RESOLVED, That the American Bar Association urges the United States Congress to protect the security and integrity of U.S. federal elections by enacting legislation that authorizes and appropriates necessary funding for the National Institute of Standards and Technology (NIST) to:

(1) Define federal standards for cybersecurity of election systems software, infrastructure, and hardware, whether provided by the government or private sector companies, used in handling, storing, processing, or transmitting data for voter registration, vote tallying, voter polling, vote reporting, or the manufacturing, servicing, or writing of election parameters of voting machines/equipment (“Election Process”).

(2) Develop a certification process for the security and integrity of election systems software, infrastructure, and hardware (and associated components and modules) used in the Election Process.

(3) Analyze the private sector’s role in the Election Process and recommend any functions or roles that should be changed or restricted to public sector election officials to address issues related to the security and integrity of federal elections;

FURTHER RESOLVED, That the American Bar Association urges the U.S. Congress to allocate adequate funding to protect the security and integrity of the federal Election Process and restrict the use of all such funding to only those election jurisdictions that:

(1) Use such funding for the Election Process in a manner consistent with the NIST federal election standards;

(2) Require annual comprehensive cybersecurity assessments by an independent third party of all systems used in the Election Process in accordance with the NIST federal election standards;

(3) Require annual comprehensive cybersecurity assessments by an independent third party of private sector companies involved in the Election Process in accordance with the NIST federal elections standards and make those assessments available to election officials contracting with them;

(4) Require that only election systems software, infrastructure, and hardware (and associated components and modules) that are certified by an independent third party in accordance with the NIST federal election standards be used in federal
(5) Require the deployment of human-readable paper ballots;
(6) Establish requirements for post-election auditing of votes, at least on the level of risk-limiting audits, and make the findings public; and

FURTHER RESOLVED, That the American Bar Association urges state, local, territorial, and tribal legislatures and governments to protect the security and integrity of U.S. election systems by allocating funding for the Election Process consistent with this Resolution.
I. STEPS TO COMBAT IMMINENT THREATS TO U.S. ELECTIONS

The American Bar Association (ABA) strongly supports free, fair, and impartial elections that form the foundation of our democracy. Ensuring trust and confidence in the election system is critical and should be given a high priority by all.

The integrity of the American election process is at risk due to two primary factors:

(1) Election vulnerabilities and possible points of exploitation within the various components of the “Election Process,” including security issues with machines and devices, the voter registration process, transmission of votes, tallying votes, voter polling, and the reporting of votes.

The role of private sector companies in the election process and possible insecurities within their systems and processes are also an aspect of this risk.

(2) Disinformation campaigns by nation states and other foreign entities aimed at influencing voters to vote for certain favored candidates and sow discord.

Volumes of evidence establish that Russian cyber operations targeted election infrastructure in the U.S. in order to undermine the integrity and availability of the 2016 elections. Russia is the largest, but not the only, threat. U.S. intelligence agencies and law enforcement have expressed concern “about ongoing campaigns by Russia, China and other foreign actors, including Iran, to undermine confidence in democratic institutions and influence public sentiment and government policies.”

The risk of foreign interference in U.S. elections remains at critical levels. On Election Day 2019 in a joint statement, government leaders of the law enforcement, homeland security and intelligence communities provided observations on election security and their outlook for the 2020 elections. They concluded that “[o]ur adversaries want to undermine our democratic institutions, influence public sentiment and affect government policies. Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process or influence voter perceptions.”

---


The Resolution Focuses on Vulnerabilities in the Election Process

This Resolution identifies essential steps that should be taken by Congress, state and local governments, election officials, and private sector entities to secure the “Election Process.” The Resolution consists of three measures designed to address the problem of election security head-on – by leveraging the power of Congress to protect federal elections when appropriating federal funds, drawing on the expertise of NIST (the federal agency designated by Congress to address complex technology issues and develop appropriate cybersecurity standards and certification processes), and recognizing the central role of states and local election officials to conduct federal, state, and local elections.

The Resolution is narrowly tailored to focus on problems within the Election Process that can be exploited to undermine the integrity of federal elections – achievable steps in reducing risks to the American election process.

As defined, the proposed requirements pertain to private sector companies and entities that handle, store, process, or transmit data involved in the Election Process. The Resolution is not intended to apply to small organizations such as grocery stores, Lion’s Clubs, VFW Halls, churches, or the like, that simply serve as a physical location for parts of the Election Process.

The Resolution addresses federal elections because the U.S. Congress has the authority to specify requirements to protect federal interests. This approach is likely to spur reforms in most state and local jurisdictions because they cannot afford to have separate equipment for federal and state elections.

The U.S. government provided $380 million in fiscal year 2018 to state and local election officials to support voting equipment purchases and security enhancements to election systems but did not specify any particular security measures to be taken. For example, the funding could have been spent to purchase voting machines or equipment with known security vulnerabilities. The Resolution requires that federal funding for federal elections be restricted to only those election jurisdictions that are undertaking reforms consistent with NIST standards developed for federal elections. The Resolution also addresses the broad and little-understood role of private sector companies in the election process. These companies – not election officials – are the primary entities involved in wiring or

---

4 The Resolution defines “Election Process” as the election systems software, infrastructure, and hardware, including those of private sector companies, involved in handling, storing, processing, or transmitting data for voter registration, vote tallying, voter polling, vote reporting, or the manufacturing, servicing, or writing of election parameters of voting machines/equipment.

5 The Resolution does not address disinformation campaigns that undermine free and fair elections. Solutions to this problem are being developed within the U.S. government, including executive departments and agencies with responsibility for elections, the intelligence community, and law enforcement. This problem involves different considerations from those involving the Election Process and will require further analysis, given the complexity and rapidly evolving nature of the threat and corresponding lack of consensus on effective approaches. The U.S. Department of Homeland Security has declared that “responding to foreign interference requires a whole of society approach.”

writing parameters for election equipment for each election, conducting voter registration, tallying votes, polling voters, and reporting votes. Currently, there are no security requirements or defined security processes for these entities and processes.

The specific proposals in the Resolution are consistent with substantial analysis and research and represent security best practices and election reforms for which there is widespread consensus.

Highlights of the Resolution are –

- Congress should enact legislation that provides funding for the National Institute of Standards and Technology (NIST) to:
  - develop federal standards for cybersecurity of election systems software, infrastructure, and hardware, including those of private sector companies, involved in handling, storing, processing, or transmitting data for voter registration, vote tallying, voter polling, vote reporting, or the manufacturing, servicing, or writing of election parameters of voting machines/equipment (“Election Process”).
  - develop a certification process for the security and integrity of election systems, software, infrastructure, and hardware (and associated components and modules) used in the Election Process.
  - analyze the private sector’s role in the Election Process and recommend any functions or roles that should be changed or restricted to public sector election officials to better ensure election security and integrity.

- Congress should restrict the use of federal election funding to those state and local jurisdictions that follow specified requirements that are accepted as best practices for federal elections.

- State, local, territorial, and tribal legislatures and governments should protect the security and integrity of U.S. election systems by allocating funding for election purposes consistent with the Resolution.

II. IDENTIFIED RISKS TO THE ELECTION PROCESS

In recent elections, 99 percent of votes in the U.S. were cast or counted on computers. Many of the core election systems – voter registration databases, election management systems, voting machines, and vote- counting systems – use aging computer equipment. The systems employ software that can no longer be updated or patched, include databases that have known vulnerabilities, or are managed by third-party vendors where supply chain risks exist.

Independent researchers have demonstrated a wide array of vulnerabilities in the Election Process. Whether it is e-poll books, paperless voting machines, or ballot marking devices that print unverifiable barcode ballots, far too much of the equipment that American

---

democracy depends [on] is fundamentally insecure.” Researchers found that vulnerabilities in voting devices could:

- alter stored vote tallies, change ballots displayed to voters, or alter the internal software that controls the machines. In particular, many vectors for so-called “Advanced Persistent Threat (APT)” attacks continue to be found or replicated. This means that an attack that could compromise an entire jurisdiction could be injected in any of multiple places during the lifetime of the system. However, it is notable—and especially disappointing—that many of the specific vulnerabilities reported over a decade earlier…are still present in these systems today.

The distributed architecture of elections presents myriad vulnerable points where sensitive voter and candidate data can be stolen or altered, and hackers have successfully targeted state election systems. The July 2018 indictment of 12 Russian intelligence officers detailed how Russian operatives stole voter data, targeted state boards of election, and hacked a voting equipment vendor. It illustrates how future attacks on election infrastructure may occur, whether committed by a domestic or foreign actor.

**Third-Party Risks – Election Management and Voting Administration**

The election management systems used to design computer ballots and program voting machines are highly centralized—run by only a few companies nationwide that work for multiple states. If an attacker could hack into one of those companies, voting software and equipment across the country could be compromised.

**Outsourcing** – The Resolution focuses on a central problem in election security and integrity that has received little publicity but must be addressed in any reform of the voting process. Private companies play an integral role in elections, from manufacturing voting machines and developing software to programming or wiring those machines for each election, designing ballots, tallying votes, and hosting results websites. Third-party vendors are an exploitation point for hackers to target election systems.

Reports that have documented the vulnerabilities and limitations of existing voting machine technology have made it clear that the implementation of new technologies and processes ultimately depends on the companies that design, manufacture, integrate, and support voting machines and the associated technological infrastructure, which have been referred to as the “election technology industry.” The firms in the election

---


9 DefCon 27 Voting Village Report 2019 at 6, supra note 5.


technology industry sell integrated voting solutions, typically including a package of hardware, software, services, and support.

Supply chain risks – Voting machines do not need to be connected to the Internet to be hackable. At points along the supply chain, hackers can infect machine parts and software with malware before they reach the U.S. The small number of companies responsible for the centralized election management systems that control voting and vote-counting machines are prime targets for attackers seeking to impair an election. Experts have shown that an attacker could hack into the company’s systems, install malware on the memory cards used to load ballot design software on voting machines, and potentially change the results of state elections.  

Election management company financed by Russian oligarch – The FBI notified the State of Maryland that a technology company responsible for keeping electronic information on voter registration, election results, and other sensitive data in state elections is “connected to a Russian oligarch who is ‘very close’ to Russian President Putin.” Such operations need not change votes to be effective. Deleting voter registration information or slowing vote counting could easily undermine confidence in elections.

III. REFORMS TO THE ELECTION PROCESS

The election process in the U.S. is highly decentralized and it is regulated state-by-state. More than 9,000 jurisdictions of varying size administer the country’s elections, with voters casting ballots in 185,000 precincts. Decisions about election technology are typically managed at the county level, although some states provide purchasing support or other central services to facilitate the procurement of election technology (typically coordinated through the office of the Secretary of State).

Elections involve much more than the election day activities that voters see when they cast their votes. Election administration includes pre-election responsibilities such as voter registration, qualifying candidates, preparing voting equipment, and absentee voting; election day voting and vote counting; and post-election certifying of results, audits and re-counts. The Resolution focuses on the various vulnerable points in the “Election Process,” as defined above. These aspects of elections must be addressed in order to ensure security and voting fairness and integrity.

---


13 The Washington Post, Surprise, Maryland: Your election contractor has ties to Russia. And other states also remain vulnerable to vote tampering. Page A12. The vendor ByteGrid LLC hosts the Maryland statewide voter registration, candidacy, and election management system, the online voter registration system, online ballot delivery system, and unofficial election night results website. According to the FBI, ByteGrid LLC is financed by AltPoint Capital Partners, whose fund manager is a Russian and its largest investor is a Russian oligarch named Vladimir Potanin.” Statement by Nikki Charlson, deputy administrator for Maryland’s State Board of Elections. NPR, Maryland Investigates Russian National’s Links to State Elections Software, Brakkton Booker (July 13, 2018), available at https://www.npr.org/2018/07/13/628998843 maryland-investigates-russian-nationals-links-to-state-elections-.  

5
Furthermore, the Resolution builds on and is consistent with the election infrastructure created by Congress in the Help America Vote Act of 2002 (HAVA). HAVA established the Election Assistance Commission (“EAC”), a federal body charged with certifying voting systems and allocating HAVA funds. The Federal Election Commission (FEC) is involved in the financing of federal elections. The EAC was mandated to develop and adopt new voluntary voting system guidelines and to provide for the testing, certification, and decertification of voting systems. HAVA also established the Technical Guidelines Development Committee (TGDC) with the duty of assisting the EAC in the development of the new guidelines. The Director of NIST chairs the TGDC, and NIST was tasked to provide technical support for its work.

The U.S. Department of Homeland Security (DHS) partners with federal, state and local government agencies, election officials, and private sector entities to enhance the security of election systems. Election infrastructure was designated as part of the nation’s critical infrastructure as a subsector under the Government Facilities sector in January 2017. Under the designation, DHS, through its Cybersecurity and Infrastructure Security Agency (CISA), is tasked with providing services to state and local election officials that can help reduce both cyber and physical risks to their election systems and facilities. The designation allows DHS to provide services on a prioritized basis at the request of state and local election officials.

**NIST Plays a Key Role in Cybersecurity and Elections**

Beginning over 30 years ago, NIST has been the federal agency designated by Congress to develop technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information systems. Over the years, the agency’s mandate has been broadened by Congress to focus on specific

---

16 According to DHS, Election Infrastructure includes but is not limited to:  
- Voter registration databases and associated IT systems  
- IT infrastructure and systems used to manage elections (such as the counting, auditing and displaying of election results, and post-election reporting to certify and validate results)  
- Voting systems and associated infrastructure  
- Storage facilities for election and voting system infrastructure  
- Polling places, to include early voting locations  
17 NIST was first designated by Congress in 1987 as the agency (then the National Bureau of Standards) within the federal government responsible for addressing complex technology issues and developing security standards and guidelines for federal computer systems. NIST has developed dozens of authoritative publications pursuant to the Federal Information Security Management Act of 2014 (FISMA), 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283, that made the agency responsible for developing information security standards and guidelines, including minimum requirements for federal systems (excluding some national security systems). As a key element of the FISMA Implementation Project, NIST developed an integrated Risk Management Framework which effectively brings together all of the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies. NIST released version 1.1 of its Cybersecurity Framework in April 2018. The framework was developed with a focus on industries vital to national and economic security and has since proven flexible enough to be adopted voluntarily by large and small companies and organizations across all industry sectors, as well as by federal, state and local governments. https://www.nist.gov/cyberframework.
cybersecurity problems and develop best practices and standards to protect the confidentiality, integrity, and availability of all aspects of computer systems.

With respect to elections, under HAVA, Congress tasked NIST with providing technical support to the TGDC, an EAC Federal Advisory Committee to which the NIST Director serves as Chair, in areas such as the security of computers, computer networks, and computer data storage used in voting systems, methods to detect and prevent fraud, protection of voter privacy, the role of human factors in the design and application of voting systems, and remote access voting, including voting through the Internet.

For more than a decade, as directed by both HAVA and the Military and Overseas Voter Empowerment Act (MOVE), the NIST Voting Program has partnered with the EAC to develop the science, tools, and standards necessary to improve the accuracy, reliability, usability, accessibility, and security of voting equipment used in federal elections for both domestic and overseas voters.

In 2005 the EAC adopted Voluntary Voting System Guidelines (“VVSG” or “Guidelines”) which increased security requirements for voting systems and expanded access for individuals with disabilities to vote privately and independently. Version 1.1 of the Guidelines, published in 2015, made the Guidelines more testable and improved portions of the Guidelines without requiring massive programmatic changes.

Since 2015, NIST, in consultation with the EAC, has been working with a broad array of stakeholders on the next iteration of the Guidelines, entitled Voluntary Voting System Guidelines 2.0. Seven working groups are focusing on the election process (pre-election, election and post-election), technical underpinnings of the Guidelines (cybersecurity, usability and accessibility, and interoperability), and issues related to testing.

The Guidelines are used by accredited testing laboratories as part of both state and national certification processes; by state and local election officials who are evaluating voting systems for potential use in their jurisdictions; and by manufacturers who need to ensure that their products fulfill the requirements so they can be certified.

The VVSG address many aspects of voting systems, including determining system readiness, ballot preparation and election definition, voting and ballot-counting operations, safeguards against system failure and protections against tampering, ensuring the integrity of voted ballots, protecting data during transmission, and auditing. In addition, the Guidelines tackle physical and systems-level security.

IV. ADDRESSING CYBERSECURITY THREATS – PROTECTION OF FEDERAL ELECTIONS

Significant evidence has been published concerning vulnerabilities in voting machines and equipment, and, in fact, aspects of the voting process have been attacked by foreign actors. Immediate steps must be taken to develop a process and standards for

---

certification of voting machines and equipment. Members of Congress introduced a broad range of legislative proposals in the 115th and 116th Congress to address critical election issues19 (please see summary in the General Information Form on page 17 herein). These types of laws are needed to protect the 2020 election and beyond.

Given the significant vulnerabilities in all aspects of the Election Process, the Resolution recognizes that a cybersecurity standard for federal elections must be developed and published. Equally important is the consistent implementation of the standard to strengthen security and integrity throughout the federal election process.

Drawing on the significant work NIST has done on election security since 2005, it is reasonable to recommend that security standards and certification processes be developed and adopted well before the 2022 elections.

The Resolution also asks NIST, as part of its evaluation of the security and integrity of election systems and standards and certification development, to analyze the private sector’s role in election processes and recommend any functions or roles that should be restricted to public sector election personnel to better ensure election security and integrity.

The Resolution focuses on a central problem in election security and integrity that must be addressed in reform of the voting process. Private sector companies have significant roles and responsibilities in elections in every state. Reports that have documented the vulnerabilities and limitations of existing voting machine technology have made it clear that the implementation of new technologies and processes ultimately relies on the companies that design, manufacture, integrate, and support voting machines and the associated technological infrastructure, which have been referred to as the “election technology industry.”20 Third-party vendors have provided the entry point for hackers to target election systems. To the best of our knowledge, most have never undergone a security review.

**Paper Ballots and Post-Election Audits**

Replacing aging, outdated, vulnerable voting machines with voter-verified paper ballots or records for every vote cast is a high priority. The National Academies of Sciences, Engineering, and Medicine’s *Securing the Vote: Protecting American Democracy* recommends that voter-verifiable paper ballots be used everywhere by 2020.21

Paper ballots or paper voting receipts are integral to election security because they provide a physical trail that can be followed if there is any question about the outcome of an election, or more generally, for audits.22 The Resolution restricts funding to election

---

19 For example, the U.S. House of Representatives passed the Securing America’s Voting Equipment (SAVE) Act, H.R.2722, on June 27, 2019. The bill addresses election security through grant programs and requirements for voting systems and paper ballots.


jurisdictions that have adopted requirements for post-election auditing of votes, at least on the level of risk-limiting audits, and make the findings public.

Post-election audits check that voting systems properly counted ballots. Audits involve manually checking a representative sample of paper ballots to confirm that counting software has functioned correctly. Risk-limiting audits, which examine a statistically significant sample of ballots based on the margin of victory, are the state-of-the-art approach.

Secure election systems are chronically underfunded. Adequate funding is needed to support all aspects of the election process, including procuring new voting equipment, as well as programs.

**Funding Restrictions – Well-Established Legislative Approach to Protect Federal Interests in Voting**

The Resolution follows the well-established approach Congress has followed over many years of enacting statutes with funding restrictions that protect federal interests.

Congress has a paramount interest in protecting federal elections and ensuring that they are fair and impartial. Voting is a central aspect of the U.S. Constitution, amendments, and federal laws. Constitutional amendments guarantee and protect the individual's right to, and integrity in, the vote. From landless white men, ex-slaves, free blacks, and women, to the historically disenfranchised, to the present.

---

23 Constitutional Amendments and Voting Laws

Article 1 of the Constitution gave states the responsibility of overseeing elections. Many Constitutional amendments and federal laws to protect voting rights have been passed since then.

**Constitutional Amendments**

- 15th Amendment: gave African American men the right to vote in 1870.
- 19th Amendment: ratified in 1920, gave American women the right to vote.
- 24th Amendment: ratified in 1964, eliminated poll taxes. The tax had been used in some states to keep African Americans from voting in federal elections.
- 26th Amendment: ratified in 1971, lowered the voting age for all elections to 18.

**Federal Voting Rights Laws** – Federal laws passed over the years help protect Americans’ right to vote and make it easier for citizens to exercise that right:

- The [Voting Rights Act of 1965](https://www.gpo.gov/fdsys/pkg/PLAW-103publ281/pdf/PLAW-103publ281.pdf) prohibited voter discrimination based on race, color, or membership in a language minority group. It also required certain places to provide election materials in languages besides English.
- The [Help America Vote Act (HAVA)](https://www.gpo.gov/fdsys/pkg/PLAW-106publ204/pdf/PLAW-106publ204.pdf) of 2002 authorized federal funds for elections. It also created the EAC that helps states comply with HAVA to adopt minimum standards on voter education, registration, and ballots.
women, and the young attaining legal voting age, to immigrants granted U.S. citizenship, the right to freely participate in the electoral process and the right to vote are the bedrock of our democracy.

In addition to voting, federal legislation to establish requirements applicable to state and local entities has been enacted to address a range of issues, including transportation and highway safety – requiring the use of seat belts, setting speed limits and the drinking age – and establishing nutrition standards for public school lunches. In response to passage of these federal laws, states enacted laws to conform with the federal requirements.

The Resolution urges state, local, territorial, and tribal legislatures and governments to protect the security and integrity of U.S. election systems by allocating funding for elections consistent with this Resolution.

Each state’s chief elections official is obligated to protect voter records and statewide voter registration databases. State cybersecurity officials must continually assess the cyber threat horizon and improve election security by promptly addressing the risks.

The Resolution Builds on Leading Reports

The recommendations in the Resolution are sound, building on consensus that has emerged among members of Congress, government officials, and leading organizations as to what must be done to enhance the security of elections. For example, the report by the National Academies of Sciences, Engineering, and Medicine (NAS), *Securing the Vote: Protecting American Democracy* recommends steps the federal government,

---


25 In the early 1970s, Congress withheld federal funding from states that did not enact a maximum speed limit of 55 mph. NCLS Speeding Overview (July 10, 2018), available at http://www.ncsl.org/research/transportation/speeding-overview.aspx

26 In 1984, Congress passed the National Minimum Drinking Age Act, which required states to raise their ages for purchase and public possession of alcohol to 21 by October 1986 or lose 10% of their federal highway funds. By mid-1988, all 50 states and the District of Columbia had raised their purchase ages to 21 (but not Puerto Rico, Guam, or the Virgin Islands). National Conference of State Legislatures (NCLS), Social Host Liability for Underage Drinking Statutes (Mar. 27, 2014), available at http://www.ncsl.org/research/financial-services-and-commerce/social-host-liability-for-underage-drinking-statutes.aspx

27 The federal Healthy, Hunger-Free Kids Act of 2010 required the U.S. Department of Agriculture (USDA) to update nutrition standards for school meals based on the 2010 Dietary Guidelines for Americans. The Act also requires each school district participating in a federal food program to implement a local school wellness policy with nutrition and physical activity goals for all schools under its jurisdiction. State Action – States have enacted various types of legislation to support these programs, including creating statewide programs and task forces, appropriating funding, creating grant programs and encouraging school gardens.

28 A summary of government and private sector recommendations and reports concerning election security and reform is included at this link.

29 NAS, *Securing the Vote: Protecting American Democracy*, supra note 19.
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.

V. REFORMS REQUIRED FOR THE 2020 ELECTION AND BEYOND

Frameworks, Standards, And Best Practices
Election officials have little time to prepare for the 2020 elections. While cybersecurity challenges may seem daunting, they can leverage existing frameworks, standards, and best practices that provide a roadmap to reduce the risks to election systems substantially. The NIST Cybersecurity Framework enables organizations to apply the principles and best practices of risk management to improve the security, integrity and resilience of election systems. States have legislation and policies to secure the voting process. The DHS Cybersecurity and Infrastructure Security Agency (CISA) published Best Practices for Securing Election Systems in May 2019. This guidance, which can be

---

implemented at little or no cost, focuses on these important steps election organizations can take to harden their enterprise networks and strengthen election infrastructure: software and patch management; log management; network segmentation; block suspicious activity; credential management; baseline for host and network activity; organization-wide information technology guidance and policies; and notice and consent banners for computer systems.

Videos developed by the Federal Bureau of Investigation (FBI) for the Protected Voices initiative address the most urgent cybersecurity issues that may leave a political campaign or other election organization’s computer networks vulnerable to attacks. The EAC has published checklists for election officials on important election security topics. In this time of scarce resources, it is important to prioritize security resources so the most critical and vulnerable aspects of election systems are addressed first. Focusing on the most common attacks such as phishing, ransomware, and stolen credentials, as well as known vulnerabilities in websites, databases, and servers that can put VRDB at risk is critical. Election officials should not purchase or implement devices, software, or systems with known vulnerabilities. The procurement process is an opportunity to strengthen election security by specifying cybersecurity requirements that third-party vendors must meet.

VI. EXISTING ABA POLICY

Since 1989, the ABA House of Delegates and the ABA Board of Governors have passed Resolutions and adopted policies to strengthen the election process. The ABA has also adopted several policies regarding cybersecurity and lawyers’ use of technology. This Resolution builds on and is consistent with those existing ABA policies, while also taking a more comprehensive approach to the recent emerging threats to election security.

These ABA policies include the following:

Adopts Election Administration Guidelines and Commentary, dated August 2005, to supplant the Ballot Integrity Standards Applying to Election Officials, dated August 1989, and the Election Administration Guidelines and Commentary, dated August 2001, and recommends that all election officials ensure the integrity of the election process through the adoption, use and enforcement of these Guidelines. Urges federal, state, local and on the following topics: election-specific guidance, and patch management, ransomware, password, and enterprise best practices.


territorial governments to provide state and local election authorities with adequate funding in order to ensure the integrity and efficiency of the electoral process. 05A102; amended 08A119A; amended 09A116

Supports state and federal initiatives to modernize and improve voter registration practices, databases and networks and urges an independent technical and security assessment of statewide voter registration databases as well as supporting efforts to achieve ongoing improvements to such databases. Delegation to a federal agency with expertise in technical standards the duty to specify minimum, uniform technical, security including defense-in-depth, and privacy standards and reporting for statewide voter registration systems, including the certification of database software, provided that a State may exceed such minimum standards. 10A114

Supports technological improvements to provide statewide database access in real time to all polling places. 13A110

Urges states, localities and territories to develop written contingency plans detailing what should be done to preserve the election process in the event of an emergency. 14A112B

Supports efforts to improve voter registration practices by a) ensuring the accuracy of voter registration rolls using existing government lists or databases and b) streamlining the procedures whereby changes in voter rolls and voter registration information are made. Urges commitment by states and local election jurisdictions to develop the necessary compatible technology and resources to improve their voter registration practices. Urges federal legislation or administrative action creating incentives to encourage election jurisdictions to adopt the above improvements. 11A121

Urges review of laws related to election and campaign activity on the Internet and application of those laws in a manner that does not discourage political activity through this medium, upholds First Amendment guarantees of free speech and association, and seeks to eliminate opportunities for unfairness, corruption or undue influence through the use of this medium. Urges appropriate steps to encourage and facilitate the use of the Internet by all segments of society in order to promote widespread, fair and equitable citizen participation in the political process. Urge five specified actions to promote the availability and reliability of political information and discourse on the Internet. 00A107

VII. CONCLUSION

This Resolution provides recommendations for essential steps that should be taken by Congress, state and local governments, election officials, and private sector entities to secure the Election Process.

Respectfully Submitted,

Martha Chumbler, Chair, State and Local Government Law Section
Julie Fleming, Chair, Science & Technology Law Section
Ruth Hill Bro and Thomas J. Smedinghoff, Co-Chairs, ABA Cybersecurity Legal Task Force
February 2020
GENERAL INFORMATION FORM

Submitting Entities:  
Section of State and Local Government Law  
Section of Science & Technology Law  
ABA Cybersecurity Legal Task Force

Submitted By:  
Martha Chumbler, Chair, State and Local Government Law Section  
Julie Fleming, Chair, Science & Technology Law Section  
Ruth Hill Bro and Thomas J. Smedinghoff, Co-Chairs, ABA Cybersecurity Legal Task Force

1. Summary of Resolution(s).

The Resolution identifies essential steps that should be taken by Congress, state and local governments, election officials, and private sector entities to secure the “election process” in federal elections. It consists of three measures designed to address the problem of federal election security and integrity head-on – by leveraging the power of Congress to protect federal elections when appropriating federal funds, drawing on the expertise of NIST (the federal agency designated by Congress to address complex technology issues and develop appropriate cybersecurity standards and certification processes), and recognizing the central role of states and local election officials to conduct federal, as well as state and local elections.

2. Approval by Submitting Entities.

The State and Local Government Law Section voted to sponsor this Resolution on November 20, 2019.

The Science & Technology Law Section voted to sponsor this Resolution on December 18, 2019.

The Section of Civil Rights and Social Justice voted to co-sponsor this Resolution on October 27, 2019.

The Criminal Justice Section voted to co-sponsor this Resolution on December 19, 2019.

The Senior Lawyers Division voted to co-sponsor this Resolution on November 14, 2019.

The Standing Committee on Election Law voted to co-sponsor this Resolution on October 16, 2019.

The Cybersecurity Legal Task Force voted to sponsor this Resolution on November 20, 2019.

3. Has this or a similar resolution been submitted to the House or Board previously?  
No.

4. What existing Association policies are relevant to this resolution and how would they be affected by its adoption?
Since 1989, the ABA House of Delegates and the ABA Board of Governors have passed Resolutions and adopted policies to strengthen the election process. The ABA has also adopted several policies regarding cybersecurity and lawyers’ use of technology. This Resolution builds on and is consistent with those existing ABA policies, while also taking a more comprehensive approach to the most recent emerging threats to election security. These policies include:

- **Address chronic underfunding of elections** - *ABA Election Administration Guidelines, 7.2 Ballot Machinery*

- **Enhance cybersecurity protection of election systems**
  - Secure voter registration systems and e-pollbooks - 13A110
  - Replace outdated voting machines and databases - 13A110
  - ABA Election Administration Guidelines - 11A121
  - Develop security standards for voting equipment and infrastructure - 10A114
  - ABA Election Administration Guidelines: 7.2 Ballot Machinery, 7.3 Pre-Vote Checking

- **Develop the capacity to respond to and recover from cyber incidents** - 14A112B

- **Enhance cybersecurity resources and expertise, and increase training** - Resolution 109 (2014)
- **Increase resilience and ensure any attacks are detectable—use voter-verified paper ballots**
- **ABA Election Administration Guidelines: 7.2 Ballot Machinery**
- **Conduct post-election audits—audit the paper trail to high confidence**
  - ABA Election Administration Guidelines -7.7 Ballot Audit, 7.8 Physical Security of Ballots and Voting Equipment
- **Expand and learn from coordinated information sharing** - Policy Adopted by the ABA Board of Governors (Nov. 2012):

  [http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cyber_security_res_and_report.authcheckdam.pdf](http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cyber_security_res_and_report.authcheckdam.pdf)

5. **What urgency exists which requires action at this meeting of the House?**

On Election Day 2019 in a joint statement, government leaders of the law enforcement, homeland security and intelligence communities provided observations
on election security and their outlook for the 2020 elections: They concluded that "[o]ur adversaries want to undermine our democratic institutions, influence public sentiment and affect government policies. Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process or influence voter perceptions."

6. Status of Legislation. (If applicable)
A summary of election security legislation proposed by members the United States Congress is set forth below.

National Defense Authorization Act for Fiscal Year 2020
Conference Report to Accompany S. 1790,

Title LXV—Election Matters

Companion bill: S. 2035, 115th Congress (James Lankford (R-OK), Amy Klobuchar (D-MN), Lindsey Graham (R-SC), Kamala Harris (D-CA), Susan Collins (R-ME), and Martin Heinrich (D-NM))

For the People Act, HR. 1, 116th Congress – “Make It Easier, Not Harder, to Vote”

Election Security Act, S. 2261, 115th Congress (James Lankford (R-OK), Amy Klobuchar (D-MN), Lindsey Graham (R-SC), Kamala Harris (D-CA), Susan Collins (R-ME), and Martin Heinrich (D-NM))


Honest Ads Act – S. 1989, 115th Congress (Mark Warner (D-VA), Amy Klobuchar (D-MV), John McCain (R-AZ))

Defending Elections from Threats by Establishing Redlines (DETER) Act. (Marco Rubio (R-FL) and Chris Van Hollen (D-MD))

Defending American Security from Kremlin Aggression Act (DASKA) of 2019 – S. 482, 116th Congress (Bob Menendez (D-N.J.), Lindsey Graham (R-S.C.), Cory

Foreign Influence Reporting in Election (FIRE) Act, S. 1562

7. Brief explanation regarding plans for implementation of the policy, if adopted by the House of Delegates.

The Resolution will be distributed to members of Congress and private and public sector organizations, and other stakeholders in order to alert them to the ABA’s newly-adopted policy and encourage them to take action consistent with the ABA policy.

8. Cost to the Association. (Both direct and indirect costs), None.


10. Referrals.

Section of State and Local Government Law
Science & Technology Law Section
ABA Cybersecurity Legal Task Force
Antitrust Law Section
Criminal Justice Section
Section on Civil Rights and Social Justice
Business Law Section
Infrastructure and Regulated Industries Section
Section of Public Contract Law
Section of Intellectual Property Law
Section of Litigation
Section of Environment
Energy, and Resources
Section of Administrative Law and Regulatory Practice
Section of International Law
Tort Trial and Insurance Practice Section
Standing Committees:
Law and National Security
Disaster Response and Preparedness
Technology and Information Systems
Lawyers’ Professional Liability
Center for Professional Responsibility
Solo, Small Firm, and General Practice Division
Judicial Division
Law Practice Division
Law Student Division
Young Lawyers Division
11. Contact Name and Address Information. (Prior to the meeting)

Lucy Thomson, Livingston PLLC, Washington, D.C.
lucythomson1@mindspring.com
(703) 798-1001

Jody Westby, Global Cyber Risk, Washington, D.C.
westby@globalcyberrisk.com
(202) 337-0097

David Wheeler, Chapman Spingola, Chicago, Illinois
dwheeler@chapmanspingola.com
(312) 606-8657

Ruth Hill Bro
Co-Chair, ABA Cybersecurity Legal Task Force
(630) 926-1273 (cell)

Thomas J. Smedinghoff
Co-Chair, ABA Cybersecurity Legal Task Force
(312) 545-1333 (cell)

12. Contact Name and Address Information. (Who will present the report to the House?)

Lucy Thomson, Livingston PLLC, Washington, D.C.
Lucythomson1@mindspring.com
(703) 798-1001
EXECUTIVE SUMMARY

1. Summary of the Resolution
   The Resolution identifies essential steps that should be taken by Congress, state
   and local governments, election officials, and private sector entities to secure the
   “election process” for federal elections. It consists of three measures designed to
   address the problem of election security head-on – by leveraging the power of
   Congress to protect federal elections when appropriating federal funds, drawing
   on the expertise of NIST (the federal agency designated by Congress to address
   complex technology issues and develop appropriate cybersecurity standards and
   certification processes), and recognizing the central role of states and local
   election officials to conduct federal, as well as state and local elections.

2. Summary of the Issue that the Resolution Addresses
   Volumes of evidence establish that Russian cyber operations targeted election
   infrastructure in the U.S. in order to undermine the integrity and availability of the
   2016 elections. Russia is the largest, but not the only threat. U.S. intelligence
   agencies and law enforcement have expressed concern “about ongoing
   campaigns by Russia, China and other foreign actors, including Iran, to undermine
   confidence in democratic institutions and influence public sentiment and
   government policies. The risk of foreign interference in U.S. elections remains at
   critical levels.

2. Please Explain How the Proposed Policy Position Will Address the Issue
   The Resolution identifies essential steps that should be taken by Congress, state
   and local governments, election officials, and private sector entities to secure the
   “Election Process.” It consists of three measures designed to address the problem
   of election security head-on – by leveraging the power of Congress to protect
   federal elections when appropriating federal funds, drawing on the expertise of
   NIST (the federal agency designated by Congress to address complex technology
   issues and develop appropriate cybersecurity standards and certification
   processes), and recognizing the central role of states and local election officials to
   conduct federal, as well as state and local elections.

4. Summary of Minority Views
   No minority views have come to our attention with respect to this Resolution and
   Report.