Statement for the Record

Natalie M. Scala
Associate Professor, Towson University

Chairperson Lofgren and Ranking Member Davis:

I greatly appreciate your decision to hold today's hearing on *Voting in America: The Potential for Polling Place Quality and Restrictions on Opportunities to Vote to Interfere with Free and Fair Access to the Ballot.* 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 member of INFORMS, which is the leading association for professionals in operations research, analytics, management science, economics, behavioral science, statistics, artificial intelligence, data science, applied mathematics, and other relevant fields. My areas of expertise include decision modeling, cyber security, and elections security – all of which benefit significantly from research and applications within analytics.

My research uses decision analysis and operations research to evaluate the security of voting systems. I lead the first academic team that defined threats to elections systemically – as an interaction between cyber, physical, and insider threats – and we focus on maintaining the integrity of votes. My research in elections security has two main themes: (1) evaluating threats and risk in mail voting, and (2) reducing insider (human) threats at polling places. Like all of you, we want votes to be counted as they are cast by the electorate, with no alteration, interference, or loss.

Key findings and outcomes from my research include:

- The United States needs a mix of expanded mail voting with broad accessibility of in-person voting locations and hours, providing multiple ways for Americans to access ballots and vote.
- Expanded mail voting is not attractive for an external adversary to attack and also increases voter access.
- Polling place security can be increased by training poll workers to identify and mitigate potential threats, helping to ensure the integrity of votes cast.
- Confidence in the electoral process can lead to increased voter turnout. Confidence in the process is also key to free and fair elections, with the outcome of those elections being supported and accepted by the American people.

These outcomes are supported by my published academic papers.[1][2][3][4][5] Descriptions of those papers can be found on my website: www.drnataliescala.com/projects with discussion found at: www.drnataliescala.com/elections-media.

I am proud to have been recognized by the U.S. Elections Assistance Commission (in partnership with Anne Arundel County, Maryland), the University System of Maryland Board of Regents, and others for the work I have done around election security, including research that has been applied to improving security at polling places and the creation of training models for poll workers to identify and mitigate election security vulnerabilities.

Voting Access Increases Elections Security

As the COVID-19 pandemic and high turnout in the 2020 General Election recently proved, Americans were seeking safe, socially distant methods of voting, and we need access in place to continue to support those needs. We saw, for example, that 40% of states had a process change during the 2020 primary (to accommodate COVID-19) and 47 states continued with expanded mail voting for the General Election.[6]

Expanded mail voting – defined as the wide use and placement of drop boxes, extended Early Voting time, and no-cost methods for the voter to request and return ballots – along with accessible in-person voting adds complexity to the system, which impedes adversaries. Those seeking to harm our election would have to attack numerous drop boxes and thousands of mailboxes in order to infiltrate or alter the vote in an impactful manner. If the adversary would attempt to attack a single drop box, for example, their attack would have less impact because only a few votes would be housed in that location. This is in contrast to an attack on a central server where all electronic votes cast in an election may be recorded and stored; a successful attack in that case would be devastating.

Our analysis of the 2016 election supports this conclusion. We examined the 21 states that the Department of Homeland Security (DHS) revealed were targeted during the 2016 election.[57] More states that had a standard process or the same equipment across the state were targeted than states that had multiple forms of voting equipment and/or a more complicated process. This is because once a standard system is breached, the attack can spread quickly through all like devices. However, each unique type of equipment in a non-standardized system would have to be independently breached in order to have full access to the system. This is much harder for an adversary to execute. Furthermore, more frequent or numerous attacks increases the chance the adversary would be caught or noticed by elections and information assurance officials. Therefore, continued use of expanded mail voting can help to discourage external adversarial attack, help to ensure the integrity of votes, and help to increase voter access.

Expanded Mail Voting Does Not Make Elections Less Secure

Our most recent research on mail voting[6] (currently under peer review) revises the U.S. Elections Assistance Commission's (EAC) attack tree for mail voting, which was originally defined in 2009.[8] An attack tree is an inventory of threats. Note that we have no evidence that the threats on the attack tree have ever been comprised, but the tree enumerates what could go wrong. My research's revision to the tree considers implications of the COVID-19 pandemic to elections security, threats to elections infrastructure as U.S. critical infrastructure, and the adaptive adversary. Examples of the 30 new threats that are incorporated in the revision include acquiring access to or destroying drop boxes, manipulation of return envelopes, ballot return misinformation, and breaking into a post office. We then enhanced the attack tree by becoming the first to analytically evaluate strength or relative likelihood of threat. From that analysis, we generally conclude the least likely threat scenarios are those that have high adversarial cost, are difficult for the adversary to pursue, and easy for us to discover if attacked.

Our attack tree or inventory of threats only identifies 10 scenarios (out of 73 total ways to attack mail voting, or 13.7%) that are attributable to voter error or fraud. A vast majority of threats to mail voting are from trusted insiders to the system. External actors can also have influence but, for reasons outlined above, are not incentivized to act. Mitigations have been in place to catch voter error or fraud, and those checks worked in 2020. An example includes the Forty Fort, Pennsylvania, resident accused of casting a ballot for his deceased mother; only three instances of voter fraud in total occurred in Pennsylvania in 2020.[9] Generally speaking, voter error threats have low relative likelihood with high likelihood of being

discovered; this means elections officials are very likely to find out about any fraud that may occur, while research models do not suggest that fraud would even occur on a large scale to begin with.

Expanded Mail Voting Means Expanded Access for Americans

Expanded mail voting enables more Americans to vote, as it provides safe, socially distant, and convenient access to ballots. It also makes it easier for Americans to vote, especially when drop boxes and postage-paid envelopes are used in the process. Expanded mail voting does not make the integrity of votes less secure, as my research has shown the quick scale up of mail voting during the 2020 primaries and General Election did not introduce new threats of high concern; our analysis of threat identified that the most concerning threats to mail voting were already known before the pandemic and likely had mitigations in place in many counties and states before the previous election.[6] Therefore, mail voting can continue in future elections at the scale utilized in 2020 to increase voter access and also disincentivize the adversary to attack the system. This double reward of increased access with less adversarial interest is of true value to free and fair elections in the United States.

Increasing Polling Place Security Through Poll Worker Training

I appreciate this hearing's focus on polling places, as polling places have not been broadly addressed in the academic discourse on elections security, were a second thought during COVID-19, but are still integral to a voting process with broad access. In addition to our work in mail voting, my team created U.S. EAC award winning training for poll workers to identify and mitigate potential cyber, physical, and insider threats that may occur at a polling place on Election Day. Training poll workers to be aware of and identify threats that may emerge at a polling place and then teaching them how to fix or mitigate those concerns is essential to the integrity of votes. Poll workers are our first line of defense in elections security. They must be empowered to take an active role in security, as America cannot risk an unchecked or undiscovered attack on Election Day. We worked closely with Anne Arundel and Harford Counties in Maryland to design and implement the training; previously, poll workers in Maryland were only receiving equipment training and no information about threats. A working academic study regarding the efficacy of the training shows that cyber, physical, and insider threat knowledge of poll workers and potential poll workers increased with statistical significance after interacting with the training, meaning they actually learned and retained threat knowledge.[10] The training was implemented in Anne Arundel County, Maryland, in 2020 with over 1,900 poll workers[11] who served over 400,000 eligible voters[12].

In summary, I appreciate the opportunity to provide some insight into the important analytical work we are doing in the election security. I look forward to working with the committee and your staff on issues related to election security going forward. Thank you for your time and attention to these important matters.

---

[1] Scala, N.M., Bloomquist, I., Mezgebe, Y., Jilcha, B., Goethals, P.L., and Dehlinger, J. (2021). A process map and risk assessment for mail-based voting. *Proceedings of the 2021 IISE Annual Conference.*

[2] Dehlinger, J., Harrison, S., and Scala, N.M. (2021). Poll worker security: Assessment and design of usability and performance. *Proceedings of the 2021 IISE Annual Conference.*

[3] Scala, N.M., Dehlinger, J., Black, L., Harrison, S., Delgado Licona, K., and Ieromonahos, K. (2020). Empowering election judges to secure our elections. *Baltimore Business Review,* p. 8-12.

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

[5] Locraft, H., Gajendiran, P., Price, M., Scala, N.M., and Goethals, P.L. (2019). Sources of risk in elections security. *Proceedings of the 2019 IISE Annual Conference.*

[6] Scala, N.M., Goethals, P.L., Dehlinger, J., Mezgebe, Y., Jilcha, B., and Bloomquist, I. (2021). Evaluating mail-based security for electoral processes using attack trees. Under review.

[7] Horwitz, S., Nakashima, E., and Gold, M. (2017). DHS tells states about Russian hacking in 2016 election. *The Washington Post.* https://tinyurl.com/HorwitzEtAl

[8] United States Election Assistance Commission Advisory Board and United States Election Assistance Commission Standards Board. (2009). Election operations assessment: Threat trees and matrices and threat instance risk analyzer (TIRA). https://www.eac.gov/assets/1/28/Election_Operations_Assessment_Threat_Trees_and_Matrices_and_Threat_Instance_Risk_Analyzer_(TIRA).pdf

[9] Marroni, S. (2020, December 30). Pa. Lt. Gov. John Fetterman pesters Texas counterpart to pay $3 million for voter fraud cases. *Penn Live Patriot-News.* https://www.pennlive.com/news/2020/12/pa-lt-gov-takes-to-twitter-asking-texas-counterpart-to-pay-3-million-for-the-states-3-voter-fraud-cases.html

[10] Scala, N.M., Dehlinger, J., and Black, L. (2021). Preparing poll workers to secure U.S. elections. Working paper.

[11] DeVille, T. (2020, October 16). Towson University professor aims to bolster local election security at voting sites. *The Baltimore Sun.* https://tinyurl.com/y5mpf5z

[12] Anne Arundel County Maryland. (2020). Voter registration statistics. https://www.aacounty.org/boards-and-commissions/board-of-elections/voter-registration-statistics/