RESOLUTION

RESOLVED, That the American Bar Association urges federal, state, local, territorial and tribal legislatures and government agencies to provide the funding necessary to develop, implement, and maintain appropriate cybersecurity programs for the courts and to train court personnel on methods to counter threats and protect judicial information systems from cyber intrusions or data breaches.
REPORT

I. INTRODUCTION

This Resolution focuses on cybersecurity threats that affect the judicial system and may pose a risk to the fair and efficient administration of justice. It urges federal, state, local, tribal and territorial legislatures and government agencies to provide the funding necessary to develop, implement, and maintain appropriate cybersecurity programs for the courts and to train court personnel on methods to counter threats and protect judicial information systems from cyber intrusions or data breaches.

The ABA Resolution is based upon the recognition that adequate funding and training are necessary to protect the public’s interest in the integrity of the courts and the data they hold. Such funding and training should enable the courts to perform a number of important tasks, including the conduct of regular risk assessments of each court’s information security program; updates to security controls; continuous vulnerability monitoring; the development and testing of comprehensive incident response and business continuity/disaster recovery (BC/DR) plans; and the sharing of cyber threat information among the courts and the legal community.

Over the years, the ABA House of Delegates has adopted a number of Resolutions sponsored by the ABA Cybersecurity Legal Task Force and the Section of Science & Technology Law that address cybersecurity threats and urge organizations to follow best practices to address them. In addition, the ABA has adopted Resolutions that address threats within courthouses and are directed toward participants in the judicial system, and any actual or perceived threat that may impede or interfere with access to the justice system and are also a threat to the fair and efficient administration of justice. The ABA has not adopted any policy that addresses the need for funding to develop, implement, and maintain an appropriate cybersecurity program for the courts.

From a security perspective, the courts in recent years have provided resources for building security. For example, the National Center for State Courts (NCSC) has been in the forefront of courthouse building security—a number of highly-publicized incidents of violence in courthouses around the country focused attention on this problem and best practices have been developed to address it. Now, as the courts modernize their information systems, adequate funding will be required to develop, implement, and maintain an appropriate cybersecurity program, assess the threats to those systems, and protect the volumes of confidential and sensitive data that the courts collect, use, store, and share.

1 The NCSC has conducted extensive research on the causes and prevention of court building violence and published Steps to Best Practices for Court Building Security (“Steps to Best Practices”), available at http://www.ncsc.org/services-and-experts/areas-of-expertise/~/media/Files/PDF/Services%20and%20Experts/Areas%20of%20Expertise/Emergency%20Preparedness/Safety_BestPractices_%20Steps_to_Best_Practices.aashx. These best practices represent collaboration with the Center for Judicial and Executive Security (“CJES”) in St. Paul, Minnesota, and the administrative offices of the courts of several states. NCSC encourages the leadership of every court building to strive to achieve and maintain best practices in every area identified in their publication so that every person who works in or visits a court building may do so in the safest environment possible.
As with all organizations, courts must remain forward-looking in managing their cybersecurity program. The threat environment, operational requirements, and innovation are constantly changing. This requires regular assessments of cybersecurity programs, evaluations of the effectiveness of controls and deployed technologies, and adjustments where necessary to maintain a strong security posture. This process necessarily involves a review of funding needs for the security program and updated training.

This is a particularly urgent need for state courts, many of which report having insufficient security budgets. The 2014 Deloitte-NASCIO study emphasized that the cybersecurity landscape for state government is a complex and challenging one, and concluded that unless deliberate action is taken, budgets will continue to be a challenge as cybersecurity threats mount.²

ABA has been an active proponent of adequate court funding. This Resolution builds on the ABA Resolutions adopted over the past decade that urge governments to provide adequate funding for the courts to ensure their security. As cybersecurity threats grow, the need for adequate funding for the courts to address these risks becomes critically important.

### II. COURT TECHNOLOGY INITIATIVES

Courts at the federal, state, and local levels are embracing a variety of new technologies; many courts have undertaken important initiatives to modernize their information systems, measures that are designed to facilitate access, openness and transparency, increase efficiency, and reduce costs. These initiatives are vitally important to the cause of justice because they can make the courts more accessible and affordable to a diverse body of litigants. The NCSC website provides a summary of technology developments in state courts over the past decade.³ Important federal and state court technology initiatives are highlighted below.

In the 2014 Year-End Report on the Federal Judiciary, Chief Justice John Roberts announced that the U.S. Supreme Court will launch an online case filing system in 2016.⁴ Once the system is implemented, all filings at the Court—petitions and responses to petitions, merits briefs, and all other types of motions and applications—will be available to the legal community and the public without cost on the Court’s website.⁵

**Electronic Case Filing and Case Management** (CM/ECF)⁶—The courts have deployed new technologies to automate the filing, acceptance, and retrieval of the vast inflow of litigation documents that reach the courts every day. More than 600,000 attorneys have filed case documents using CM/ECF, and they currently file electronically more than 2.5 million documents each month. This system is not limited to attorneys. By logging onto the Public

---

⁵ Id. at 9.
Access to Court Electronic Records (PACER) system, members of the public can instantly access and review federal court filings located in courthouses across the Nation.7

“Next Gen” CM/ECF—The national roll out of the Next Generation of the CM/ECF has begun in the U.S. courts of appeals. It is designed to increase chambers’ and clerks’ office efficiency and, when fully implemented, will provide a single sign-on that will allow court users and attorneys to file and retrieve information in any federal court using the same login and password, greatly simplifying access to the system. Testing in district and bankruptcy courts will begin in 2015.

Courtroom Modernization—The federal judiciary has likewise modernized courtrooms to take advantage of technological innovations in exchanging information and ideas. Attorneys can rely on computer-assisted graphics, video, and other technological aids to introduce evidence and facilitate communications with judges and juries.

Video conferencing of court hearings is used to save costs and improve security in some situations by eliminating the need to transport prisoners and making it easier to allow victims and child witnesses to testify. Judges use it to conduct hearings remotely.

Computer-assisted legal research has been integrated into the case resolution process. Courts now have access to extensive legal databases and can quickly locate relevant authority through search commands on desktop computers, tablets, and mobile devices.

Integrated Workplace Initiative (IWI)— While the impetus for the IWI was to reduce the judiciary’s real estate footprint, courts are creating a better and more efficient workplace environment by capitalizing on the flexibility that new and emerging technologies provide. IWI examines how court units work, researches work style changes, and identifies successful mobile working situations, for example, where probation officers work remotely in the field rather than in the courthouse.

eVoucher—An automated system for processing and managing vouchers submitted by lawyers appointed to represent indigents under the Criminal Justice Act was developed by the District of Nevada. Through a collaborative effort, the eVoucher system is being adopted for national use and shared with courts throughout the country.

Other systems are being developed to assist litigants, jurors, and members of the public, including:

- Online jury services support
- Centralized and automated payable processes
- Virtual self-help centers to assist self-represented litigants

Additional technology changes are expected in the coming years to enhance court services.

Electronic Discovery—Amendments to the Federal Rules of Civil Procedures have spurred the transformation of litigation through e-discovery.8 e-Discovery has resulted in the transfer of

---


8
huge amounts of confidential and sensitive data from companies and other organizations to the courts, law firms, technology companies, and other third party outsourcing entities.

**Governments Are Going Paperless**—The federal government and the states are transitioning from print-only publishing to either an environment in which legal materials, including judicial decisions and legislation, are published in a mix of formats or one in which legal material are published in electronic format only. To address these developments, the Uniform Law Commission adopted the Uniform Electronic Legal Material Act (UELMA), a model state law that provides for authentication of legal material, and preservation and archiving of this material for the future. This transition creates an immediate need for all federal, state and local courts to protect their electronic records. At the federal level, the Government Publication Office (GPO) is developing best practices for authentication of official documents.  

III. TECHNOLOGY CHALLENGES

**Sensitive Data at Risk**

Litigation often involves sensitive matters: criminal prosecutions, bankruptcy petitions, malpractice suits, discrimination cases, and patent disputes may all lead to the collection of confidential information that should be shielded from public view to protect the safety of witnesses, the privacy of litigants, and the integrity of the adjudicatory process.  

--Chief Justice John Roberts, U.S. Supreme Court (2014)

With the opportunities presented by information technology come many challenges and risks that the courts must address. As courts modernize many aspects of their operations, their information systems are becoming interconnected and users are now able to access court services through the Internet. In today’s digital world, threats to data and information systems are found almost everywhere a computer, server, smart phone, thumb drive, or other electronic device is operating (including the cloud). The proliferation of mobile devices and wireless technologies present vulnerable points in the flow of sensitive data in computer networks. Services are provided and documents are stored in the cloud. These developments present cybersecurity issues that must be assessed and taken into consideration as the courts determine their funding requirements for court security.

**Law Offices, Governments, and the Courts Are Targets of Cyber Attacks**

The recent highly-publicized data breaches of leading retail companies, health insurers, and government agencies have caught the attention of the public, politicians, and law enforcement.

---

The indictment of a Russian national charged in the largest known data breach prosecution provides details of attack methodology used by hackers in several of the largest data breaches.\textsuperscript{11} A website that goes by the name “information is beautiful” provides a visualization of hundreds of the major data breaches over the past decade and serves as a useful resource to identify and learn about the massive data breaches that have affected the private sector and government.\textsuperscript{12}

Similarly, the courts have suffered data breaches. For example, more than one million driver's license numbers and 160,000 Social Security numbers (SSN) were accessed in a data breach at the Washington State Administrative Office of the Courts' website.\textsuperscript{13} Citizens booked at a city or county jail, or with a traffic case in a district or municipal court through 2012, or anyone with a DUI citation in the state going back to 1989, may have had their data compromised. The courts have since taken steps to enhance their online security.

It is believed that hackers launched a successful denial-of-service attack against the PACER system that shut down online access for several hours in January 2014.\textsuperscript{14} Also uscourts.gov and various other federal court websites around the country were affected. The U.S. Court of Appeals website in the Middle District of Florida was also not available for an entire afternoon; no one could file or retrieve documents. A spokesperson for the Administrative Office of the U.S. Courts suggested that the outage was the result of a malicious attack, and the European Cyber Army claimed responsibility in a Twitter message.\textsuperscript{15}

The Florida Department of Juvenile Justice (DJJ) reported the theft of a mobile device containing youth and employee records in January 2011. The Tallahassee Police Department (TPD) was responsible for investigating the theft. The device, which was stolen from a secure DJJ office, was not encrypted or password-protected as required by DJJ’s technology policy.\textsuperscript{16}

Both large and small law firms have been the target of hacker attacks in the U.S. as well as abroad. The \textit{ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals} (2013) provides details about the threat landscape of legal organizations. The FBI

\begin{footnotesize}
\textsuperscript{11} United States v. Drinkman, et. al., No. 09-626 (JBS) (S-2) (D. N.J.) available at http://www.justice.gov/sites/default/files/op/press-releases/attachments/2015/02/18/drinkman_vladimir_et_al_indictment_comp.pdf (second superseding indictment); http://www.justice.gov/op/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states (February 18, 2015). "This case reflects the cutting-edge problems posed by today's cybercrime cases, where the hackers didn't target just a single company; they infiltrated most of the country's email distribution firms," said Acting U.S. Attorney John Horn in Atlanta. "And the scope of the intrusion is unnerving, in that the hackers didn't stop after stealing the companies' proprietary data—they then hijacked the companies' own distribution platforms to send out bulk emails and reaped the profits from email traffic directed to specific websites."

\textsuperscript{12} http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.


\end{footnotesize}
has issued warnings to firms and held a meeting in early 2012 with approximately 200 law firms in New York City to discuss the risk of breaches and theft of client data.\textsuperscript{17} A cybersecurity firm that helps organizations secure their networks against threats and resolve computer security incidents estimated that 80 major law firms were breached in 2011 alone.\textsuperscript{18}

Hackers targeted law enforcement officers from 70 different U.S. law enforcement agencies.\textsuperscript{19} In August 2011 hackers associated with Anonymous and the disbanded hacktivist group LulzSec published 10 GB of personal data of law officers, including thousands of SSNs and dozens of bank account numbers. Security firm Identity Finder CEO Todd Feinman, who disclosed this breach, characterized it as a “staggering amount of personal data that could cause identity theft problems for years to come.”\textsuperscript{20}

**Privacy Violations**—Personally identifiable information (PII) that can be used for fraud and identity theft is being collected and often stored unprotected, putting many Americans at risk.\textsuperscript{21} PII, including SSN, has been publicly available through court online filing systems, and even published on court websites. There is a vibrant market for these data, and the harm to individuals from identity theft has been well-documented. As just one example, on its website, the Internal Revenue Service (IRS) indicates that it “has seen a significant increase in refund fraud that involves identity thieves who file false claims for refunds by stealing and using someone’s Social Security number.”\textsuperscript{22}

Data breaches of government agencies are occurring with alarming frequency. In the annual report on the Federal Information Security Management Act (FISMA), the Office of Management and Budget (OMB) stated that federal agencies reported nearly 70,000 information security incidents in FY 2014, up 15 percent from FY 2013.\textsuperscript{23} The Government Accountability Office (GAO) found that the number of reported information security incidents involving PII have more than doubled over the last several years.\textsuperscript{24}

In a state government breach, about 1,500 computers in the Massachusetts Office of Labor and Workforce Development were infected with the computer virus that was designed to let an

\begin{itemize}
  \item \textsuperscript{18} Mandiant Intelligence Center Report, APT1: Exposing One of China’s Cyber Espionage Units, page 20, available at http://www.mandiant.com.
  \item \textsuperscript{19} http://www.pcmag.com/article2/0,2817,2390582,00.asp.
  \item \textsuperscript{20} Id.
  \item \textsuperscript{21} For example, a Vietnamese national was indicted recently for allegedly participating in an international scheme to steal and sell hundreds of thousands of Americans’ PII through various websites he operated. United v. Ngo, No. 13-cr-1116 (D.N.H. 2013), available at http://www.justice.gov/opa/pr/2013/October/13-crn-1116.html.
  \item \textsuperscript{24} GAO Federal Agencies Need to Enhance Responses to Data Breaches (April 2, 2014), available at http://www.gao.gov/assets/670/662227.pdf.
\end{itemize}
attacker take control of infected computers and transmit confidential information to the digital thieves. Personal financial information, including names, addresses and SSN of up to 210,000 unemployed Massachusetts residents may have been stolen in the data breach in May 2011. In March 2012 hackers from Eastern Europe illegally accessed a Utah Department of Technology Services (DTS) server containing patients' SSN and data on children's health plans. It is believed that a weak password lead to the breach of about 780,000 patient files of Medicaid claims.

Malware on a San Francisco utilities agency server lead to a data breach of customer names, account numbers, addresses, phone numbers and some e-mail addresses for 180,000 customers. The agency notified customers that hackers used an open port on an unsecured server to infect it with computer viruses. Improper disclosure of sensitive records is a frequent cause of data breaches. In the State of Texas, 3.5 million records were accidentally published online, including names, addresses, SSN, DOB, and driver’s license numbers.

The problem of data breaches will only become more serious in the future as the courts receive increasing amounts of confidential and sensitive data, reflecting a growing trend in data analytics. The sensitive personal data being amassed by companies and governments is staggering. Inexpensive storage has enabled companies to collect and store large amounts of data, and data analytics is driving companies to retain it far longer than they would have if it were in paper. Litigation will reflect these trends, resulting in the presentation of large amounts of critical, highly-valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-discovery.

Security is only as strong as its weakest link. Failed security has resulted in thousands of data breaches that have led to the loss or compromise of millions of personally identifiable records, as well as the theft of classified information, valuable intellectual property and trade secrets, and the compromise of critical infrastructure. In many cases, data breaches or other types of cyber incidents could have been prevented or detected early and the risks of the incident mitigated if the organization had undertaken proper security planning and implemented appropriate security safeguards. The NCSC launched the eCourts 2014 initiative to raise awareness of cyber threats and educate court personnel about the steps they need to take to secure their information systems and sensitive data.

---

25 http://www.mass.gov/lwd/
IV. ABA POLICIES

Cybersecurity

The House of Delegates adopted Resolution 109 during the 2014 Annual Meeting, sponsored by the ABA Cybersecurity Legal Task Force and the Section of Science & Technology Law. Resolution 109 encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected. The Report that accompanies the Resolution identifies accepted frameworks and standards that can serve as a reference for developing, implementing, and maintaining an appropriately-tailored cybersecurity program.

Risk Assessment—Cybersecurity is based on a systematic assessment of risks that are present in a particular operating environment. Risk assessments are undertaken to identify gaps and deficiencies in a cybersecurity program due to operational changes, new compliance requirements, an altered threat environment, or changes in the system architecture and technologies deployed. The National Institute of Standards and Technology (NIST) recently published the Framework for Improving Critical Infrastructure Cybersecurity and mapped the Framework to other accepted security frameworks and standards.30

Risk assessments are the basis for the selection of appropriate security controls and the development of remediation plans so that risks and vulnerabilities are reduced to a reasonable and appropriate level. Administrative, technical, organizational and physical controls help ensure the confidentiality, availability, and integrity of digital assets. Such controls should be carefully determined, implemented, and enforced. NIST has published extensive guidance on the selection of controls for government systems.31

Due to the nature of the threat environment, certain activities in a cybersecurity program are ongoing. Continuous monitoring and log analysis are designed to provide data that can enable the early detection of threats. To maintain a proactive security posture, potential threats should be investigated and targeted attacks detected in advance or addressed as they occur. The objective is to address cybersecurity threats and risks in a timely, disciplined, and structured fashion.

Incident Response and Business Continuity/Disaster Recovery (BC/DR)—Incident response is the practice of detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future reference. Fully developed and tested incident response plans and business continuity/disaster recovery (BC/DR) plans are components of a cybersecurity program. Organizations should be prepared if a cyber attack or data breach occurs or if an event interrupts their operations. Response plans, policies,

and procedures should be able to accommodate the full array of threats, not just data breaches. A cybersecurity incident that is initially handled under an incident response plan may cause a business interruption that requires implementation of business continuity procedures. GAO has recommended key management and operational practices to be included in policies for responding to data breaches of PII.32

The NCSC has focused on the need for emergency planning and response.33

As is the case with most organizations today, data, in electronic as well as hard copy form, have become the life blood of courts. Managing data and files has become an essential court function. [ ] court operations face the risk of disruption that can be caused by many kinds of disasters or emergencies, both man-made and natural. When a disaster disrupts a court’s data system, the court will be hard pressed to discharge even its most basic and essential responsibilities. Therefore, courts must develop plans not only to prevent disruptions to data systems to the maximum extent feasible, but also to recover such systems as soon and as effectively as feasible after a significant disruption occurs.34

**Court Security**

Resolution 106C, adopted by the ABA House of Delegates at the Annual Meeting in 2005, made comprehensive recommendations related to federal court security. This Resolution also made recommendations that related to both the federal and state judiciaries, including urging Internet vendors and government entities to voluntarily remove certain personal information about a judge upon request, urging federal and state government departments and agencies to assess security needs of the administrative adjudication programs within their control, supporting the creation of a National Clearinghouse on Federal and State Court Security to facilitate information sharing, and urging Congress to explore ways to assist state courts with enhancing court security. The Resolution expands the scope of ABA policy on court security to fully encompass state, local, and territorial courts, including urging state, local, and territorial legislative bodies and governmental agencies to adopt laws and policies providing for the development and funding of adequate judicial system security protocols and to take the necessary steps to minimize the impact of court-related violence.

The Resolution further emphasizes the importance of applying principles of judicial administration to court security by recommending that courts engage in a comprehensive review of each court’s respective judicial system security needs, create and regularly review judicial system security protocols that fulfill those needs, and seek the funding necessary to implement those protocols. The Resolution also encourages the development of resources to educate those who participate in the justice system how to identify potential security threats related to the administration of justice, and how to be effective first responders in the event of an incident of violence. This multi-faceted approach was designed to enhance court security for all participants, promote fair and impartial courts, and increase public confidence in the judicial system.

---

34 Id.
Resolution 106C included nine resolved clauses pertaining to court building and judicial security in the federal courts. For example, it urges Congress and the Department of Justice Judicial Security Review Group to review changes to U.S. Marshals Service (USMS) procedures to determine whether security vulnerabilities have been remedied. The Resolution also urges Congress to enact legislation requiring the USMS and the Administrative Office of the United States Courts to consult on a continuing basis, and for Congress and the Department of Justice to consider amending existing laws to strengthen court building and judicial security. Resolution 106C also encourages Congress to include sufficient funds in its annual appropriations for the federal judiciary and the USMS so that existing and additional security measures can be fully and effectively implemented.

A 2004 U.S. Department of Justice Office of the Inspector General Report, Resolution 106C, and numerous congressional hearings led to significant changes that benefit the federal courts. The USMS established the National Center for Judicial Security (NCJS) in fiscal year 2008. The goal of the NCJS is to provide educational, operational, and technical functionality in the areas of security not only to federal courts but to all levels of state courts as well. The USMS also established a Threat Management Center within its Office of Protective Intelligence. The purpose of the Threat Management Center is to provide 24/7 response support and information sharing between the USMS and state and local entities. During the 2012 fiscal year the Threat Management Center investigated and analyzed 1,370 threats and inappropriate communications to those protected by the USMS.36

Court Funding

Ensuring effective court security at the federal, state, and local levels is in many ways related to funding issues. The ABA has been an active proponent of adequate court funding. The Task Force on Preservation of the Justice System (Task Force), under the leadership of past ABA Presidents Stephen N. Zack and Wm. T. (Bill) Robinson III, convened high-profile symposiums, hearings, and programs on the issue of court funding, and sponsored two Resolutions in 2011 and 2013. The House of Delegates adopted Resolution 302 at the 2011 Annual Meeting. Resolution 302 urges state, territorial, and local bar associations to document the impact of funding cutbacks to the justice system and to publicize those impacts so that the public may be informed of the need to support their court systems. Resolution 302 also urges state, territorial, and local governments to provide stable and predictable levels of funding to justice systems. The Task Force also sponsored Resolution 10C which was adopted at the 2013 Annual Meeting. Resolution 10C urges legislative bodies and governmental agencies to adopt laws or policies to ensure full and adequate court funding. Resolution 10C also adopted the Principles for Judicial Administration, promulgated by NCSC and adopted by CCJ in an effort to assist courts in their efforts to restructure court services and secure adequate funding.

The introduction to the Principles for Judicial Administration states that “[j]udicial leaders have the responsibility to demonstrate what funding level is necessary and to establish administrative

structures and management processes that demonstrate they are using the taxpayers’ money wisely.”

Reflecting that responsibility, this Resolution urges courts to create and review judicial system security protocols on a regular basis. The author urges courts to be proactive in assessing the needs and effectiveness of their judicial security systems so that they may effectively communicate with appropriators and policymakers. As the commentary to Principle 18 explains, “[t]he court management team is in the best position to know what resources are needed to fulfill its constitutional mandate and how best to present and justify its needs for those resources.” The proactive assessment of security needs is not only a vital component towards effective communication with appropriators, but is also crucial to the preservation of courts as a separate and co-equal branch of government.

Principle 22 directly addresses the issue of court security, stating that “[r]esponsible funding entities should ensure that courts have facilities that are safe, secure and accessible and which are designed, built and maintained according to adopted courthouse facility guidelines.” Courts must examine existing national standards, including the resources discussed above, to determine how best to implement principle 22 in their jurisdictions. Every individual who interacts with the court must have access to proceedings in a safe environment. Adequate court funding is a necessary component in this endeavor. Principle 23 focuses on the importance of technology to provide required security, stating “the court system should be funded to provide technologies needed for the courts to operate efficiently and effectively and to provide the public services comparable to those provided by the other branches of government and private businesses.”

V. ABA POLICIES—SUMMARY

This section provides a list of ABA policies related to cybersecurity, court security, and court funding, with a brief summary and citation for each policy.

Cybersecurity

In recent years, the ABA House of Delegates and Board of Governors have adopted several policies regarding cybersecurity and lawyers’ use of technology, and the proposed Resolution is consistent with those existing ABA policies. These ABA policies include the following:

**Resolution 109, Adopted by the House of Delegates at the 2014 Annual Meeting in Boston (August 2014)**

Resolution 109, which was sponsored by the Cybersecurity Legal Task Force and the Section of Science & Technology Law, encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature

---


38 *Id.* at 15 (Principle 18 states “Judicial Branch budget requests should be considered by legislative bodies as submitted by the Judicial Branch.”).

39 *See Principles for Judicial Administration* at 4 (“Court leaders, whether state or local, should exercise management control over all resources that support judicial services within their jurisdiction.”).
and scope of the organization, and the data and systems to be protected.

The Resolution and Report are available at:


* * *

Resolution 118, Adopted by the House of Delegates at the 2013 Annual Meeting in San Francisco (August 2013)

This Resolution condemns intrusions into computer systems and networks utilized by lawyers and law firms, urges federal, state, and other governmental bodies to examine and amend existing laws to fight such intrusions, and makes other related recommendations.

The Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf

* * *

Policy Adopted by the ABA Board of Governors (November 2012)

The ABA Board of Governors approved a policy in November 2012 comprised of five cybersecurity principles developed by the ABA Cybersecurity Legal Task Force.

The Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cybersecurity_res_and_report.authcheckdam.pdf

* * *

Resolutions 105 A, B and C, Adopted by the House of Delegates at the 2012 Annual Meeting in Chicago (August 2012)

Resolution 105A amends the black letter and Comments to Model Rule 1.0 (Terminology), the Comments to Model Rule 1.1 (Competence) and Model Rule 1.4 (Communication), and the black letter and Comments to Model Rule 1.6 (Confidentiality of Information) and Model Rule 4.4 (Respect for Rights of Third Parties) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and confidentiality. Resolution 105B amends the black letter and Comments to Model Rules 1.18 and 7.3, and the Comments to Model Rules 7.1, 7.2 and 5.5 of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and client development.
Resolution 105C amends the Comments to Model Rule 1.1 (Competence) and Model Rule 5.5 (Unauthorized Practice of Law; Multijurisdictional Practice of Law), and the title and Comments to Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding the ethical implications of retaining lawyers and nonlawyers outside the firm to work on client matters (i.e., outsourcing).

The Resolutions and Reports are available at:

http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105a.doc

http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_105b.authcheckdam.pdf

http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105c.doc

**Court Security**

Resolution 106C, Adopted by the House of Delegates at the 2005 Annual Meeting in Chicago (August 2005)

Resolution 106C made comprehensive recommendations related to federal court security. It includes nine resolved clauses pertaining to court building and judicial security in the federal courts.

The Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/directories/policy/2005_am_106c.authcheckdam.pdf

**Court Funding**

Resolution 302, Adopted by the House of Delegates at the 2011 Annual Meeting in Toronto, Canada (August 2011)

Resolution 302 urges state, territorial, and local bar associations to document the impact of funding cutbacks to the justice system and to publicize those impacts so that the public may be informed of the need to support their court systems; and urges state, territorial, and local governments to provide stable and predictable levels of funding to justice systems.
The Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/administrative/tips/Court%20Funding/2011%20Annual%20Resolution%2010C.authcheckdam.pdf

Resolution 10C, Adopted by the House of Delegates at the 2013 Annual Meeting in San Francisco, CA (August 2013)

This Resolution urges legislative bodies and governmental agencies to adopt laws or policies to ensure full and adequate court funding. It also adopted the Principles for Judicial Administration, promulgated by NCSC and adopted by CCJ in an effort to assist courts in their efforts to restructure court services and secure adequate funding.

The Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/administrative/tips/Court%20Funding/2013%20Annual%20Resolution%2010C.authcheckdam.pdf

VI. CONCLUSION

This Resolution focuses on cybersecurity threats that affect the judicial system and may pose a risk to the fair and efficient administration of justice. Now, as the courts modernize their information systems, adequate funding will be required to develop, implement, and maintain an appropriate cybersecurity program, assess the threats to those systems, and protect the volumes of confidential and sensitive data that the courts collect, use, store, and share. This Resolution builds on the ABA Resolutions adopted over the past decade that urge governments to provide adequate funding for the courts to ensure their security. As cybersecurity threats grow, the need for adequate funding for the courts to address these risks becomes critically important. The adoption of this Resolution will enhance court cybersecurity and promote fair and impartial courts.

Respectfully Submitted,

Judith Miller
Harvey Rishikof
Co-Chairs, ABA Cybersecurity Legal Task Force

August 2015
GENERAL INFORMATION FORM

Submitting Entity: ABA Cybersecurity Legal Task Force

Submitted By: Judith Miller and Harvey Rishikof, Co-Chairs
ABA Cybersecurity Legal Task Force

1. Summary of Resolution.

This Resolution focuses on cybersecurity threats that affect the judicial system and may pose a risk to the fair and efficient administration of justice. Now, as the courts modernize their information systems, adequate funding will be required to assess the threats to those systems, and protect the volumes of confidential and sensitive data that reside in the courts. This Resolution builds on the ABA resolutions adopted over the past decade that urge governments to provide adequate funding for the courts to ensure their security. As cybersecurity threats grow, the need for adequate funding for the courts to address these risks becomes critically important. The adoption of this Resolution will enhance court security and promote fair and impartial courts.

2. Approval by Submitting Entities.

The Cybersecurity Legal Task Force approved the Resolution on April 10, 2015.

The Section of Science & Technology Law voted to co-sponsor this Resolution by email vote of the Section Council (in accordance with the Section Bylaws) on April 29, 2015; the Criminal Justice Section voted to co-sponsor this Resolution by vote of the Section Council on April 25, 2015; the International Law Section voted to co-sponsor this Resolution by vote of the Section Council on May 1, 2015; the Judicial Division voted to co-sponsor this Resolution by vote of the Section Council on May 5, 2015; the Environment, Energy and Resources Section voted to co-sponsor this Resolution by vote of the Section Council on May 8, 2015; the Standing Committee on Law and National Security voted to co-sponsor this Resolution by vote of the Committee Council on May 16, 2015; and the Standing Committee on Technology and Information Systems voted to cosponsor this Resolution by vote of the Committee Council on May 21, 2015.

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?

ABA voted to support the Uniform Law Commission’s Uniform Electronic Legal Material Act (UELMA) on February 6, 2012.

The proposed Resolution is consistent with, and would build upon, several existing ABA policies, including the following:
Resolution 118, Adopted by the House of Delegates at the 2013 Annual Meeting in San Francisco (August 2013)

This Resolution condemns intrusions into computer systems and networks utilized by lawyers and law firm, urges federal, state, and other governmental bodies to examine and amend existing laws to fight such intrusions, and makes other related recommendations.

* * *

Policy Adopted by the ABA Board of Governors (November 2012)

The ABA Board of Governors approved a policy comprised of five cybersecurity principles developed by the ABA Cybersecurity Legal Task Force.

* * *

Resolutions 105 A, B and C, Adopted by the House of Delegates at the 2012 Annual Meeting in Chicago (August 2012)

Resolution 105A amends the black letter and Comments to Model Rule 1.0 (Terminology), the Comments to Model Rule 1.1 (Competence) and Model Rule 1.4 (Communication), and the black letter and Comments to Model Rule 1.6 (Confidentiality of Information) and Model Rule 4.4 (Respect for Rights of Third Parties) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and confidentiality.

Resolution 105B amends the black letter and Comments to Model Rules 1.18 and 7.3, and the Comments to Model Rules 7.1, 7.2 and 5.5 of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and client development.

Resolution 105C amends the Comments to Model Rule 1.1 (Competence) and Model Rule 5.5 (Unauthorized Practice of Law; Multijurisdictional Practice of Law), and the title and Comments to Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding the ethical implications of retaining lawyers and nonlawyers outside the firm to work on client matters (i.e., outsourcing).

Court Security

Resolution 106C, Adopted by the House of Delegates at the 2005 Annual Meeting in Chicago, IL (August 2005)

Resolution 106C made comprehensive recommendations related to federal court security. It includes nine resolved clauses pertaining to court building and judicial security in the federal courts.
Court Funding

Resolution 302, Adopted by the House of Delegates at the 2011 Annual Meeting in Toronto, Canada (August 2011)

Resolution 302 urges state, territorial, and local bar associations to document the impact of funding cutbacks to the justice system and to publicize those impacts so that the public may be informed of the need to support their court systems; and urges state, territorial, and local governments to provide stable and predictable levels of funding to justice systems.

* * *

Resolution 10C, Adopted by the House of Delegates at the 2013 Annual Meeting in San Francisco, CA (August 2013)

This Resolution urges legislative bodies and governmental agencies to adopt laws or policies to ensure full and adequate court funding. It also adopted the Principles for Judicial Administration, promulgated by NCSC and adopted by CCJ in an effort to assist courts in their efforts to restructure court services and secure adequate funding.

5. If this is a late Report, what urgency exists which requires action at this meeting of the House?

Although not a later Report, this Resolution focuses on cybersecurity threats that affect the judicial system and may pose a risk to the fair and efficient administration of justice. The threat environment today is highly sophisticated, and massive data breaches are occurring with alarming frequency. Now, as the courts modernize their information systems, adequate funding will be required to develop, implement, and maintain an appropriate cybersecurity program, assess the threats to those systems, and protect the volumes of confidential and sensitive data that the courts collect, use, store, and share.

The only effective defense is a fully-implemented cybersecurity program with controls based on operational criteria and magnitude of harm and risk categorization. In many cases, data breaches or other types of cyber incidents could have been prevented or detected early and the risks of the incident mitigated if the organization had undertaken proper cybersecurity planning and implemented appropriate security safeguards.

6. Status of Legislation. (If applicable)

Not applicable.

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

The Resolution will be distributed to federal, state, local, tribal and territorial court judges and executives, the U.S. Department of Justice and the U.S. Marshals Service, appropriate
members of federal, state, local, tribal and territorial legislatures and government agencies, and other stakeholders in order to alert them to the ABA’s newly-adopted policy and to encourage them to take action consistent with that policy.

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

9. **Disclosure of Interest.** (If applicable) Not Applicable.

10. **Referrals.**

    The proposed Resolution and Report has been sent to the Chairs and staff liaisons of each ABA Section, Division, Task Force, Standing Committee and Commission represented on the ABA Cybersecurity Legal Task Force. They are: Section of Administrative Law, Business Law, Center for Professional Responsibility, Criminal Justice Section, Section of Individual Rights and Responsibilities, Section of Environment, Energy and Resources, International Law, Law Practice Division, Litigation, Science and Technology Law, Special Committee on Disaster Response and Preparedness, Standing Committee on Law and National Security, Standing Committee on Technology and Information Systems, State and Local Government Law, Tort, Trial and Insurance Practice and Public Utility, Communications and Transportation Law.

11. **Contact Name and Address Information.** (Prior to the meeting)

    Lucy L. Thomson  
    Livingston PLLC  
    1455 Pennsylvania Ave., N.W. Suite 400  
    Washington, D.C.  20004  
    lucythomson1@mindspring.com  
    (703) 798-1001 (cell)

    Judith Miller  
    Co-chair, Cybersecurity Legal Task Force  
    1050 Connecticut Avenue, Suite 400  
    Washington, D.C.  20036  
    (202) 341-8127 (cell)  
    judith.miller3@gmail.com

    Harvey Rishikof  
    Co-chair, Cybersecurity Legal Task Force  
    1050 Connecticut Avenue, Suite 400  
    Washington, D.C.  20036  
    (202) 288-2013 (cell)  
    rishikofh@me.com
12. Contact Name and Address Information. (Who will present the report to the House?)

Judith Miller  
Co-chair, Cybersecurity Legal Task Force  
1050 Connecticut Avenue, Suite 400  
Washington, D.C. 20036  
(202) 341-8127 (cell)  
Judith.miller3@gmail.com

Neal Sonnett, nrslaw@sonnett.com  
Stephen Saltzberg, ssaltz@law.gwu.edu  
Ellen Flannery, eflannery@cov.com  
Lucy Thomson, lucythomson1@mindspring.com  
Delegates, ABA House of Delegates
EXECUTIVE SUMMARY

1. **Summary of the Resolution**

   This Resolution focuses on cybersecurity threats that affect the judicial system and may pose a risk to the fair and efficient administration of justice. This Resolution urges federal, state, local, tribal and territorial legislatures and government agencies to provide the funding necessary to develop, implement, and maintain appropriate cybersecurity programs for the courts and to train court personnel on methods to counter threats and protect judicial information systems from cyber intrusions or data breaches.

   This Resolution builds on the ABA Resolutions adopted over the past decade that urge governments to provide adequate funding for the courts to ensure their security. As cybersecurity threats grow, the need for adequate funding for the courts to address these threats becomes critically important. The adoption of this Resolution will enhance court cybersecurity and promote fair and impartial courts.

2. **Summary of the Issue that the Resolution Addresses**

   This Resolution focuses on cybersecurity threats that affect the judicial system and may pose a risk to the fair and efficient administration of justice. The threat environment today is highly sophisticated, and massive data breaches are occurring with alarming frequency. Now, as the courts modernize their information systems, adequate funding will be required to develop, implement, and maintain an appropriate cybersecurity program, assess the threats to those systems, and protect the volumes of confidential and sensitive data that the courts collect, use, store, and share.

   The only effective defense is a fully-implemented cybersecurity program with controls based on operational criteria and magnitude of harm and risk categorization. In many cases, data breaches or other types of cyber incidents could have been prevented or detected early and the risks of the incident mitigated if the organization had undertaken proper cybersecurity planning and implemented appropriate security safeguards.

3. **Please Explain How the Proposed Policy Position Will Address the Issue**

   Through this Resolution, the ABA highlights the importance of adequate funding for the courts to address cybersecurity threats. This Resolution and Report will educate stakeholders, heighten their sensitivity to cybersecurity risks, and help the courts effectively evaluate their own specific risks and request adequate funding on behalf of their organizations.

4. **Summary of Minority Views**

   This Resolution and Report have been revised in response to input received from several ABA entities. No minority views have come to our attention with respect to the Report.