FDRA
FOOTWEAR DISTRIBUTORS AND RETAILERS OF AMERICA

April 19, 2022

Mr. Seth D. Renkema
Branch Chief, Economic Impact Analysis Branch
U.S. Customs and Border Protection
Washington, D.C. 20229

Re: ***Notice Seeking Public Comments on the Customs-Trade Partnership Against Terrorism (CTPAT) Program and CTPAT Trade Compliance Program***

Dear Mr. Renkema:

On behalf of the Footwear Distributors & Retailers of America (FDRA), we write to provide comments on proposed changes to the information collected under the Customs-Trade Partnership Against Terrorism (CTPAT) Program and CTPAT Trade Compliance Program.

FDRA is the footwear industry's trade and business association, representing more than 500 footwear companies and brands across the U.S. This includes the majority of U.S. footwear manufacturers and over 95 percent of the industry. FDRA has served the footwear industry for more than 75 years, and our members include a broad and diverse cross section of the companies that make and sell shoes, from small family-owned businesses to global brands that reach consumers around the world.

U.S. Customs & Border Protection (CBP) collects certain information to identify whether participating CTPAT companies, or those applying to participate in the programs, are at a "high risk for committing illegal activity." CBP has proposed a significant expansion to its current data collection – to include the sensitive personal data *of the individual point of contact* for each CTPAT company and applicant. This will include the point of contact's date of birth, country of birth, country of citizenship, visa or passport number, immigration status information, driver's license information, Social Security number, Trusted Traveler membership type and number, and IP address. FDRA objects to the proposed collection of individual data for several reasons:

- CBP does not adequately explain how collecting sensitive personal data about an *individual point of contact* will assist CBP in vetting businesses that seek to participate in CTPAT programs. CTPAT programs are designed for companies, not individuals who serve as points of contact. The corporate point of contact is frequently a member of the compliance or logistics departments, and his or her background is immaterial to the company's risk profile. CBP does not offer sufficient explanation as to how the data will limit risk. Further, it does not address how obtaining personal information on the point of contact will help assess risks for multinational corporations with operations that span the globe. If more data is needed, it should be data about the company, not a specific person at the company.

Matt Priest, President & CEO
1319 F Street, NW, Suite 700, Washington, DC 20004 • (p) 202.737.5660 • (f) 202.638.2615 • mpriest@fdra.org • www.fdra.org

- The personal data that CBP will require is highly sensitive information. Its release could lead to significant data and privacy breaches including identity theft. CTPAT information is posted on the CTPAT portal. CBP does not explain how it will protect sensitive data like Social Security and driver's license numbers from unauthorized disclosure, data breaches, or Freedom of Information Act (FOIA) requests.

- CTPAT participants cannot compel an employee acting as the point of contact to release the proposed information. It is not reasonable for CBP to reject an otherwise qualified CTPAT participant because the company cannot identify an employee that is willing to provide his or her sensitive personal identifying information (without any guarantee that it will be safeguarded).

Thank you for the opportunity to provide input on this critical issue. Please feel free to contact me if you have any questions.

Sincerely,

Matt Priest
President & CEO
Footwear Distributors and Retailers of America