

WEST VIRGINIA LEGISLATURE

2026 REGULAR SESSION

Introduced

Senate Bill 1050

FISCAL
NOTE

By Senator Rucker

[Introduced February 21, 2026; referred
to the Committee on Government Organization; and
then to the Committee on Finance]

1 A BILL to amend the Code of West Virginia, 1931, as amended, by adding a new section,
 2 designated §3-1A-6A, relating to creating the West Virginia Task Force on Election
 3 Integrity; and charging task force with identifying optimal, timely, fully secure, fully
 4 transparent, and auditable vote tabulation and election management methods and/or
 5 systems.

Be it enacted by the Legislature of West Virginia:

ARTICLE 1A. STATE ELECTION COMMISSION AND SECRETARY OF STATE.

§3-1A-6A. West Virginia Task Force on Election Integrity; charged with identifying optimal, timely, fully secure, fully transparent and auditable vote tabulation and election management methods and systems.

1 (a) As used in this section, "Task Force" means the West Virginia Task Force on Election
 2 Integrity established by this section.

3 (b) The West Virginia Task Force on Election Integrity is created and shall be organized
 4 within the Office of the Secretary of State, subject to the chief executive authority of the Governor.

5 (c) The Task Force shall be composed of the following members:

6 (1) One ex officio, non-voting member from the House of Delegates, appointed by the
 7 Speaker of the House of Delegates.

8 (2) One ex officio, non-voting member from the State Senate, appointed by the President
 9 of the Senate.

10 (3) The Attorney General or his or her designee.

11 (4) The Secretary of the Department of Homeland Security or his or her designee with
 12 experience in election security and election cybersecurity operations.

13 (5) One member representing the cybersecurity industry with experience relevant to the
 14 work of the Task Force, appointed by the Governor with the advice and consent of the Senate and
 15 House members of the Task Force.

16 (6) Four citizen members representing the election integrity citizen network with

17 experience relevant to the work of the Task Force, appointed by the Governor with the advice and
18 consent of the Senate and House members of the Task Force.

19 (7) Two county clerks with experience relevant to the work of the Task Force, appointed by
20 the Governor with the advice and consent of the Senate and House members of the Task Force.

21 (8) One member from the West Virginia Fusion Center with experience in election security
22 and election cybersecurity operations.

23 (9) The Chief Information Officer of the Office of Technology or his or her designee with
24 experience in election security and election cybersecurity operations.

25 (d) The Governor shall designate the Chair of the Task Force, which designee shall be in
26 addition to those members listed in subsection (c).

27 (e) The responsibilities of the Task Force shall include, but not be limited to, the following:

28 (1) Investigation of all feasible, secure methods and secure technologies in order to
29 identify and recommend the optimal choice for a timely, fully secure, and fully transparent and
30 auditable vote tabulation and election management method and system; and proposing legislation
31 for the adoption in West Virginia Code of the Task Force's recommendation; and

32 (2) In its investigation of all feasible, secure methods and secure technologies, the Task
33 Force shall research thoroughly:

34 (A) The technical specifications of any equipment or interconnected system or subsystem
35 of equipment that is used in the automatic acquisition, storage, manipulation, management,
36 movement, control, display, switching, interchange, transmission, or reception of data or
37 information related to critical election infrastructure;

38 (B) Any equipment, systems, software, services, software as a service, and/or cloud
39 computing used as or in conjunction with any critical election infrastructure;

40 (C) The feasibility of hand counting hand marked paper ballots at the precinct level as a
41 method of timely, fully secure, and fully transparent and auditable vote tabulation; and

42 (3) In investigating any and all technologies under consideration for use as or in

43 conjunction with any critical election infrastructure, the Task Force shall:

44 (A) Thoroughly monitor, review, consider and abide by any information, reports, findings or
45 orders issued by the U.S. Director of National Intelligence or the President of the United States or
46 his or her designee, regarding known or suspected, malware, malicious code or source code,
47 system design or operation vulnerabilities, or other internal or external threats in the sphere of
48 digital application or cybersecurity in the broadest possible application of those terms in
49 investigating any technologies for use as or in conjunction with any critical election infrastructure,
50 and ensure that any recommendations of the Task Force shall be subject to any restrictions or
51 prohibitions applicable to critical election infrastructure mandated by federal law or Executive
52 Order of the President of the United States;

53 (B) Thoroughly investigate and assess in all methods and technologies considered the
54 degree to which such prospects, including software, hardware, tabulating equipment, printers, and
55 any other accessories, do or may incorporate hardware or software designed, produced, owned,
56 or licensed by any person or entity owned, operated, or majority-controlled by a foreign company,
57 domestic company registered in another country if a domesticated subsidiary of a foreign
58 corporation, or by a person who is not a United States citizen, or is produced, in whole or in part in
59 a foreign country, which would be prohibited under federal law as information and communications
60 technology or services (ICTS) supplied by persons owned by, controlled by, or subject to the
61 jurisdiction of foreign adversaries;

62 (C) Thoroughly investigate and assess in all methods and technologies considered
63 whether the prospect contains within its hardware components a wireless modem, cellular,
64 Bluetooth, or other wireless computer networking, intranet, ethernet, internet, other computer
65 networking capability, and forensically investigating any residual vulnerability even if the
66 operational system, software or firmware purports to disable the wireless connection capability;

67 (D) Thoroughly investigate and assess in all methods and technologies considered the
68 particular and aggregate risks of ballot harvesting, ballot trafficking, algorithmic manipulation of

69 votes or vote tabulations, cyber-attack or manipulation, inaccurate voter registration rolls,
70 manipulated electronic tabulation of votes by any electronic voting system, the compromise or
71 corruption of the tabulation of votes, and of votes being electronically counted or tabulated with
72 decimal values instead of a whole numeric value of one per vote;

73 (E) Thoroughly investigate and assess in all methods and technologies considered the
74 particular and aggregate risks of any vote tabulator, electronic voting system, electronic poll book
75 (or "e-poll book"), and computer connected to the electronic voting system network of being
76 connected to, or being capable in its internal hardware of being connected to, any wireless or
77 cellular network, or by actual physical connection, or by the transfer of data of any kind to or from a
78 tabulator or electronic voting system via portable hard drives or similar hardware;

79 (F) Thoroughly consider the feasibility of defining in code "Public Election Related
80 Information and Data" as meaning all data contained within, or transferred to or by the Election
81 Management System database, except for cybersecurity and individual voter personal
82 identification information, including, but not limited to any and all executable code, data transferred
83 via secure physical or wireless network, specifically including any routing through any Albert
84 Sensor or analogous device or system to any external servers or cloud based servers, data
85 transferred by and/or executable code contain within portable drives, system log files, audit log
86 files, data files, system audit files, and all other files of every kind and nature including all election
87 definition files, cast vote records (or "CVRs"), election summary with group detail, precinct
88 summary report(s) with group detail, numbered key canvass(es), results corrections log(s),
89 system log(s), machine log report(s) as CSV (comma separated values) files, precinct, county and
90 state election management system audit log(s), administrative audit events report(s), and/or
91 election audit events report(s), or any electronic data performing the same or functional
92 equivalence of the previously listed categories of data, with the widest possible presumption of
93 inclusion within the category to be given; and

94 (4) Determining and making recommendations regarding whether the Task Force should

95 be extended to monitor, analyze, and make findings and recommendations to keep pace with
96 future changes in Election Integrity methods and technology and uses of such methods and
97 technology;

98 (5) Taking an inventory of the current or proposed vote tabulation and election
99 management methods, technology and systems within the state and each county within the state;

100 (6) Other topics related to Election Integrity that may arise from testimony or reports to the
101 Task Force submitted by its members, invited guests, or the public, or from federal authorities.

102 (f) The Office of Technology and the Fusion Center shall provide technical support to the
103 Task Force with full transparency granted to the member representing the cybersecurity industry.

104 (g) All initial appointments to the task force shall be made not later than 60 days after the
105 effective date of this section. Any vacancy shall be filled by the appointing authority, as applicable,
106 within 30 days of such vacancy arising.

107 (h) The Task Force shall hold its first meeting not later than 90 days after the effective date
108 of this section and shall meet quarterly thereafter with options to either attend in-person or online.

109 (i) The Task Force shall submit an interim electronic progress report six months after its
110 first meeting, and shall submit an annual electronic report by July 1, 2027 to the House of
111 Delegates, Senate, and the Governor and present the report to the Joint Committee on
112 Government and Finance covering the Task Force's findings and recommendations related to the
113 responsibilities under subsection (e). The Task Force shall submit reports in a like manner for a
114 second year at six months and by July 1, 2028, unless the Task Force concludes that it has
115 satisfactorily fulfilled its charge upon the filing of its first annual report.

116 (j) The Task Force shall terminate on July 1, 2028, unless the Task Force concludes that it
117 has satisfactorily fulfilled its charge as of July 1, 2027, or the Governor directs by decree that the
118 Task Force's charge must be extended in order to satisfactorily fulfill its charge.

NOTE: The purpose of this bill is to create the West Virginia Task Force on Election

Integrity.

Strike-throughs indicate language that would be stricken from a heading or the present law and underscoring indicates new language that would be added.