Cybersecurity for Elections

A Commonwealth Guide to Best Practice

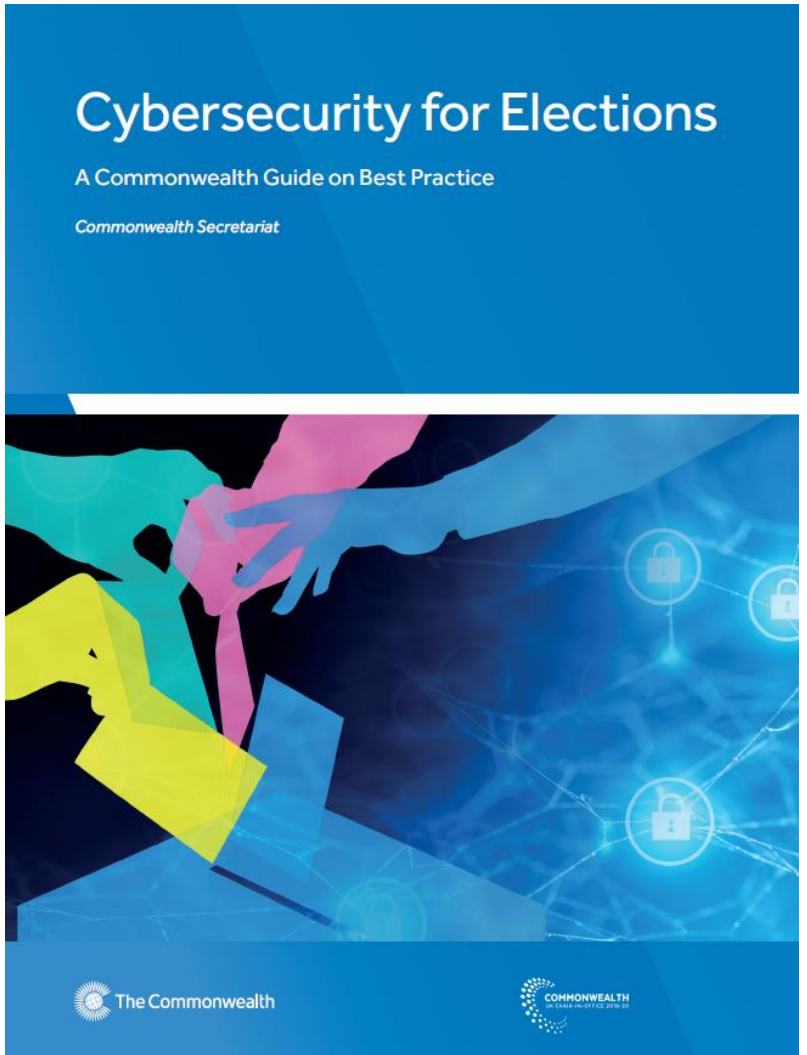
The Commonwealth

Matthew Moorhead

June 2020

The Commonwealth

A guide for Election Management Bodies (EMBs)



The Commonwealth Charter recognises the inalienable right of individuals to participate in democratic processes

In particular through free and fair elections.

- Governments, political parties and civil society are all responsible
  - for upholding and promoting democratic culture and practice and
  - are accountable to the public in this regard.

International human rights law, in particular through the International Covenant on Civil and Political Rights (ICCPR),

- also enshrines the right to take part in the conduct of public affairs,
- and to vote and to be elected at genuine periodic elections
- by universal and equal suffrage
- and to be held by secret ballot.

Commonwealth Cyber Declaration, adopted by Heads of Government at CHOGM 2018

- Importance of a free, open, inclusive and secure cyberspace,
  - achieved through the importance of common standards and
  - the strengthening of data protection and security frameworks.
- Importance of tolerance and respect for diversity and understanding
- Affirms: the same citizens' rights offline must also be protected online

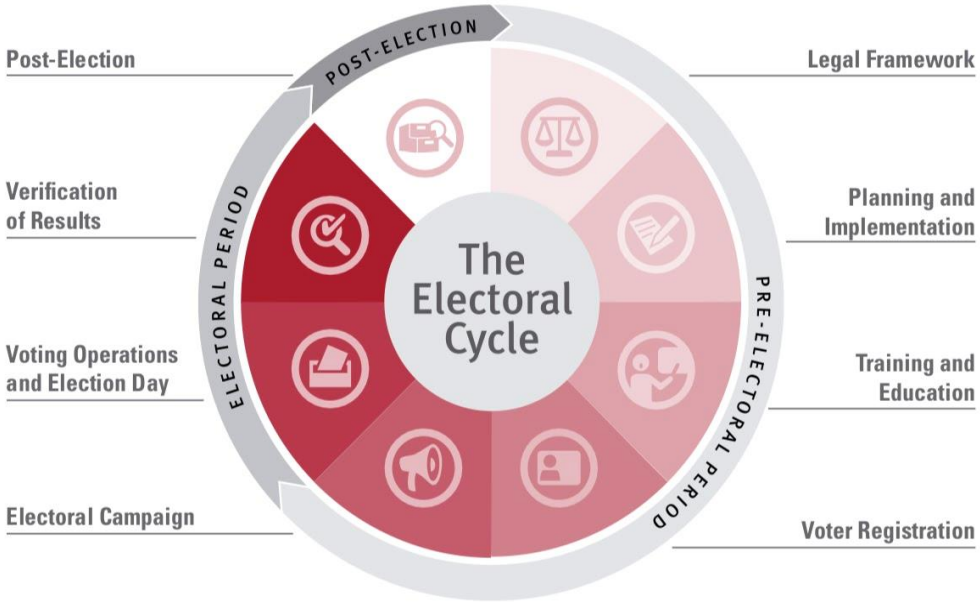
The Commonwealth

Principles and recommendations

The Guide contains **58 specific recommendations** for action, organised around the following principles: democratic self-determination, international law and cooperation, enhancing the safety of ICTs for elections, and non-discrimination.

The recommendations address cybersecurity concerns **across the electoral cycle**: planning and logistics; electoral rolls; campaigning; voting; communication of results; auditing and challenging results.

Examples of good practice are drawn from EMBs in the 54 Commonwealth countries and the wider international community.



Source: International IDEA

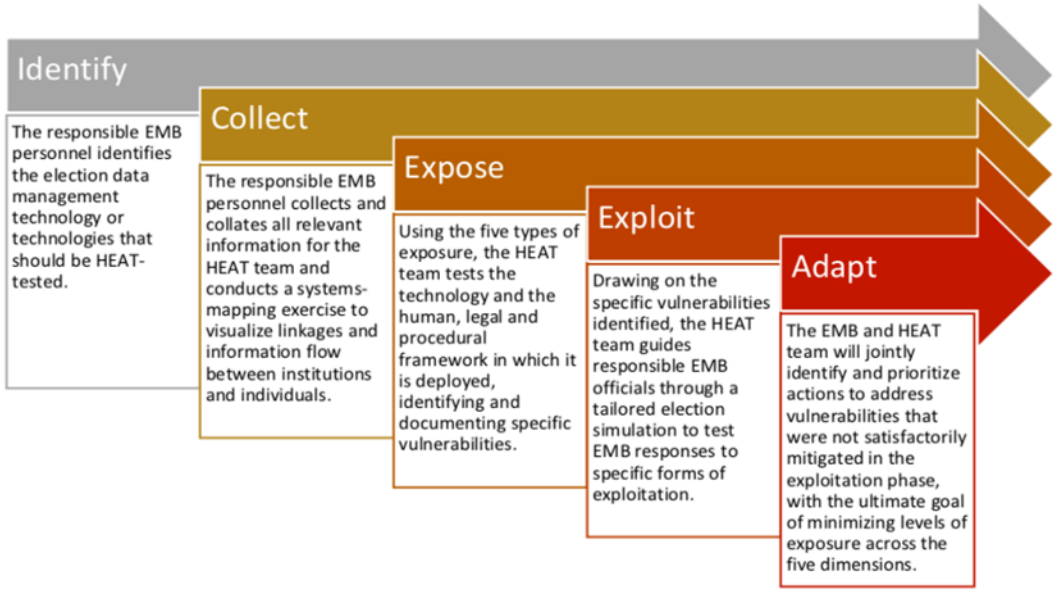
The Commonwealth

Selected recommendations

- EMBs should give careful consideration to use of technology in the elections process if and where it demonstrably addresses a clear need, while carefully managing the resulting cybersecurity risks with measures that are proportionate.

- EMBs and national cybersecurity agencies should consider whether designation of key election systems as part of critical national infrastructure will improve their security.

- EMBs should conduct comprehensive, regular threat assessments, using a tool such as the IFES HEAT Process (Holistic Exposure and Adaptation Testing)



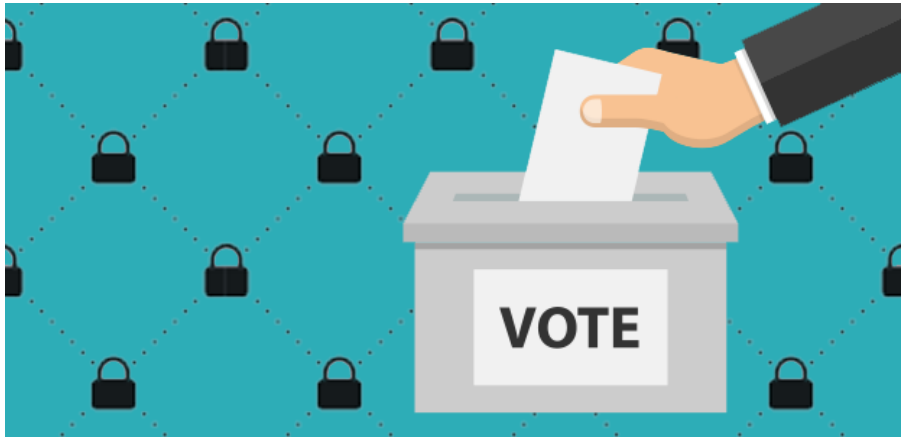
The Commonwealth

Selected recommendations contd.

- EMBs should consider obtaining external certification of security-critical elements of election infrastructure to build public trust.

- EMBs should have in place procedures for ongoing secure configuration and testing of all systems used in elections, with regular exercises to test responses to attacks.

- EMBs and/or their cybersecurity partners should actively monitor election infrastructure for intrusions, as well as having the capability to rapidly escalate and respond during election periods at the direction of senior decision-makers.



The Commonwealth

Building and running secure systems

It is critical for EMBs to ensure appropriate **testing, piloting and auditing** of new technologies when they are deployed in elections.

The European Union's Network and Information Security (NIS) Cooperation Group has recommended that **security tests** of election systems' cybersecurity include the following:

Systems security testing: Ensuring an independent review team cannot cause election systems to act in unwanted ways, using techniques such as searching for known vulnerabilities in underlying software, looking for common programming mistakes and random or 'fuzz' testing.

Penetration testing: A so-called 'red team' attempts to compromise the security of deployed election systems using creative approaches by highly technically skilled testers (sometimes recruited from former hackers), reporting the results to the EMB.

Public testing: A wide range of experts are invited to try and find flaws in election systems, via 'hackathons' or offering 'bug bounty' prizes to anyone that can find security vulnerabilities. This is appropriate for EMBs with mature cybersecurity policies and already well-tested systems.

Application code audit: EMBs and their cybersecurity partners require auditing for vulnerabilities of the source code of applications they procure from third-party suppliers, including open source software.

Exercises: Full election attack simulations, involving senior technical and policy-making officials, will enable the most realistic test of EMB preparedness, but are expensive and time-consuming, and so most useful where there are significant concerns about forthcoming elections. Non-technical table-top exercises can be used more routinely by policy-makers. In either case, EMBs should consider involving key partner agencies and, where appropriate, private sector service providers.

EU NIS Cooperation Group (2018), 'Compendium on Cyber Security of Election Technology' (03/2018), pp.27—31.

The Commonwealth

Comprehensive approach

Those looking to breach the cybersecurity of an electoral process have many different opportunities, given all the various technologies used throughout the whole electoral cycle. EMBs and their cybersecurity partners need to model all of these potential avenues of attack, and ensure the risk of each is appropriately managed.

South Africa's Electoral Commission has identified the following nine principles for its comprehensive approach to security:

Focus is defensive – Both proactive and defensive monitoring

Security in depth – multi-layered segmented networks and subnets

Security-driven application design and development frameworks

User account management and access control

Filtering of all traffic – malware, worms, viruses, spyware, etc.

Continuous security monitoring of all elements

User access is based on a need to know

Continuous monitoring – Knowing when security is breached

Transparency – Stakeholder engagement and data sharing

South Africa's strategic security focus

Source: South Africa Electoral Commission

Conclusion

Commonwealth countries use digital election technologies in a variety of ways – to more efficiently administer electoral registers and communicate results; to authenticate voters using biometric technologies; and to enable voters to register more easily and check details of polling venues. **Electoral authorities should continue to give careful consideration to use of technology in the elections process if and where it demonstrably addresses a clear need, while carefully managing the resulting cybersecurity risks, with measures that are proportionate to the risk.**

> *We must not … make the mistake of placing our faith in technical solutions to political problems. When opposition parties and donors invest in the transformative power of new scientific advances, they often overlook the fact that even the most advanced forms of election technology rely on human programming and management. And there is nothing about digital technology that means that those who use it are likely to be any more trustworthy or fair. As John Githongo, Kenya's former anti-corruption tsar, has put it: 'You cannot digitise integrity.*

Nic Cheeseman and Brian Klaas (2019), *How to Rig an Election*, Yale University Press, New Haven, pp.236–237.

The Commonwealth

Get the Guide at:
https://books.thecommonwealth.org/cybersecurity-elections-paperback

Presented by: Matthew Moorhead

Email: m.moorhead@commonwealth.int

June 2020

The Commonwealth