NEWS

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

Sept. 6, 2018

FOR IMMEDIATE RELEASE

New Report Identifies Steps to Secure Americans' Votes; All U.S. Elections Should Use Paper Ballots by 2020 Presidential Election; Internet Voting Should Not Be Used at This Time

WASHINGTON -- To protect the integrity and security of U.S. elections, all local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election, says a new report from the National Academies of Sciences, Engineering, and Medicine. In addition, every effort should be made to use paper ballots in the 2018 federal election. Ballots that have been marked by voters should not be returned over the Internet or any network connected to it, because no current technology can guarantee their secrecy, security, and verifiability, the report says.

"The 2016 presidential election was a watershed moment in the history of elections – one that exposed new challenges and vulnerabilities that require the immediate attention of state and local governments, the federal government, researchers, and the American public," said Michael McRobbie, president of Indiana University and co-chair of the committee that conducted the two-year study and wrote the report. The committee included computer science and cybersecurity experts, legal and election scholars, social scientists, and election officials.

Assessments by the U.S. intelligence community found that during the 2016 presidential election, America's election infrastructure was targeted by actors sponsored by the Russian government who obtained and maintained access to elements of multiple U.S. state or local election systems. The intrusions made clear the vulnerability of election infrastructure to cyberattack, the new report says -- a vulnerability exacerbated by aging equipment and a lack of sustained funding. Foreign state-sponsored attacks present a challenge for even the most well-resourced jurisdictions; small, under-resourced jurisdictions are at serious risk.

State and local governments must work together with the federal government to secure and improve election systems, the report says. The cybersecurity of electronic systems used in elections, such as voter registration databases and vote tabulation systems, should be continuously monitored and improved. And audits of paper ballots should be used to verify that votes have been tabulated correctly and to detect when electronic systems have been compromised.

"This is a critical time for our country," said committee co-chair Lee Bollinger, president of Columbia University. "As a nation, we need to take collective action to strengthen our voting systems and safeguard our democracy. In addition, the nation's leaders need to speak candidly and apolitically about threats to election systems. The American people must have confidence that their leaders place the larger interests of democracy above all else."

The report recommends steps that the federal government, state and local governments, and election administrators should take to improve the security of election infrastructure and safeguard its integrity and credibility, including:

- **Elections should be conducted with human-readable paper ballots.** Paper ballots form a body of evidence that is not subject to manipulation by faulty software or hardware and that can be used to audit and verify the results of an election. Human-readable paper ballots may be marked by hand or by machine (using a ballot-marking device), and they may be counted by hand or by machine (using

an optical scanner), the report says. Voters should have an opportunity to review and confirm their selections before depositing the ballot for tabulation. Voting machines that do not provide the capacity for independent auditing – i.e., machines that do not produce a printout of a voter's selections that can be verified by the voter and used in audits – should be removed from service as soon as possible.

- **States should mandate a specific type of audit known as a "risk-limiting" audit prior to the certification of election results.** By examining a statistically appropriate random sample of paper ballots, risk-limiting audits can determine with a high level of confidence whether a reported election outcome reflects a correct tabulation of the votes cast. Risk-limiting audits offer a high probability that any incorrect outcome can be detected, and they do so with statistical efficiency; a risk-limiting audit performed on an election with tens of millions of ballots may require examination by hand of as few as several hundred randomly selected paper ballots. States should begin with pilot programs of risk-limiting audits and fully implement these audits for all federal and state election contests – and local contests where feasible – within a decade.

- **Internet voting should not be used at the present time, and it should not be used in the future until and unless very robust guarantees of secrecy, security, and verifiability are developed and in place.** Currently, no known technology can guarantee the secrecy, security, and verifiability of a marked ballot transmitted over the Internet. (The Internet is an acceptable way to transmit unmarked ballots to voters as long as voter privacy is maintained and the integrity of the received ballot is protected.)

- **Election administrators should routinely assess the integrity of voter registration databases and put in place systems that detect efforts to probe, tamper with, or interfere with voter registration systems.** States should require election administrators to report any detected compromises or vulnerabilities in voter registration systems to the U.S. Department of Homeland Security, the U.S. Election Assistance Commission, and state officials.

- **Jurisdictions that use electronic pollbooks should have backup plans in place to provide access to current voter registration lists in the event of any disruption.** Traditionally, pollbooks – which are used to verify an individual's eligibility to vote – have been printed lists, but 36 states now use e-pollbooks in at least some of their jurisdictions.

- **Election systems should continue to be considered as U.S. Department of Homeland Security-designated critical infrastructure.** In addition, the U.S. Election Assistance Commission and the U.S. Department of Homeland Security should continue to develop and maintain a detailed set of cybersecurity best practices that election system vendors and state and local election officials should incorporate into their practices.

- **Congress should:**
  - appropriate funds for distribution by the U.S. Election Assistance Commission for the ongoing modernization of election systems;
  - provide funding for state and local governments to improve their cybersecurity capabilities on an ongoing basis;
  - require state and local election officials to provide the U.S. Election Assistance Commission with data on voting system failures and other difficulties arising during elections (for example, long lines, fraudulent voting, or intrusions into voter registration databases), and such information should be made publicly available;
  - fully fund the U.S. Election Assistance Commission to carry out its existing functions as well as the additional functions articulated in the report; and
  - authorize and fund immediately a major initiative on voting that supports research relevant to the administration, conduct, and performance of elections. This initiative should include academic centers to foster collaboration both across disciplines and with state and local election officials and industry.

The study was sponsored by the Carnegie Corporation of New York and the William and Flora Hewlett Foundation. The National Academies of Sciences, Engineering, and Medicine are private, nonprofit institutions that provide independent, objective analysis and advice to the nation to solve complex problems and inform public policy decisions related to science, technology, and medicine. The National Academies operate under an 1863 congressional charter to the National Academy of Sciences, signed by President Lincoln. For more information, visit http://national-academies.org.

Contacts:
Sara Frueh, Media Relations Officer
Andrew Robinson, Media Relations Assistant
Office of News and Public Information
202-334-2138; e-mail news@nas.edu

Social Media:
Follow us on Twitter: @theNASEM
Follow us on Instagram: @theNASEM
Follow us on Facebook: @NationalAcademies

Copies of ***Securing the Vote: Protecting American Democracy*** are available at www.nap.edu or by calling 202-334-3313 or 1-800-624-6242. Reporters may obtain a copy from the Office of News and Public Information (contacts listed above).

THE NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE

Policy and Global Affairs Division
Committee on Science, Technology, and Law
Division on Engineering and Physical Sciences
Computer Science and Telecommunications Board

Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology

Lee C. Bollinger *(co-chair)*
President
Columbia University
New York City

Michael A. McRobbie *(co-chair)*
President
Indiana University
Bloomington

Andrew W. Appel
Eugene Higgins Professor of Computer Science
Princeton University
Princeton, N.J.

Josh Benaloh
Senior Cryptographer
Microsoft Research
Redmond, Wash.

Karen S. Cook[1]
Ray Lyman Wilbur Professor of Sociology, and
Vice Provost for Faculty Development and Diversity, and
Director
Institute for Research in the Social Sciences

Stanford University
Stanford, Calif.

Dana DeBeauvoir
Travis County Clerk
County of Travis
Austin, Texas

Moon Duchin
Associate Professor
Department of Mathematics and
Founding Director
Program in Science, Technology, and Society
Tufts University
Medford, Mass.

Juan E. Gilbert
Andrew Banks Family Preeminence Endowed Professor and Chair
Department of Computer and Information Science and Engineering
University of Florida
Gainesville

Susan L. Graham[2]
Pehong Chen Distinguished Professor Emerita
Computer Science Division
Department of Electrical Engineering and Computer Sciences
University of California
Berkeley

Neal Kelley
Registrar of Voters
County of Orange
Santa Ana, Calif.

Kevin J. Kennedy
Director and General Counsel (retired)
Wisconsin Government Accountability Board
Madison

Nathaniel Persily
James B. McClatchy Professor of Law
Stanford Law School
Stanford, Calif.

Ronald L. Rivest[1,2]
Institute Professor
Department of Electrical Engineering and Computer Science
Massachusetts Institute of Technology
Cambridge

Charles Stewart III
Kenan Sahin Distinguished Professor of Political Science
Massachusetts Institute of Technology
Cambridge

STAFF

Anne-Marie C. Mazza
Staff Officer

---

[1]Member, National Academy of Sciences
[2]Member, National Academy of Engineering