Josiah Dykstra, Ph.D.
Trail of Bits
12228 Mount Albert Road
Ellicott City, MD 21042

March 3, 2025

Re: **Nomination Statement for Best Scientific Cybersecurity Paper Competition 2025**

To Whom It May Concern:

It is an honor to nominate the paper "INAUGURAL WORKSHOP ON CYBER PUBLIC HEALTH" for its groundbreaking contribution to cybersecurity science by systematically developing a public health framework for understanding and measuring cybersecurity at a population scale. As a former NSA Senior Executive and author of the book *Essential Cybersecurity Science*, it is clear to me that this paper exemplifies scientific merit, significance, and how to perform and report scientific research in cybersecurity.

This paper makes several critical scientific contributions:

- It establishes a rigorous foundation for applying proven epidemiological and public health methodologies to cybersecurity. Rather than simply drawing superficial analogies, the authors carefully analyze how public health concepts like prevalence, incidence, and population-level measurements can be meaningfully adapted to cyber contexts to describe systems' security properties and behaviors quantifiably.
- It demonstrates exceptional scientific rigor in identifying and defining precise terminology and atomic units of measurement (devices, accounts, users) and their relationships, creating a taxonomy that enables quantitative analysis. It proposes concrete data collection and analysis methods that will likely be adopted and extended.
- The paper's approach to "Digital Activities of Daily Living" demonstrates how to operationalize abstract concepts into measurable units, a crucial aspect of scientific cybersecurity research. The authors' careful consideration of measurement challenges, from defining "cyber vital statistics" to addressing privacy concerns in data collection, provides a model for rigorous scientific thinking in cybersecurity.
- The work opens new avenues for evidence-based cybersecurity research. It contributes to a general framework for principled design and adopts an entire, proven framework for principled population health improvement. The authors provide objective techniques to compare the proposed solution to other approaches, avoiding a common trap in cybersecurity science. By establishing frameworks for measuring population-level cyber health indicators, it enables future research to quantify the effectiveness of security interventions, study the spread and impact of cyber threats across populations, develop predictive models for cyber risk, and make data-driven policy recommendations.

- The paper exemplifies bridging theoretical frameworks with practical measurement and application. Its systematic approach to defining research questions, measurement units, and methodological challenges provides a template for future scientific work in the field. The work has already attracted the attention and support of Google.[1]

This groundbreaking work deserves recognition for establishing a scientific foundation for measuring and improving cybersecurity at scale, demonstrating exemplary research methodology, and creating frameworks enabling more rigorous, quantitative cybersecurity research.

Sincerely,

Josiah Dykstra, Ph.D.

[1] https://cloud.google.com/blog/products/identity-security/cyber-public-health-a-new-approach-to-cybersecurity