To: All Licensees

From: State Corporation Commission's Bureau of Insurance

Re: Log4j Vulnerability

On December 10, 2021, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA"), the National Security Agency, and others announced a critical remote code execution vulnerability in many versions of Apache's Log4j software library. Log4j is a java-based logging utility incorporated in frameworks, websites, and applications, and is widely used by major cloud services and well-known software vendors and manufacturers. According to senior cybersecurity professionals, this vulnerability is among the most serious seen to date.

Threat actors are actively exploiting Log4j vulnerabilities. Successful exploitation of the vulnerability can be used to deploy ransomware, steal data, and disrupt operations.

All licensees should promptly assess risk to their organization, customers, consumers, and third-party service providers based upon the evolving information and take action to mitigate risk. CISA is maintaining and regularly updating a webpage dedicated to Log4j vulnerability guidance. Licensees should consult the CISA guidance and implement it wherever appropriate.

Licensees are reminded to report cybersecurity events that meet the criteria of the Virginia Insurance Data Security Act (§§ 38.2-621 through 38.2-629 of the Code of Virginia) and report any cybersecurity events to the Commissioner of Insurance within three days of determining that the cybersecurity event has occurred. Cybersecurity events should be reported using this email: BOIDataSec@scc.virginia.gov