TOWSON UNIVERSITY

Quantitative Threat Modeling and Risk Assessment in Socio-Technical Critical Infrastructure Systems

Dr. Natalie M. Scala (PI) and Dr. Josh Dehlinger

SoS Virtual Institute (VI) Kick-off Meeting

January 2024

EMPOWERING SECURE ELECTIONS

Motivation

- 16 critical infrastructure sectors, as defined by DHS
- Assets, systems, networks – physical or virtual
- Problems lead to significant impacts to national security, economic security, public health and safety, etc.
- Key target for cyber attacks
- Study and model systems within the sectors
  - Identify vulnerabilities
  - Develop strategies
  - Intent to prevent and respond to attacks, helping to safeguard infrastructure

Goals

EMPOWERING SECURE ELECTIONS

Considering national critical infrastructure sociotechnical systems and processes:

1. Develop and disseminate a systematic threat and mitigation analysis approach
    - Address cyber, physical, and insider risks
    - Adversaries and trusted insiders

2. Create a framework to model a relative likelihood risk assessment
    - Include actions of adversaries and trusted insiders as contributors to cyber, physical, and insider threat scenarios

3. Develop, model, and analyze policy implications and security mitigations
    - Quantify ability to reduce cyber, physical, and insider risks

How Are We Going To Do This?

- Government Facilities sector
  - Subsector: Election Infrastructure
- Case study / test bed

- Security and integrity of elections are in forefront of national discourse
  - Russian Federation interference in 2016
  - Senate Intelligence Committee (2019): Election systems in all 50 states targeted in 2016
  - Robert S. Mueller, III (2019): Interference ongoing
  - Director of National Intelligence (2020): Iran and Russia obtained US voter registration information

Empowering Secure Elections

- Research lab at Towson University
- First to define threats to elections as a systemic interplay
  - Cyber, physical, and insider risks
- Risk analysis of mail voting
  - Expanded mail voting disincentivizes adversarial interference and increases voting access
- Poll worker training
  - Increase security and integrity of critical elections infrastructure
- U.S. Election Assistance Commission: Clearinghouse Award for Outstanding Innovation in Election Cybersecurity and Technology
- University of Maryland Board of Regents Award for Excellence in Public Service

Problem Statement

- Model the relative risks of adversaries and trusted insiders exploiting threat scenarios in developed attack trees, using critical infrastructure precinct count optical scanner (PCOS) in-person voting machines as a case study.

- PCOS
  - Auditable paper trail
  - Will be used in almost 70% of the country in 2024 (Verified Voting)

Outcomes and Objectives

EMPOWERING SECURE ELECTIONS

	Year 1	Year 2	Year 3
1. A comprehensive, updated attack tree and mitigation analysis for critical infrastructure equipment and processes	√		
2. A scenario analysis to categorize threat scenarios as cyber, physical, or insider with an adversarial or insider source	√		
3. A risk assessment of threat scenarios on the updated attack tree that considers insider / adversarial attack costs and technical difficulties as well as information assurance assessments of the difficulties to discover an attack	√	√	
4. The identification of risks of most concern within the process across temporal phases		√	

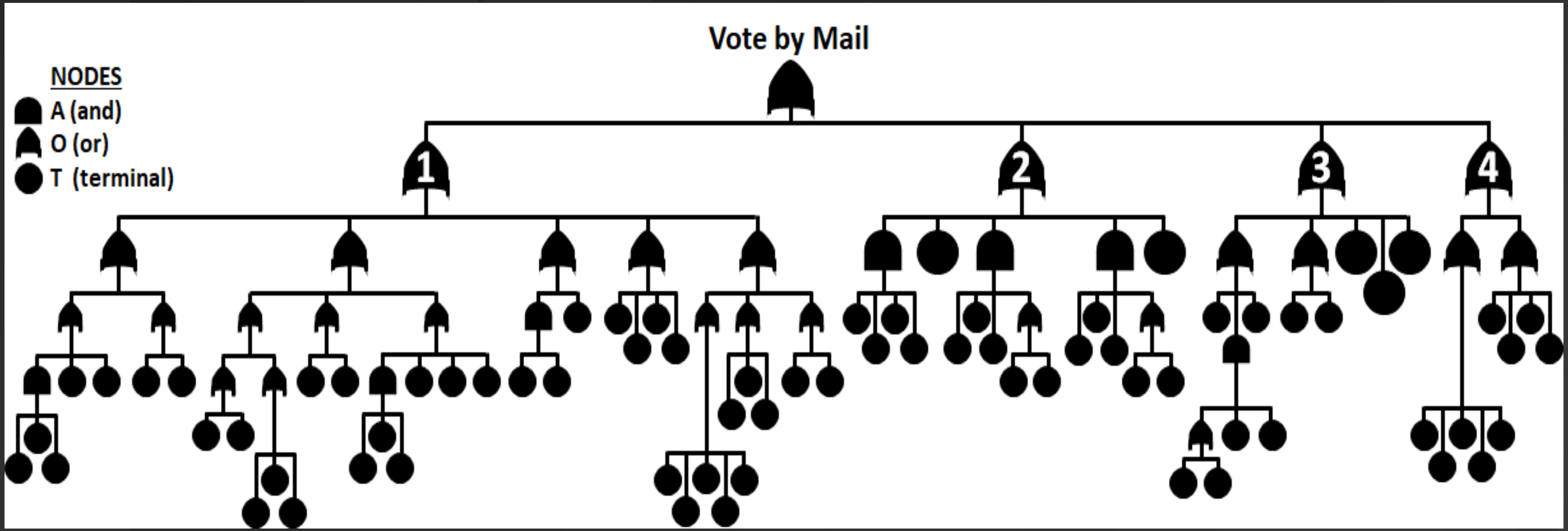
Outcomes and Objectives

	Year 1	Year 2	Year 3
5. An impact analysis of suggested policy implications and security mitigations (e.g., adversarial implications, human behavior interdictions) and their ability to reduce cyber, physical, and insider risks			√
6. The dissemination of the threat and mitigation analyses results		√	√
7. An assessment of the systematic threat and mitigation analysis approach's utility for use in national critical infrastructure socio-technical systems and processes, and recommendations for the adoption of the approach at the national level		√	√

1. Attack Tree + Mitigation Analysis

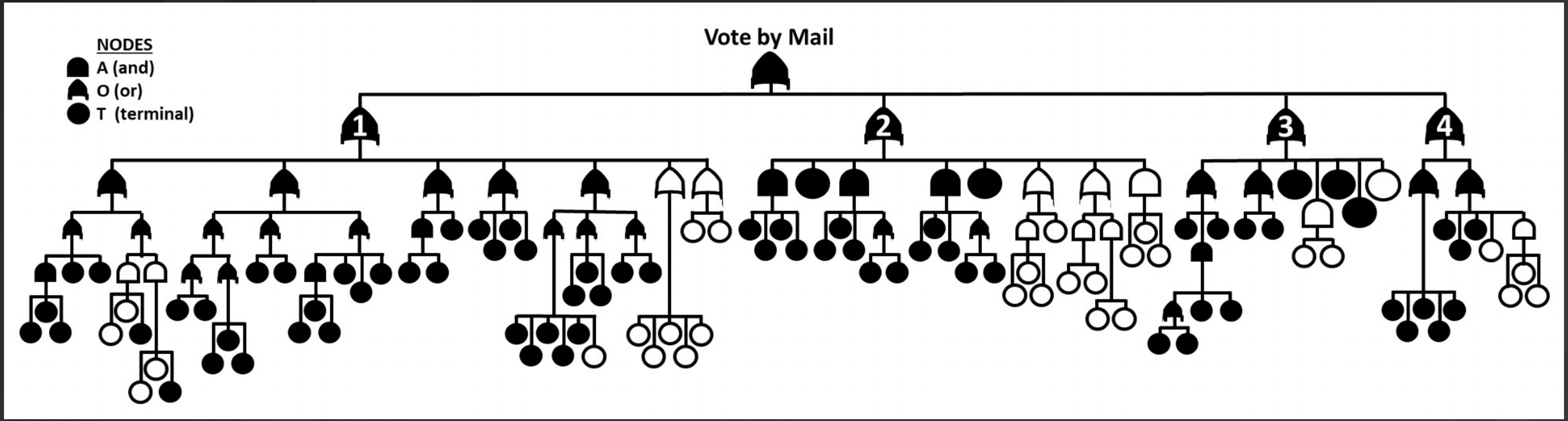
- Elections Assistance Commission (2009) attack tree data
- Attack tree: Inventory of risks
  - Does not identify strength or likelihood
- Decompose complex actions into hierarchical levels
- Graphic representation of security problem
- Much has changed
  - Critical infrastructure designation
  - COVID-19
  - Adaptive adversary

Example: Mail Voting



- EAC (2009) tree
- Threat scenarios
  - Insider = 32
  - External = 16
  - Voter error = 9
  - Total = 57

Example: Updated Attack Tree



- 30 new threats
- Threat scenarios
    - Insider = 40
    - External = 23
    - Voter error = 10

How is PCOS different?

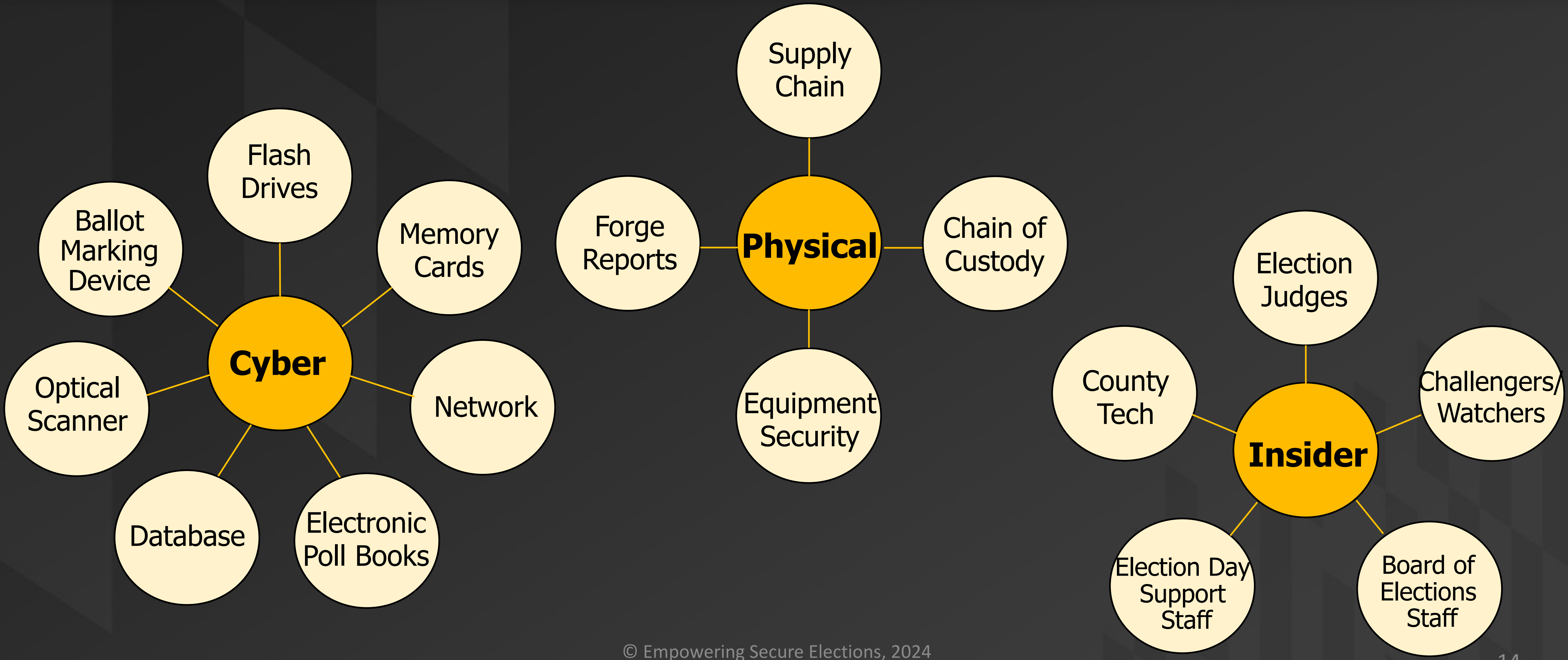
- Much larger problem space
- 7 branches
- 1000+ threats
- Three phases: Set up, voting, tear down

- Broader sense of critical infrastructure
  - Systematic approach to building and revising trees
- How do we validate a complete tree?
  - Failure Modes and Effects Analysis

2. Cyber, Physical, Insider

- Each threat and systemic interplay
- Framing extends beyond elections
- Cyber
  - Digital machines and media
  - Regardless of Internet connection
- Physical
  - Tampering with or disrupting equipment
- Insider
  - Adversaries and insiders
  - Simple, honest mistakes
  - Deliberate actions with ill-harm effects

Sources of Threat



3. Risk Assessment

EMPOWERING SECURE ELECTIONS

- Relative strength or likelihood of threat
- Each terminal node assessed for utility on three dimensions
  - Attack cost (AC) u_1
  - Technical difficulty (TD) u_2
  - Discovering difficulty (DD) u_3
- Criteria adapted from Du and Zhu (2013)

Attack Cost (AC)		Technical Difficulty (TD)		Discovering Difficulty (DD)	
Grade	**Standard**	**Grade**	**Standard**	**Grade**	**Standard**
5	Severe consequences likely	5	Extremely difficult	1	Extremely difficult
4	High consequences likely	4	Difficult	2	Difficult
3	Moderate consequences likely	3	Moderate	3	Moderate
2	Mild consequences likely	2	Simple	4	Simple
1	Little to no consequences likely	1	Very simple	5	Very simple

Calculating Relative Likelihood

- Relative likelihood for each terminal node X_j:

$$P(X_j) = w_1 u_{1j} + w_2 u_{2j} + w_3 u_{3j}$$

  - $j \in \{1, 2, \dots, n\}$, n terminal nodes
  - $w_k, k \in \{1, 2, 3\}$, weight assigned to utility function k; $\sum w_k = 1$
    - $w_k = {}^1/_3 \,\forall k$
  - $u \in [0, 1]$, using scale factor (0.2) to convert ordinal scales

Our Team: PI

- Dr. Natalie M. Scala
  Associate Professor
  Department of Business Analytics and Technology Management
- Director, Graduate Program in Supply Chain Management
- Faculty Affiliate: University of Maryland Applied Research Lab for Intelligence and Security
- Research
  - Decision modeling, military applications, cybersecurity, election security

Our Team: Co-PI

EMPOWERING SECURE ELECTIONS

- Dr. Josh Dehlinger
  Professor
  Department of Computer and Information Sciences
- Director, Undergraduate Program in Computer Science
- Research
  - Software engineering, software safety/reliability, cybersecurity, election security

Our Team: Contingent Assistant

EMPOWERING SECURE ELECTIONS

- Vince Schiavone
- MS Supply Chain Management, Towson University
- Northrup Grumman: Operations Project Manager
- Research
  - Collaborative scheduling, project management, statistical analysis, data mining

Our Team

EMPOWERING SECURE ELECTIONS

- Graduate Research Assistant: Hao Nguyen
- MS Thesis Student: Skylar Gayhart
- Undergraduates: Vanessa Gregorio, Erich Newman, Yavor Gray
- University of Maryland Undergraduates: Noah Hibbler, Aaryan Patel
- Students working on adjacent projects: Amara Offor, Sadie Barrett

Questions?

Dr. Natalie M. Scala
Email: nscala@towson.edu
Web: www.drnataliescala.com

Dr. Josh Dehlinger
Email: jdehlinger@towson.edu

Our Papers

EMPOWERING SECURE ELECTIONS

- Scala, N. M., Goethals, P. L., Dehlinger, J., Mezgebe, Y., Jilcha, B., & Bloomquist, I. (2022). Evaluating mail-in security for electoral processes using attack trees. In *Risk Analysis.*
- Dehlinger, J., Harrison, S., & Scala, N. M. (2021). Pollworker security: Assessment and design of usability and performance. *Proceedings of the 2021 IISE Annual Conference.* https://tinyurl.com/hvwde2ep
- Locraft, H., Gajendiran, P., Price, M., Scala, N. M., & Goethals, P. L. (2019). Sources of risk in elections security. *Proceedings of the 2019 IISE Annual Conference.* https://tinyurl.com/LocraftEtAl2019
- Price, M., Scala, N. M., & Goethals, P. L. (2019). Protecting Maryland's voting processes. *Baltimore Business Review: A Maryland Journal*. https://www.cfasociety.org/baltimore/Documents/BBR_2019%20Final.pdf#page=38
- Scala, N. M., Dehlinger, J., Black, L., Harrison, S., Delgado Licona, K., & Ieromonahos, A. (2020). Empowering election judges to secure our elections*. Baltimore Business Review: A Maryland Journal,* 8-20.