Executive Summary

Cybersecurity and Elections Assessment in Bosnia and Herzegovina

March 2020

Executive Summary
Cybersecurity and Elections Assessment in Bosnia and Herzegovina

March 2020

Executive Summary: Cybersecurity and Elections Assessment in Bosnia and Herzegovina

International Foundation for Electoral Systems
2011 Crystal Drive, 10th Floor
Arlington, VA 22202
Email: editor@ifes.org
Fax: 202.350.6701

This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The opinions expressed herein are those of the author(s) and do not necessarily reflect the views of USAID or the United States Government.

Cybersecurity and Elections Assessment in Bosnia and Herzegovina

Executive Summary

Election management bodies (EMBs) worldwide have been the victims of devastating attacks that aim to delegitimize the electoral process. While many have now built up their defenses, the scope and sophistication of attacks on democratic systems and institutions continues to increase regionally and globally. While no detected attack has impacted its electoral processes so far, the Central Election Commission (CEC) of Bosnia and Herzegovina (BiH) needs to prepare itself for both opportunistic attacks looking for financial gain, such as ransomware attacks that impact local and central government organizations worldwide, and politically motivated attacks against the electoral system as a whole.

The International Foundation for Electoral Systems (IFES) outlines strategies for EMBs to strengthen their technology and procedures to counter vulnerabilities by following its Holistic Exposure and Adaptation Testing (HEAT) process. Since no electoral process or technology is infallible, the HEAT process aims to identify and test the potential exploitation of vulnerabilities of election management technology and the legal and operational frameworks in which the technology operates. The methodology assesses technological, human, political, legal and procedural exposures and encourages a more holistic assessment of what could go wrong.

The Cybersecurity and Elections Assessment consisted of desk research using IFES' previous assessments, open information available online and a series of meetings and consultations held with relevant stakeholders, which took place from March 9-13, 2020. The assessment was led by an IFES cybersecurity and elections team, including IFES Technology and Cybersecurity Adviser and team lead Thomas Chanussot, cybersecurity and information security expert Srdjan Babic, IFES Regional Director for Europe and Eurasia Dr. Beata Martin-Rozumiłowicz and IFES Senior Electoral Technical Assistance Expert Nermin Nisic. The desk research and consultations informed the team of the challenges faced by the CEC, the current BiH cybersecurity landscape, cybersecurity resources and threats faced in BiH.

The assessment team found that the cybersecurity capacity and legislative framework in BiH is still at an early stage of development. Of particular concern for the CEC is the absence of a national body to coordinate and manage incident responses, leaving the CEC without support from competent agencies regarding cybersecurity incidents.

The core staff of the CEC's Information and Communication Technology (ICT) department are longstanding employees and have a strong operational understanding of elections but have insufficient technical capacity to provide ongoing support to the existing CEC systems. Additionally, the ICT department is critically understaffed and under-resourced; the difficulty to fill ICT positions in the public sector is a global problem, particularly in Europe and Eurasia, and is not specific to the CEC. This is, in part, due to renumeration differences between the public and private sector, leading to a consequent shortage of skills and improper segregation of staff duties, creating a risk of misuse, leakage and unauthorized access. This leaves the CEC vulnerable to internal attacks, manipulation or sabotage that could be financially or politically motivated.

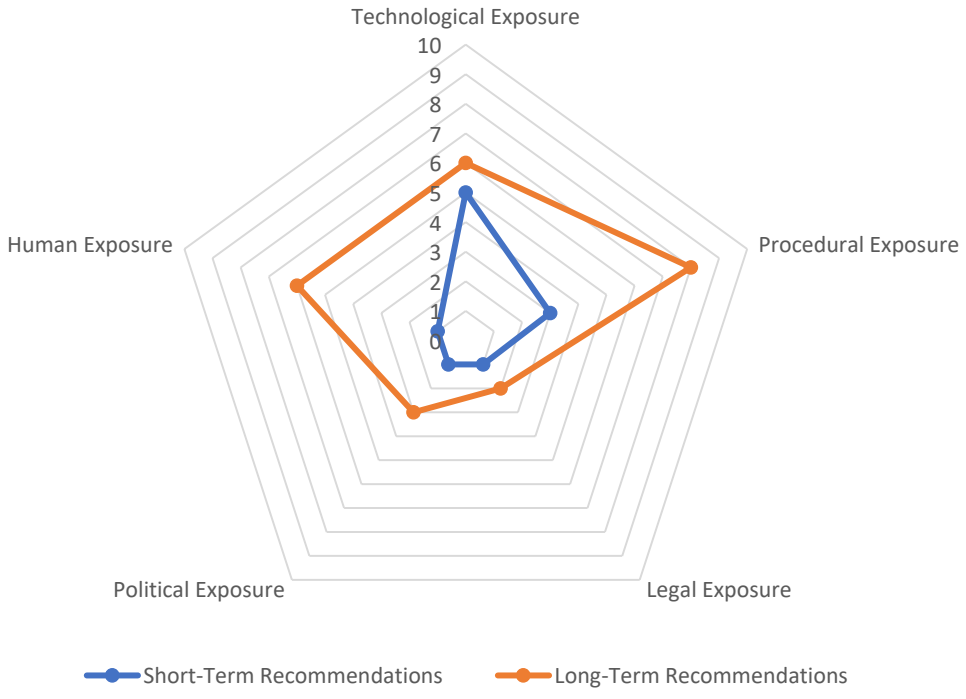
The ICT department has managed to establish and maintain trust among its users; cybersecurity incidents have been swiftly reported before they escalated and did not impact operations. The ICT department should now strive to maintain this trust, as it will remain the first layer of defense against malicious activity targeting the CEC.

Further, the CEC is unprepared to face cyberattacks, both on the technical and organizational levels. Web-facing services lack proper protection and could be compromised by moderately sophisticated attacks, putting the CEC's data integrity and reputation at risk. Overall, the CEC does not have adequate network protection and cybersecurity services in place to protect its infrastructure. The CEC's main data center is physically located at the CEC's headquarters, but there is no existing back-up data center. There is also no disaster recovery plan or business continuity plan to mitigate risks during a crisis.

In general, there is a lack of cybersecurity training and lack of resources to provide training at the CEC and most other agencies, which is a major hindrance to overall cybersecurity posture. More general courses in cybersecurity awareness and cyber hygiene would benefit all general, non-ICT staff in the CEC and in Municipal Election Commissions. Staff should be trained to identify cybersecurity vulnerabilities and threats and be equipped on how to deal with cyberattacks.

The more technology is used in an organization, the more there is a need for a top-down security approach. Although the CEC does not administer online or electronic voting, it is still vulnerable to multiple internal and external threats. The CEC needs a management-driven effort to develop risk-mitigation plans involving representatives from all departments, not only the ICT department.

IFES presented short- and long-term recommendations in the full assessment report to strengthen staff capacity, prioritize the strengthening of network and infrastructure defense and reduce or mitigate cybersecurity-related risks, overall. The radar chart below demonstrates the types of recommendations by their exposure risks.



Global Expertise. Local Solutions.
Sustainable Democracy.

IFES | 2011 Crystal Drive | 10th Floor | Arlington, VA 22202 | www.IFES.org