Department of Legislative Services

Maryland General Assembly
2004 Session

FISCAL AND POLICY NOTE

House Bill 195 (Delegate Lee, *et al.*)
Judiciary

Crimes - Unauthorized Computer Access for Sabotage of State Government or Public Utilities

This bill establishes that it is a crime for a person to intentionally and willfully gain unauthorized access to all or part of a computer, computer system, network, software, database, or service with the intent to impair or interrupt the functioning of State government, or any service provided in the State by a common carrier or a public utility.

Fiscal Summary

State Effect: Potential minimal increase in general fund revenues and expenditures due to the bill's penalty provisions.

Local Effect: Potential minimal increase in revenues and expenditures due to the bill's penalty provisions.

Small Business Effect: None.

Analysis

Bill Summary: The bill provides that a person may not intentionally, willfully, and without authorization access or attempt to access, cause to be accessed, or exceed authorized access to all or part of a computer network, language, software, system, services, or database. A person may not commit unlawful access with the intent to cause the malfunction or interruption of any or all parts of a computer, network, language, software, services, or data. A person may not intend to alter, damage, or destroy all or any part of data or program stored, maintained, or produced by a computer, network,

software, system, services, or database. A person may not intentionally, willfully, and without authorization possess, identify or attempt to identify, a valid access code or publicize or distribute a valid access code to an unauthorized person. A person may not commit any of the aforementioned acts with the intent to interrupt or impair the functioning of State government or any service provided by a public service company. Public service companies include common carriers, telephone and telegraph companies, electric, gas, steam heating, sewage disposal companies, and water companies.

If a person who violates these provisions causes an aggregate amount of loss of $50,000 or more, then the person is guilty of a felony and subject to a maximum imprisonment term of 15 years, a maximum fine of $50,000, or both. If the aggregate loss is less than $50,000, a violator is guilty of a misdemeanor and is subject to a maximum imprisonment term of five years, a maximum fine of $25,000, or both.

Current Law: A person may not intentionally, willfully, and without authorization access or attempt to access, cause to be accessed, or exceed authorized access to all or part of a computer network, language, software, system, services, or database. A violation of this provision is a misdemeanor and the violator is subject to a maximum imprisonment term of three years, or a maximum fine of $1,000, or both.

A person may not commit unlawful access with the intent to cause the malfunction or interruption of any or all parts of a computer, network, language, software, services, or data. A person may not intend to alter, damage, or destroy all or any part of data or program stored, maintained, or produced by a computer, network, software, system, services, or database. A person may not intentionally, willfully, and without authorization possess, identify, or attempt to identify a valid access code, or publicize or distribute a valid access code to an unauthorized person. If the aggregate amount of loss is $10,000 or more, the violator is guilty of a felony and is subject to a maximum imprisonment term of 10 years, a maximum fine of $10,000, or both. If the aggregate loss is less than $10,000, the violator is guilty of a misdemeanor and is subject to a maximum imprisonment term of five years, a maximum fine of $5,000, or both.

Access achieved in a prohibited manner under a single scheme or a continuing course of conduct may be considered one violation. A defendant may be tried in any county in Maryland where the act was performed or the accessed computer was located.

Background: On August 14, 2003, a major power outage struck simultaneously across major portions of the eastern U.S. and Canada. New York City, Detroit, Cleveland, and other metropolitan areas were suddenly without power. State and federal authorities were able to quickly determine that the outage was not an act of terrorism. What was also

immediately apparent, however, is that an act of terrorism *could* have played havoc with energy delivery systems, causing an outage not unlike what happened in August.

According to the American Power Association, in a 2003 survey conducted by the Federal Bureau of Investigation (FBI) and the Computer Security Institute, a majority of the responding organizations reported one or more security incidents and a continued, growing trend toward insider abuse of networks. In fact, most of the survey respondents said that disgruntled employees are the most likely source of an attack, more than independent hackers, competitors, or foreign entities. Most survey respondents reported incidents of network access abuse by insiders and nearly half reported unauthorized access by insiders.

Since the terrorist attacks of September 11, 2001, addressing the threat of cyber terrorism has become an essential part of what is called "homeland security." The Intelligent Transportation Society of America reports that a jointly planned physical attack and cyber-attack on 9-1-1, air traffic control, or dam floodgate systems could cause massive disruption and damage. For example, in 1998, a 12 year old computer hacker broke into the computer network that runs the Roosevelt Dam in Arizona. He had complete control of the system that manages the dam's floodgates and holds back 489 trillion gallons of water. If that volume of water had been unleashed, it could have submerged the entire city of Phoenix, Arizona in five feet of water. In April 2000, in Queensland Australia, someone was arrested for intentionally causing harm to the area's wastewater treatment system. That person used commercially available technology and stolen computer equipment to cause the leaking of hundreds of thousands of gallons of sludge into parks, rivers, and commercial properties for two months. Cyber security specialists have studied this case because it is one of the few where a person was able to use a digital control system to deliberately cause harm.

State Revenues: General fund revenues could increase minimally as a result of the bill's monetary penalty provision from cases heard in the District Court.

State Expenditures: General fund expenditures could increase minimally as a result of the bill's incarceration penalty due to more people being committed to Division of Correction (DOC) facilities and increased payments to counties for reimbursement of inmate costs. The number of people convicted of this proposed crime is expected to be minimal.

Persons serving a sentence longer than 18 months are incarcerated in DOC facilities. Currently, the average total cost per inmate, including overhead, is estimated at $1,850 per month. This bill alone, however, should not create the need for additional beds, personnel, or facilities. Excluding overhead, the average cost of housing a new DOC

inmate (including medical care and variable costs) is $350 per month. Excluding medical care, the average variable costs total $120 per month.

Persons serving a sentence of one year or less in a jurisdiction other than Baltimore City are sentenced to local detention facilities. For persons sentenced to a term of between 12 and 18 months, the sentencing judge has the discretion to order that the sentence be served at a local facility or DOC. The State reimburses counties for part of their incarceration costs, on a per diem basis, after a person has served 90 days. State per diem reimbursements for fiscal 2005 are estimated to range from $14 to $58 per inmate depending upon the jurisdiction. Persons sentenced to such a term in Baltimore City are generally incarcerated in DOC facilities. The Baltimore City Detention Center, a State-operated facility, is used primarily for pretrial detentions.

Local Revenues: Revenues could increase minimally as a result of the bill's monetary penalty provision from cases heard in the circuit courts.

Local Expenditures: Expenditures could increase minimally as a result of the bill's incarceration penalty. Counties pay the full cost of incarceration for people in their facilities for the first 90 days of the sentence, plus part of the per diem cost after 90 days. Per diem operating costs of local detention facilities are expected to range from $29 to $97 per inmate in fiscal 2005.

Additional Information

Prior Introductions: None.

Cross File: None.

Information Source(s): Department of Public Safety and Correctional Services, American Power Association, Intelligent Transportation Society of America, Cable News Network (CNN), Department of Legislative Services

Fiscal Note History: First Reader - January 26, 2004
ncs/jr

Analysis by: Karen D. Morgan

Direct Inquiries to:
(410) 946-5510
(301) 970-5510