Supported Resolution 2—2022

In Support of Increased Cybersecurity Practices in State Courts

CONFERENCE OF CHIEF JUSTICES

CONFERENCE OF STATE COURT ADMINISTRATORS

WHEREAS, state courts handle a majority of the litigation in the United States, processing 96% of the nation's annual litigation, or 85 million cases, on average involving hundreds of millions of records ranging from orders, judgments, indictments, warrants, and other forms of legal process; and

WHEREAS, state courts retain hundreds of billions of pieces of personally identifiable information on litigants such as names, addresses, social security numbers, unique identifiers, state identification numbers, financial histories, criminal charges, and filed documents; and

WHEREAS, over the past 50 years, state courts have moved from exclusively paper-based docket management systems to electronic case management systems that are a widely-utilized source of information on people, businesses, and government agencies; and

WHEREAS, state courts have been designated by the United States Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) as an area of critical infrastructure;[1] and

WHEREAS, significant amounts of information retained in state court systems is provided to other state and federal authorities, often for national distribution through various other information sharing platforms; and

WHEREAS, the reliability, predictability, and finality of state court records and the ability to ensure continuity of operations of state court systems is vital to sustaining the rule of law; and

WHEREAS, state courts have been the subject of multiple cybersecurity attacks in recent years, with at least three state court systems being subject to ransomware attacks in the past 18 months; and

WHEREAS, 2020 statistics reveal that it takes up to 228 days for the average entity to detect a cybersecurity breach, 80 days to contain the breach, at a global average cost of $3.86 million per incident;[2] and

[1] https://www.cisa.gov/sites/default/files/publications/Version_4.0_CISA_Guidance_on_Essential_Critical_Infrastructure_Workers_FINAL%20AUG%2018v3.pdf.

[2] Sobers, Rob. "98 Must-Know Data Breach Statistics for 2021," Varonis, 6 Apr. 2021.

WHEREAS, it is incumbent on state court leaders to take action to prepare for and protect against cybersecurity attacks;

NOW, THEREFORE, BE IT RESOLVED, that the Conference of Chief Justices and the Conference of State Court Administrators urge their members to take concrete action to address cybersecurity risks as identified in the COSCA/NACM Joint Technology Committee's September 2021 publication titled "Cybersecurity Basics for Courts," including the following:

1) designate personnel within the state court system who are responsible for cybersecurity prevention, preparedness and response efforts;
2) prioritize investment in training and infrastructure for cyberattack prevention, response, and preparedness that includes all partner exposure;
3) designate a cybersecurity incident response team and cybersecurity governance body to set cybersecurity and information technology policies;
4) invest in cybersecurity and information technology risk assessments to determine areas for improvement;
5) protect equipment, facilities, systems, processes, and data to the degree possible and segment the network to limit exposure to cyberattacks;
6) implement multi-factor authentication for all users;
7) ensure that there is redundancy in backups of data and court records necessary for the operation of the courts;
8) participate in regular penetration testing of state court networks and systems;
9) ensure that cybersecurity response plans are included in the state courts' continuity of operations plans and that there is regular testing of cybersecurity response plans;
10) designate a staff person within the state court system to serve as a liaison to the state's designated regional office of CISA and establish a connection with the CISA regional contact;[3] and
11) participate in the free cybersecurity services offered to state and local governments through the Multi-State Information Sharing & Analysis Center (MS-ISAC); and

BE IT FURTHER RESOLVED, that the Conference of Chief Justices and the Conference of State Court Administrators urge CISA to include state courts in its advisory committee on state and local government and in its planning for allocating the cybersecurity funding provided by the Bipartisan Infrastructure Law signed by President Biden in November 2021; and

BE IT FURTHERED RESOLVED, that the Conference of Chief Justices and the Conference of State Court Administrators urge the National Center for State Courts (NCSC) to enhance the cybersecurity consulting and technical assistance services offered by NCSC to assist state courts in their efforts to improve cybersecurity.

Adopted as proposed by COSCA/NACM Joint Technology Committee at the COSCA 2021 Midyear Meeting and by the CCJ Board of Directors on December 22, 2021.

On November 8, 2022, the NACM Board voted to support this resolution.

[3] https://www.cisa.gov/cisa-regions