NSC backs disclosing software vulnerabilities

April 13 2014

Disclosing vulnerabilities in commercial and open source software is in the national interest and shouldn't be withheld from the public unless there is a clear national security or law enforcement need, President Barack Obama's National Security Council said Saturday.

The statement of White House policy came after a computer bug called "Heartbleed" caused major security concerns across the Internet and affected a widely used encryption technology, the variant of SSL/TLS known as OpenSSL, that was designed to protect online accounts. Major Internet services worked this week to insulate themselves against the bug.

The NSC, which Obama chairs, advises the president on national security and foreign policy matters. Its spokeswoman, Caitlin Hayden, said in a statement Saturday that the federal government was not aware of the Heartbleed vulnerability in OpenSSL until it was made public in a private sector cybersecurity report. The federal government relies on OpenSSL to protect the privacy of users of government websites and other online services, she said.

"This administration takes seriously its responsibility to help maintain an open, interoperable, secure and reliable Internet," she said. "If the federal government, including the intelligence community, had discovered this vulnerability prior to last week, it would have been disclosed to the community responsible for OpenSSL."

The president's Review Group on Intelligence and Communications

Technologies, which Obama appointed last year to review National Security Agency surveillance programs and other intelligence and counterterrorism operations, recommended in December that U.S. policy should generally move to ensure that previously unknown vulnerabilities "are quickly blocked, so that the underlying vulnerabilities are patched on U.S. government and other networks."

"The White House has reviewed its policies in this area and reinvigorated an interagency process for deciding when to share vulnerabilities. This process is called the Vulnerabilities Equities Process," Hayden said. "Unless there is a clear national security or law enforcement need, this process is biased toward responsibly disclosing such vulnerabilities."