TOWSON UNIVERSITY

Dr. Natalie M. Scala
College of Business and Economics
8000 York Road
Towson, MD 21252

EMPOWERING SECURE ELECTIONS

Chairwoman Klobuchar and Ranking Member Fischer:

I greatly appreciate your decision to hold this hearing on *Ongoing Threats to Election Administration* on November 1, 2023. The security of polling locations and ensuring access to the ballot are critical for our democracy and providing Americans with confidence in our elections.

My name is Dr. Natalie M. Scala, and I am an Associate Professor and Director of the Graduate Programs in Supply Chain Management in the College of Business and Economics at Towson University in Maryland. I am also a Faculty Affiliate Associate Research Scientist at the University of Maryland's Applied Research Lab for Intelligence and Security. I am a member of INFORMS, the largest professional association for the data and decision sciences. My areas of expertise include election security, cybersecurity, and decision modeling – all of which benefit significantly from research and applications within analytics.

I co-direct the Empowering Secure Elections (ESE) research lab at Towson University, which is committed to non-partisan academic research that increases the security of U.S. elections and ensures the integrity of votes from the moment they are cast to the moment they are counted. The lab's mission is to develop risk assessments for U.S. elections and actionable countermeasures to reduce threat. Recently, the lab published groundbreaking work on risk assessments for mail voting[1] that concludes that expanded mail voting disincentivizes adversarial interference and increases voting access, which are significant implications for the security and accessibility of election processes. The lab also created cyber, physical, and insider threat training for poll workers[2] that was recognized by the U.S. Election Assistance Commission with a Clearinghouse Award in 2020 for Outstanding Innovation in Election Cybersecurity and Technology.

The ESE research lab is the first academic team to define threats to elections as systemic – encompassing cyber, physical, and insider risks – and one of the few research teams to focus efforts on polling places and the public's experience with voting[3,4]. Poll workers are the first line of defense in election security, and our work enables poll workers to take an active role in keeping elections safe. We specifically study human behavior – one of the National Security Agency's Five Hard Problems of Cybersecurity – considering interactions between humans and cyber systems which necessitate development of models of user and adversarial behavior[5]. Human behavior can compromise security measures built into systems. This behavior may be unintentional, in which an individual inadvertently misuses a system, yet still creates a vulnerability, or it may be deliberate, in which an individual interacts with a system with the intention of causing harm. Poll workers and elections officials are trusted

410.704.2773
nscala@towson.edu
www.drnataliescala.com

insiders to the election process, and the lab's work creates an understanding of their security behaviors to better assess risk.

The ESE lab's current work focuses on risk assessments for in-person voting, belief in mis/dis-information, countermeasures for threats, and emerging technologies in voting. Misinformation and disinformation are quickly becoming the fourth systemic threat to elections, as the spread of accidental or deliberate incorrect information can leave voters confused about safety and security of voting methods and erode confidence in the legitimacy of election systems and processes. In work to be presented at the 17th NATO Operations Research and Analysis Conference in October 2023, we argue, supported by data and evidence, that election misinformation is an attack on critical infrastructure; clear plans and mitigations are needed to combat this issue. There must be a concerted effort to depoliticize election systems and processes.

Within this context, I propose the following questions for the committee to consider and potentially pose at the hearing:

1. Given the role that poll workers have as the first line of defense in elections, what cyber, physical, and insider threat training and enhancements are being implemented across the country in preparation for the 2024 Elections?
2. As intentional or unintentional human behavior can compromise security measures in election systems, what mitigations and countermeasures are being implemented to prevent issues on and related to Election Day?
3. As election mis/dis-information is an attack on critical infrastructure, what steps are being taken to assure voters of the safety and security of voting methods? How will states and localities provide true and complete voting information to their citizens?
4. As mail voting was used in record numbers during 2020 and has been shown to increase voter access and disincentivize adversarial interference, what is being done to ensure states continue to support access to mail voting in 2024?

I appreciate the opportunity to provide some insight into the important analytical work the ESE research lab is doing. Please consider me a resource as you continue to focus on this important issue.

Sincerely,

Dr. Natalie M. Scala

References:

[1]Scala, N. M., Goethals, P. L., Dehlinger, J., Mezgebe, Y., Jilcha, B., & Bloomquist, I. (2022). Evaluating mail-based security for electoral processes using attack trees. *Risk Analysis, 42*, 2327-2343.

[2]Scala, N. M., Black, L., & Dehlinger, J. (2023). Preparing poll workers to secure U.S. elections. *Proceedings of the American Society for Engineering Management 2023 International Annual Conference*.

[3]Price, M., Scala, N. M., and Goethals, P. L. (2019). Protecting Maryland's voting processes. *Baltimore Business Review: A Maryland Journal*, 36-39.

[4]Locraft, H., Gajendiran, P., Price, M., Scala, N. M., & Goethals, P. L. (2019). Sources of risk in elections security. *Proceedings of the IIE Annual Conference* (pp. 1572-1577).

[5]Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the Five Hard Problems of Cybersecurity. *Risk Analysis, 39*(10), 2119 - 2126.