

---

---

# SENATE RESOLUTION

REQUESTING THAT THE CHIEF INFORMATION OFFICER REVIEW WHETHER ALL DEPARTMENTS, AGENCIES, AND OFFICES OF THE STATE HAVE UP-TO-DATE TECHNOLOGY TO REDUCE CYBER THREATS AND HELP PROTECT THE STATE AGAINST CYBERATTACKS.

1           WHEREAS, the frequency, scale, and sophistication of  
2           cyberattacks against key infrastructure and government systems  
3           have been on the rise in recent years; and  
4

5           WHEREAS, many of these cyberattacks lead to data breaches  
6           of highly sensitive and personal information, such as the major  
7           security breach suffered by the United States (U.S.) Marshals  
8           Service on February 17, 2023; and  
9

10           WHEREAS, the U.S. Marshals Service is a division of the  
11           United States Department of Justice that provides for the  
12           protection of judges and court personnel, transportation of  
13           federal prisoners, and operation of the federal Witness  
14           Protection Program; and  
15

16           WHEREAS, according to United States Department of Justice  
17           officials, hackers attacked the computer system through  
18           ransomware and stole law enforcement data that included returns  
19           from the legal process, administrative information, and  
20           personally identifiable information relating to U.S. Marshals  
21           Service investigative targets, third parties, and certain U.S.  
22           Marshals Service employees; and  
23

24           WHEREAS, recent significant cyberattacks on other  
25           governmental entities include the ransomware attacks on various  
26           governmental institutions of Costa Rica throughout April and May  
27           of 2022, and the attack on Vanuatu's government servers and  
28           websites in November 2022; and  
29

30           WHEREAS, the ransomware attacks on the Costa Rican  
31           government not only caused losses of tens of millions of dollars  
32           a day to the country's import/export industry for months, but



1 also widespread disruptions to the country's social security  
2 fund and health care system, causing Costa Rica to be the first  
3 nation to declare a national emergency due these attacks; and  
4

5 WHEREAS, Vanuatu is an archipelagic state in the Pacific  
6 with a population of just over 315,000 people and the  
7 cyberattack to this nation took down virtually all of the  
8 government's digital networks, including but not limited to its  
9 emergency systems, medical records, vehicle registrations,  
10 driver's license databases, and tax systems, thereby causing its  
11 agencies to conduct their work on paper and by using personal  
12 email accounts for months following the attack; and  
13

14 WHEREAS, the ongoing cyberwarfare between Russia and  
15 Ukraine, which has resulted in skewed election results, theft  
16 and destruction of data, blackouts, and other forms of data  
17 breaches and service disruptions, demonstrates the magnitude of  
18 chaos that can be caused by cybercriminals, not only to key day-  
19 to-day operations, but also to major institutions and  
20 infrastructure; and  
21

22 WHEREAS, the growing state of cyber threats and speed at  
23 which cyber criminals target government entities require that  
24 the State have up-to-date technology to lower the chances of a  
25 possible data breach or worse; now, therefore,  
26

27 BE IT RESOLVED by the Senate of the Thirty-second  
28 Legislature of the State of Hawaii, Regular Session of 2023,  
29 that the Chief Information Officer is requested to review  
30 whether all departments, agencies, and offices of the State have  
31 up-to-date technology to reduce cyber threats and help protect  
32 the State against cyberattacks; and  
33

34 BE IT FURTHER RESOLVED that all departments, agencies, and  
35 offices of the State are requested to cooperate with and assist  
36 the Chief Information Officer to determine whether any and what  
37 upgrades are needed to current technology to reduce the chances  
38 of falling victim to cyber threats, including but not limited to  
39 disruptive hacks, ransomware attacks, data breaches, and digital  
40 scams; and  
41



1 BE IT FURTHER RESOLVED that the Chief Information Officer  
2 is requested to submit a report of its findings and  
3 recommendations, including any proposed legislation and the  
4 prioritization of projects to upgrade the technology of the  
5 State, to the Legislature prior to the convening of the Regular  
6 Session of 2024; and

7  
8 BE IT FURTHER RESOLVED that certified copies of this  
9 Resolution be transmitted to the Governor and Chief Information  
10 Officer.

