A3 communications
A DIVISION OF THE COOK & BOARDMAN GROUP, LLC

National Defense Authorization Act: What does it mean for schools?

By Kevin Wren

Signed into law August 13, 2018, Section 889 of the National Defense Authorization Act (NDAA) prohibits federal agencies, their contractors and grant or loan recipients from procuring or using telecommunications and video surveillance products from specific Chinese companies—specifying a range of equipment produced by Huawei, ZTE, Hytera, Hikvision and Dahua.

But, why did the government take such an aggressive stance against these brands and their products?

With allegations posed that these technology companies are being used by the Chinese government, United States officials aren't willing to risk America's data to Chinese surveillance and espionage. Although Huawei, one of the identified firms, vigorously denies these claims, findings from the United Kingdom detail serious systematic defects in the product's software engineering and cyber security competence.

Despite the federal product bans in the US, local governments are not prohibited from purchasing this equipment although some state and local entities have chosen to exclude specified manufacturers from procurement activities. However, eliminating these products from Requests for Proposals is not as simple as specifying Hikvision or Dahua. Both brands manufacture/re-brand cameras for use by other companies. IPVM, an independent security publication, published a list of companies who rebrand their cameras and products on their website, however the list is growing.

For schools this means they can continue to buy products from non-compliant NDAA companies as long as they don't use federal grant funding, like the School Violence Prevention Program. If a school uses local funds to purchase these products, buyer beware. Stakeholders must research and perform risk assessments with consideration beyond the opportunity for unwanted parties to view data. Vulnerabilities like these can open a pathway to your network for hackers to access confidential information.

Does the cost of these solutions outweigh the financial impact of a student data breach or potential thread to your school? Is your network prepared for the cyber security threat these non-NDAA devices establish?

Although the choice to continue using or begin procuring non-compliant NDAA technology is yours to make, we implore you to explore other cost-effective, NDAA-compliant solutions and ask yourself: why spend precious American taxpayer dollars on products banned for espionage and illegal surveillance?

ABOUT THE AUTHOR

As a School Safety Advocate for A3 Communications, Kevin Wren helps schools and districts with security and emergency management planning. He has been in K12 security and emergency management for over 20 years with two of South Carolina's largest school districts. While at Rock Hill Schools, he was named "School Safety Director of the Year" by Campus Safety Magazine. Currently, he is involved with several national school safety groups, including the Partner Alliance for Safer Schools, and speaks at conferences throughout the United States.