

## INTERIM STUDY PROPOSAL 2019-144

1  
2  
3       REQUESTING THAT THE JOINT COMMITTEE ON ADVANCED COMMUNICATIONS  
4       AND INFORMATION TECHNOLOGY CONDUCT A STUDY TO CREATE A CURRENT  
5       INVENTORY OF STATE GOVERNMENT BUILDINGS, BUILDING SYSTEMS,  
6       SUPPORTING TECHNOLOGY, AND DATA; ASSESS THE STATUS OF STATE  
7       CYBERSECURITY MEASURES IN PLACE TO PROTECT STATE GOVERNMENT  
8       BUILDINGS, ONLINE SYSTEMS, NETWORKS, AND DATA AGAINST  
9       CYBERATTACKS; AND DETERMINE BEST PRACTICES AND ESTABLISH  
10       STANDARDS FOR STATE BUILDING CYBERSECURITY THAT MAY BE  
11       IMPLEMENTED TO INCREASE STATE BUILDING CYBERSECURITY AND PROTECT  
12       STATE GOVERNMENT INTERESTS.

13  
14       WHEREAS, state governments and the property of state governments,  
15       including state government buildings, building systems, supporting  
16       technology, and data, are vulnerable to cyberattacks; and

17  
18       WHEREAS, state governments have been subject to recent cyberattacks and  
19       depending on whether the attacker was seeking intelligence or trying to  
20       disrupt government operations, state government buildings, supporting  
21       technology, data, business operations, security systems, HVAC and electrical  
22       systems, and any other state or local systems that are plugged in to online  
23       networks could be the targets of such attacks; and

24  
25       WHEREAS, due to electronic and online information being scattered  
26       across a variety of online systems and networks maintained by individual  
27       government entities and the lack of a designated state entity responsible for  
28       the maintenance and security of all state government property, including  
29       state government buildings, online systems, networks, and data, it is unknown  
30       which buildings, building systems, supporting technology, or data could be  
31       subject to a cyberattack; and

32  
33       WHEREAS, state government buildings, whether owned or leased by the  
34       state, may not meet any standards for ensuring security and therefore may  
35       require costly expenditures for cybersecurity protections necessary to  
36       protect state government interests; and

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36

WHEREAS, data collection across the state from various stakeholders, including quasi-independent stakeholders, is needed to gather information on state government property in order to create an accurate inventory of state government property, including buildings, building systems, supporting technology, and data,

NOW THEREFORE,  
BE IT PROPOSED BY THE JOINT COMMITTEE ON ADVANCED COMMUNICATIONS AND INFORMATION TECHNOLOGY OF THE NINETY-SECOND GENERAL ASSEMBLY OF THE STATE OF ARKANSAS:

THAT the Joint Committee on Advanced Communications and Information Technology conduct a study to:

- (1) Create a current inventory of state government buildings, building systems, supporting technology, and data;
- (2) Assess the status of state cybersecurity measures in place to protect state government buildings, building systems, supporting technology, and data against cyberattacks; and
- (3) Determine the best practices and establish standards for state building cybersecurity measures that may be implemented to increase state building cybersecurity and protect state government interests.

BE IT FURTHER PROPOSED THAT the study identify:

- (1) The exact number of buildings owned or leased by the state, including the square footage of each building and current cybersecurity systems in place in and around each building;
- (2) The personnel who are responsible for maintaining each building and providing cybersecurity services within and around each building;
- (3) The presence of any other cybersecurity systems connected to any state government online system or network, including without limitation HVAC systems and electrical systems; and
- (4) Relevant stakeholders, including quasi-independent stakeholders, in order to recommend potential solutions to cybersecurity vulnerabilities and the cost impact of those proposed solutions.

1 BE IT FURTHER PROPOSED THAT the study review and analyze:

2 (1) Current state readiness to respond to a hypothetical  
3 cyberattack;

4 (2) Existing backup systems to state government building  
5 systems, supporting technology, and data and how backup data is stored and  
6 compares to the original data; and

7 (3) Any other pertinent information related to increasing state  
8 cybersecurity and protecting state government property, including state  
9 government buildings, building systems, supporting technology, and data.

10  
11 Respectfully submitted,

12  
13  
14  
15 Representative Stephen Meeks  
16 District 67

17  
18  
19  
20 Senator Mark Johnson  
21 District 15

22  
23 Prepared by: ANS/ANS  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36