new smart accessories and apparel, FIA believes that the federal government should continue with voluntary public-private partnership efforts established through the NIST Cybersecurity Framework released in February 2014.[4] The Framework's flexible approach is suitable for both enterprise technology companies entering into the wearable tech arena as well as startups building security into their first connected ring or bracelet.

The Fashion Innovation Alliance also recommends that the federal government take a public-private collaborative approach in supporting efforts to increase the security of IoT networks and interoperability, while taking into account global innovation and current standards and best practices. IoT cybersecurity standards and best practices must include strategies to secure data in transit and storage, as well as effective solutions to reduce the amount of time in addressing vulnerabilities through patches and other measures.

### Innovative and Inclusive Cybersecurity Workforce

Cyber talent is key to ensuring that both the public and private sectors are able to implement effective cybersecurity practices, especially as the technologies and cyber challenges continue to evolve and change. Expanding the cybersecurity workforce has been an ongoing issue in policy discussions for a number of years.[5]

The current challenges for a robust and inclusive cybersecurity workforce are clear. Women represent 10% of the cybersecurity workforce, and according to the *(ISC)$^2$ 2015 Women in Security Study*, the percentage remained unchanged from 2013-2015.[6] Also, it is estimated that an additional 1.5 million cybersecurity professionals will be needed by 2020 to accommodate the

[4] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), February 12, 2014, *available at* https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[5] Cybersecurity Workforce Assessment Act, Pub. L. No. 113-246 (2014); see also S. 3414, 112th Cong. (2012).

[6] (ISC)$^2$ 2015 Women in Security Study, *available at* https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/2015-Women-In-Security-Study.pdf.

projected workforce shortfall of cyber talent.[7] NIST pointed out in its informational video on the Cybersecurity Framework that we will need additional cybersecurity talent.[8]

The National Cybersecurity Workforce Framework—launched by the National Initiative for Cybersecurity Education (NICE)—provides a useful guide for educating, training, and retaining a top cybersecurity workforce.[9] FIA recommends that the public and private sectors continue to collaborate on ways to build an effective and robust cybersecurity workforce and further expand upon related guidance in the NIST Cybersecurity Framework. Public-private partnerships must also invest in programs to help recognize and advance cybersecurity talent from all backgrounds.

For example, startups and fashion brands integrating tech into their platforms have used fashion as a way to get more young girls interested in technology, and thus helping to increase the pipeline of women in science, technology, engineering, and math (STEM) fields. Fashion tech companies rely on information security professionals to help keep customer data transmitted via smart accessories and apparel safe and secure. Thus, building an innovative and inclusive cybersecurity workforce will be key in protecting such data against cyber intrusions and privacy compromises.

**The Role of Government in Enhancing Cybersecurity for the Private Sector**

The public and private sectors should continue to collaborate and work together, building upon the work that government and industry have accomplished through the NIST Cybersecurity Framework and other programs. FIA also recommends that before implementing new rules or regulations, the government should collaborate with the innovators developing the technologies working to address cyber challenges.

Also, given the global reach of digital products and services, FIA welcomes NIST's current outreach efforts to multi-national organizations and foreign governments.[10] FIA recommends that the federal government evaluate guidance and policy documents developed by international organizations before regulating in this area. For example, the EU's Alliance for Internet of Things Innovation (AIOTI) released a policy report in October 2015, which references NIST's Cyber Physical Systems Public Working Group. The report includes a detailed section on security, noting the interdependencies of security with privacy, resiliency, and other domains while also providing policy recommendations and references to the European Union Agency for Network and Information Security, the UK Government Cyber Essentials Scheme, and other

[7] (ISC)$^2$ 2015 Global Information Security Workforce Study, *available at* https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)²-Global-Information-Security-Workforce-Study-2015.pdf.

[8] The Cybersecurity Framework Video, U.S. Department of Commerce, NIST, May 23, 2016, *available at* https://www.nist.gov/video/cybersecurity-framework.

[9] The National Cybersecurity Workforce Framework, *available at* http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf.

[10] Cybersecurity Framework Feedback: What We Heard and Next Steps, National Institute of Standards and Technology (NIST), June 9, 2016, *available at* https://www.nist.gov/sites/default/files/workshop-summary-2016.pdf.

committees and organizations.

**Cybersecurity Resources for Startups**

The Alliance recommends that the government expand upon its efforts to provide cybersecurity training and business resources for the growing startups and entrepreneurs designing innovative fashion tech products and services. The Federal Trade Commission's (FTC) *Start with Security* initiative's guidance for business and NIST's SMB outreach efforts have served as useful resources for startups building security into their products and services.

FTC staff recently released guidance on how NIST's Cybersecurity Framework relates to the Commission's data security program.[11] As NIST, the National Telecommunications and Information Administration, the Department of Homeland Security, the Justice Department and other federal entities continue to evaluate cybersecurity policies, the Alliance recommends that the agencies coordinate and provide resources and tools on how the various agency documents relate to one another. Additional guidance will help to minimize confusion for startups and entrepreneurs, allowing more time to advance their innovations.

**Conclusion**

The Fashion Innovation Alliance appreciates the opportunity to submit these comments and would be happy to provide you with additional information or clarification. For the reasons stated above, the Alliance respectfully requests that the federal government collaborate and work with the private sector when considering the current and future states of cybersecurity in the digital economy. Any new policies governing cybersecurity for e-commerce and mobile or Internet-connected accessories/apparel should consider the broader impact of the digital economy as a whole without limiting the innovation powering fashion tech.

Respectfully submitted,

Kenya N. Wiley
Founder and CEO
Fashion Innovation Alliance

[11] FTC Blog Post Outlines How NIST Cybersecurity Framework Relates to FTC Data Security Program, Federal Trade Commission, August 31, 2016, *available at* https://www.ftc.gov/news-events/press-releases/2016/08/ftc-blog-post-outlines-how-nist-cybersecurity-framework-relates.