To: Policymakers, Media, and Experts
Fr: Roslyn Layton and John Strand, Co-Founders, ChinaTechThreat.com
Re: DoD Must Act to Eliminate Suspicious Technology Manufacturers
Da: August 2019

Pentagon IG Report Reveals Cybersecurity Risks Ignored

A Department of Defense IG Report, Released On July 30, 2019, Found That Over Than 9,000 Commercially Available IT Products (COTS) Bought In FY 2018 with a Total Cost of at Least $32.8 Million Could Be Used To Spy On Or Hack U.S. Military Personnel And Facilities.

- **The Army And Air Force Purchased Over 8,000 Lexmark Printers.** "Lexmark is a company with connections to Chinese military, nuclear, and cyberespionage programs. The National Vulnerabilities Database lists 20 cybersecurity vulnerabilities for Lexmark including storing and transmitting sensitive network access credentials in plain text and allowing the execution of malicious code on the printer. These vulnerabilities could allow remote attackers to use a connected Lexmark printer to conduct cyberespionage or launch a denial of service attack on a DoD network." (pg. 6-7)

- **The Army And Air Force Purchased 117 GoPro Action Cameras.** "[T]he cameras have vulnerabilities that could allow a remote attacker access to the stored network credentials and live video streams. By exploiting these vulnerabilities, a malicious actor could view the video stream, start recording, or take pictures without the user's knowledge." (pg. 7)

- **The Army And Air Force Purchased 1,573 Lenovo Devices.** Lenovo products have been banned, investigated or deemed vulnerable by the State Department in 2006, the Department of Homeland Security in 2015, the Joint Chiefs of Staff Intelligence Directorate in 2016 and the DoD Information Network in 2018. (pg. 7)

"If the DoD continues to purchase and use COTS information technology items without identifying, assessing, and mitigating the known vulnerabilities associated with COTS information technology items, missions critical to national security could be compromised." (pg. i)

DoD Officials Have Until August 26 to Respond to IG Recommendations

The IG Suggested Four Recommendations and Pentagon Officials Responded, but the IG Found Most of their Answers Inadequate. The DoD Officials Now have until August 26th to Provide Additional Plans.

1. **No Organization Has Been Given Responsibility For Developing A Strategy To Mitigate Cybersecurity Risks Through COTS Purchases**. "The DoD did not establish responsibility for an organization or group for managing the cybersecurity risks posed by COTS information technology items across the DoD. We reviewed DoD acquisition policy and the items banned from purchase or use by Congress and the DoD and did not identify an organization responsible for managing the cybersecurity risks of COTS information technology items." (pg. 7)

ChinaTechThreat.com
Roslyn Layton – Roslyn@chinatechthreat.com | John Strand – John@chinatechthreat.com

2. **The DoD Lacks Sound Acquisition Policies. "**DoD acquisition policy did not require DoD Components to consider known cybersecurity risks before acquiring COTS information technology items or to mitigate cybersecurity risks before integrating the items into DoD programs… the DoD's increased reliance on COTS information technology items as components for larger systems increases the risk that missions and operations could be compromised by adversaries who exploit known cybersecurity vulnerabilities." (pg. 12-13)

3. **Pentagon's Approved Products List Includes Products with Cyber Risks.** "[T]he Unified Capabilities APL [approved products list] includes COTS information technology items with known cybersecurity risks. For example, the APL includes Lenovo products which have known cybersecurity vulnerabilities. According to the Chief of the Assessments and Authorizations Division at the Defense Information Systems Agency, cybersecurity risks introduced through the supply chain are not considered when evaluating whether to add COTS information technology items to the DoD Unified Capabilities APL." (pg. 15)

4. "The DoD Did Not Establish Controls To Prevent The Purchase Of COTS Information Technology Items With Known Cybersecurity Risks." (pg. 15)

"Of the nine COTS information technology manufacturers or items that have been banned, four were banned by Congress instead of the DoD despite numerous reports of cybersecurity vulnerabilities." (pg. 16)

Congress Must Demand Answers and Action

ChinaTechThreat.com Suggests Five Additional Questions for Policymakers, Media, and Experts:

1. **Why Are The Manufacturers Not Already Banned?** The IG report characterizes Lenovo, GoPro and Lexmark products as "known cybersecurity risks." Considering the clear risk, why are they not already banned?

2. **Why Does It Take So Long to Ban Manufacturers?** The IG report identifies several examples of the federal government not taking action on its own warnings. In 2012, the House Permanent Select Committee on Intelligence issued a report in recommending that government systems and contractors not use Huawei or ZTE telecommunications equipment in their systems, yet the DoD ignored these findings for five years until Congress finally prohibited the manufacturers in 2017. (pg. 15-16)

3. **Why Don't Authorities Ban Products Based On Intelligence Rather Than On Publicity?** The IG report notes that the DoD eventually banned suspicious manufacturers "in response to cybersecurity incidents or public exposure, not based on risks..." (pg. 16)

4. **Why Do The Service Secretaries Fail To Act When They Have The Ability To Do So?** In 4 of 9 COTS manufacturer bans, Congress acted before the DoD, despite the fact that the service secretaries have the authority to do so but have only acted once. (pg. 16)

5. Beyond The Defense Department, What Is The Responsibility Of The U.S. Government And Its Plan To Inform State And Local Governments And Businesses That Have A Role In Security?

ChinaTechThreat.com
Roslyn Layton – Roslyn@chinatechthreat.com | John Strand – John@chinatechthreat.com