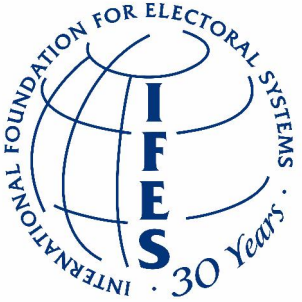
Cybersecurity in Elections

Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies

Dr. Beata Martin-Rozumilowicz
International Foundation for Electoral Systems



How can EMBs secure systems from technical vulnerabilities that leave them exposed and may lead to post-election challenges, while at the same time protecting principles of open data and transparency?

Iterative Process

Cyber threats have become an increasing concern since at least the mid-2000s. Main attacks in Europe include:

Estonia 2007: DDoS attack nearly shut down Internet infrastructure

Georgia 2008: cyber attacks in concert with traditional military operations; 11 websites knocked offline prior to Russian invasion

Lithuania 2008: 300 websites vandalized/DoS attack following law prohibiting SU symbols; linked to computers outside the country

Kyrgyzstan 2009: hackers take Kyrgyzstan offline after 10-day DDoS cyber assault, effectively eliminating 80% of the country's online capacity. Analysts felt that this was a ‘weapons test’

Ukraine 2014: 3-pronged wave of cyber-attacks in presidential vote. CEC website hacked in parliamentary elections. Moscow reports hacked win

Cybersecurity in Elections

- Cybersecurity should be considered and implemented at the inception phase of building or upgrading any technology-based election system.
- At the same time, EMBs must act transparently and ensure election results are verifiable. Therefore, it is important to protect both cybersecurity and transparency in the electoral context – a challenge that is particularly unique to EMBs.

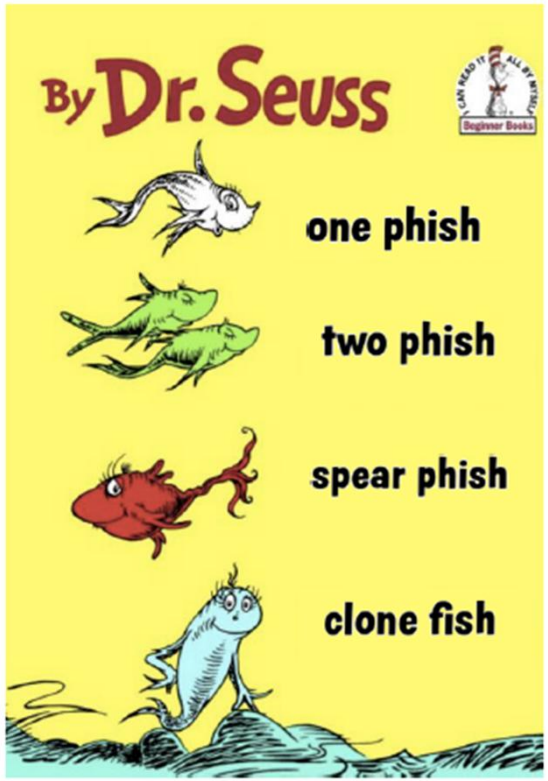
Cybersecurity in Elections

- Election administrators must focus on cybersecurity as an ongoing and ever-changing concern.
- While it is important to learn from experience, rapid technological innovation means that EMBs should endeavor to secure the next election, not focus on vulnerabilities in the last election.

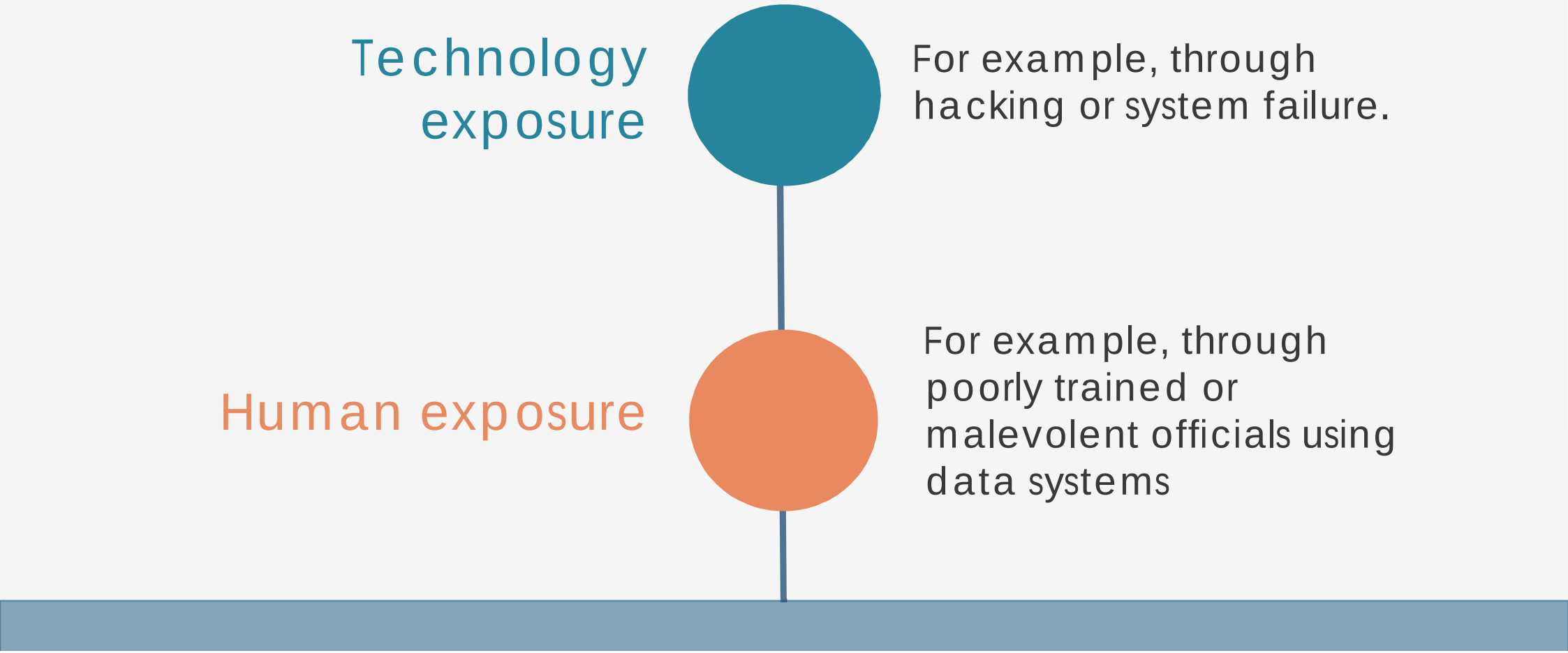
Cybersecurity in Elections

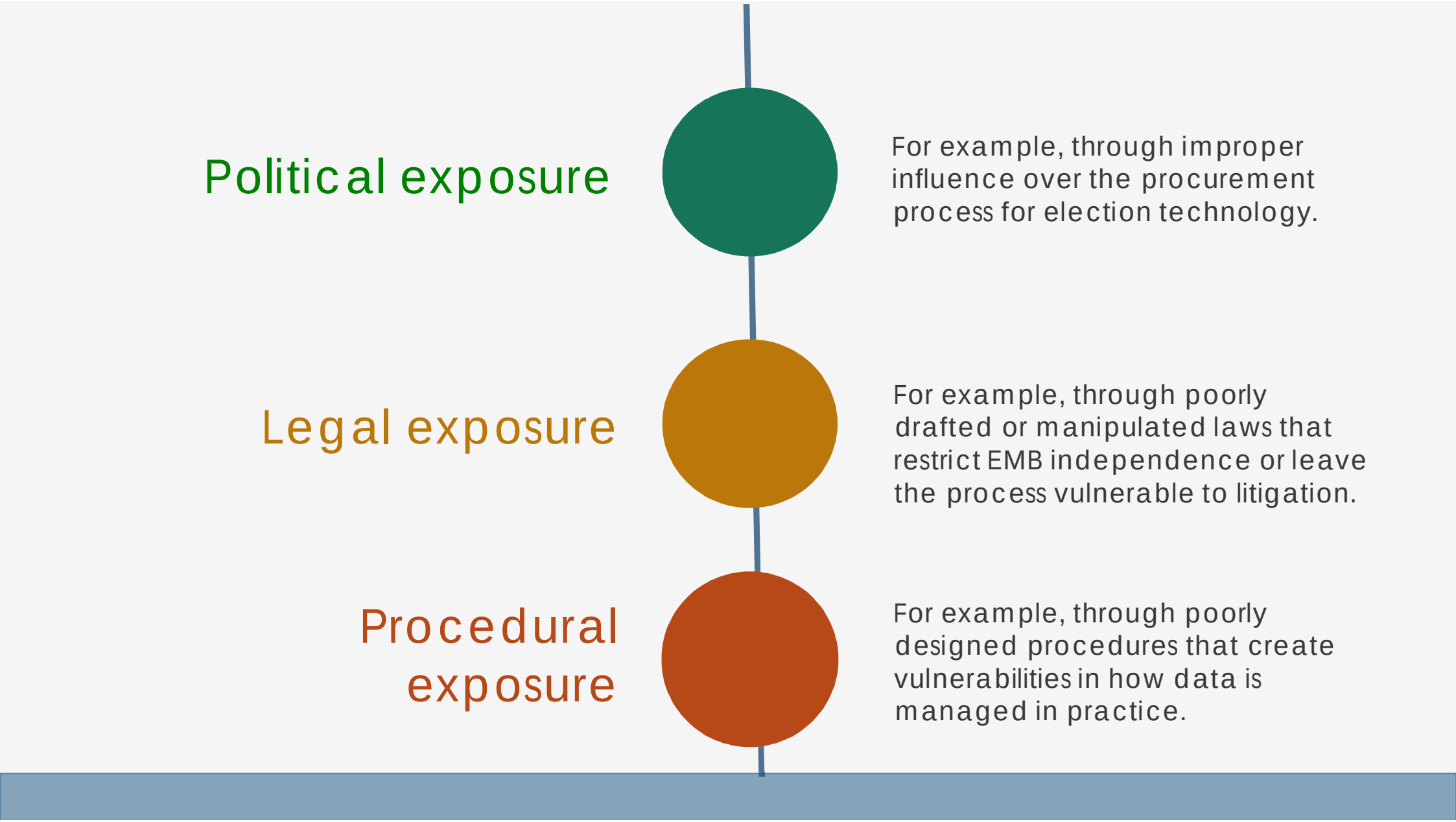
- It is important to look at cybersecurity holistically, as one type of vulnerability may be addressed in isolation while another is exploited instead.
- Or, different types of cybersecurity exposure may compound to produce a unique vulnerability that can result in significant problems, whether through malpractice (negligence or mistake) or fraud (deliberate exploitation).

Types of cybersecurity exposure in elections

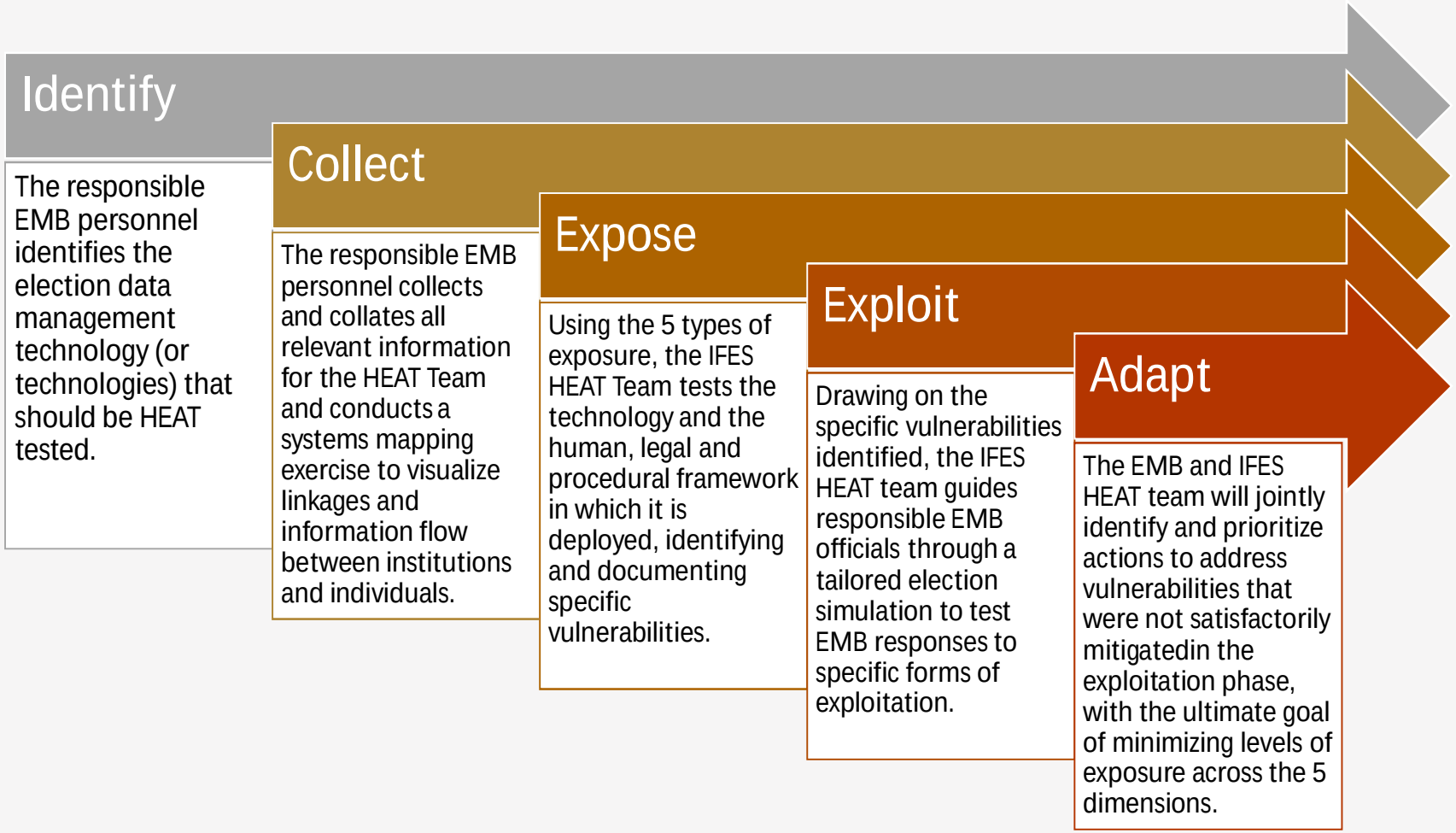


Types of cybersecurity exposure in elections




Political exposure
For example, through improper influence over the procurement process for election technology.
Legal exposure
For example, through poorly drafted or manipulated laws that restrict EMB independence or leave the process vulnerable to litigation.
Procedural exposure
For example, through poorly designed procedures that create vulnerabilities in how data is managed in practice.

Holistic Exposure and Adaptation Testing Process (HEAT Process)



EMBs should seek to change the optics when introducing technology into the electoral process from a “black box” into a “glass box”.