

# U.S. Sen. Johnson, colleague: Introduce bipartisan bill to help secure federal information technology supply chains against threats

Posted on Thursday, Jul 1, 2021

>> **WisPolitics is now on the State Affairs network. Get custom keyword notifications, bill tracking and all WisPolitics content. [Get the app or access via desktop.](#)**

**WASHINGTON** — U.S. Senators Ron Johnson (R-Wis.) and Gary Peters (D-Mich.) introduced bipartisan legislation to help protect against cybersecurity threats and other technological supply chain security vulnerabilities that arise when the federal government purchases services, equipment or products. The *Supply Chain Security Training Act* would create a standardized training program to help federal employees responsible for purchasing services and equipment identify whether those products could compromise the federal government's information security.

“Counterintelligence training for federal workers who buy and sell goods and services for the government is critical at a time when our adversaries are probing cyber vulnerabilities to breach our systems and steal information,” **said Senator Johnson.** “This type of training will help close a potential gap in our cyber and physical security defenses.”

“Recent attacks against American networks show that our foreign adversaries and criminal organizations will stop at nothing to breach federal networks, steal information and compromise our national security,” **said Senator Peters.** “Federal employees need to know how to recognize possible threats when they are purchasing software and equipment that could allow bad actors a back door into government information systems. This bill will help strengthen national security by safeguarding against cybersecurity vulnerabilities and other threats posed by the

technology our government uses.”

Training and preparing federal acquisitions employees to recognize and mitigate these growing threats is an essential step in preventing hostile actors from compromising America’s national security. Recent breaches of federal information systems exploited vulnerabilities in the SolarWinds and Microsoft Exchange networks, highlighting the need for robust technological supply chain security and the importance of ensuring agency personnel responsible for managing these resources are well versed and up-to-date on cybersecurity threats and other attempts to steal sensitive or valuable information.

The *Supply Chain Security Training Act* directs the General Services Administration (GSA), in coordination with the Department of Homeland Security (DHS), the Department of Defense (DOD) and the Office of Management and Budget (OMB), to create a supply chain security training program for federal officials with supply chain risk management responsibilities. The bill would also require the OMB to develop guidance for federal agencies to adopt and use the training program and how to select officials to participate in the training.

The bill is based on [similar legislation](#) Johnson and Peters introduced last Congress. The legislation also builds on a recent executive order from President Biden that made it easier for federal agencies to share threat information, modernize their cybersecurity infrastructure and enhance federal software supply chain security in the wake of recent serious breaches.