Cybersecurity in Elections

The HEAT Process
How can EMBs secure systems from vulnerabilities that leave them exposed, while at the same time protecting transparency?
Types of exposure

Technology exposure
For example, through hacking or system failure.

Human exposure
For example, through poorly trained or malevolent officials using data systems.
For example, through poorly drafted or manipulated laws that restrict EMB independence or leave the process vulnerable to litigation.

For example, through improper influence over the procurement process for election technology.

For example, through poorly designed procedures that create vulnerabilities in how data is managed in practice.
The responsible EMB personnel identifies the election data management technology (or technologies) that should be HEAT tested.

The responsible EMB personnel collects and collates all relevant information for the HEAT Team and conducts a systems mapping exercise to visualize linkages and information flow between institutions and individuals.

Using the 5 types of exposure, the IFES HEAT Team tests the technology and the human, legal and procedural framework in which it is deployed, identifying and documenting specific vulnerabilities.

Drawing on the specific vulnerabilities identified, the IFES HEAT team guides responsible EMB officials through a tailored election simulation to test EMB responses to specific forms of exploitation.

The EMB and IFES HEAT team will jointly identify and prioritize actions to address vulnerabilities that were not satisfactorily mitigated in the exploitation phase, with the ultimate goal of minimizing levels of exposure across the 5 dimensions.