

# Congress of the United States

WASHINGTON, DC 20510

August 9, 2011

The Honorable Leon Panetta  
Secretary of Defense  
1000 Defense Pentagon  
Washington, DC 20301-1000

The Honorable Steven Chu  
Secretary of Energy  
1000 Independence Avenue, SW  
Washington, DC 20585

The Honorable Mary Schapiro  
Chairman  
Securities and Exchange Commission  
100 F Street NE  
Washington, DC 20549-2000

Dear Secretary Panetta, Secretary Chu, and Chairman Schapiro:

As you may know, MPAK Technologies recently won a competition to supply technology to the University of Tennessee's National Center for Computational Engineering, and press reports indicate that MPAK will be installing Huawei/Symantec technology at the center. As the Administration Task Force reviews our current supply chain vulnerabilities, it appears Huawei is seeking new strategies to mask its penetration of our information systems in ways that demand careful and thorough review.

The center has conducted cutting-edge research in many disciplines over the years. It has also provided research assistance to the government – including the Departments of Energy and Defense – on a variety of important projects, including certain classified programs.

Reports suggest the Huawei-MPAK proposal may have been significantly cheaper than bids offered by competitors. Huawei is well known to benefit from a variety of preferential government policies of the People's Republic of China (PRC) and billions of dollars in government loans and export financing. According to Fred P. Hochberg, the Chairman and President of the Export-Import Bank of the United States, "This backing allows Huawei to significantly reduce its cost of capital and to offer financing to their buyers at rates and terms that are better than their competitors."<sup>1</sup> However, given the ambiguous relationship between MPAK

---

<sup>1</sup> Fred P. Hochberg, "How the U.S. Can Lead the World in Exports: Retooling Our Export Finance Strategy for the 21st Century." The Center for American Progress. Washington, DC. June 15, 2011. See, [http://www.exim.gov/about/leadership/hochberg\\_20110615.cfm](http://www.exim.gov/about/leadership/hochberg_20110615.cfm) (last visited July 27, 2011)

and Huawei/Symantec, it is unclear if the university was aware it was purchasing Huawei technology, with all the risks that such technology – provided by a company that may act as an agent of the PRC – entails. As a report on the subject notes, “Rather than trying to sell direct, it [Huawei] has established partnerships with U.S. companies like MPAK and Force 10 Networks to do it for them.”<sup>2</sup>

As Huawei continues to increase its share of the global market, the U.S. government has not yet pursued trade actions against Huawei for the massive support it enjoys from the government of the PRC. However, if Huawei’s government support and artificially low prices appear to be the company’s lynchpin for expanding its footprint in the United States, then our nation will have no choice but to seek appropriate trade remedies.

Additionally, there are longstanding concerns about Huawei’s relationship to the military and intelligence sectors of the PRC. These concerns reportedly compelled the Committee on Foreign Investment in the United States to block Huawei’s attempt to acquire U.S. technology firms on two occasions, and prompted both the National Security Agency and the Secretary of Commerce to advise two major U.S. telecom carriers against selecting Huawei as a supplier.<sup>3,4</sup>

Given Huawei’s close ties to the PRC government and its military and intelligence sectors, its history of alleged corrupt practices and infringement on intellectual property rights, and concerns it may act as an agent for a foreign government, Huawei is not an appropriate partner for advanced U.S. research centers – especially those working on critical or classified defense projects for the United States government.

With this in mind, we would appreciate your expeditious response to the following questions:

- Were the Departments of Defense and Energy aware that MPAK was introducing Huawei gear into the supply chain of the University of Tennessee’s National Center for Computational Engineering?
- What steps have the Departments of Defense and Energy taken to evaluate the possibility of illicit or unauthorized leakage to the PRC of information from the University of Tennessee’s National Center for Computational Engineering as a result of its agreement with MPAK-Huawei?
- Are the Departments of Defense and Energy aware of whether Huawei employees will have any access to the center as a result of this deal between the center and MPAK?

---

<sup>2</sup> Jeffrey Carr, “Hawei Symantec Hardware Powers U.S. Critical Technology Research.” *Digital Dao*. July 21, 2011. See, <http://jeffreycarr.blogspot.com/2011/07/huawei-symantec-hardware-powers-us.html> (last visited July 27, 2011)

<sup>3</sup> Todd Shields, “Locke Says Sprint’s Chief Was Called About Huawei Bid Concerns.” *Bloomberg Businessweek*. December 7, 2010. See, <http://www.businessweek.com/news/2010-12-07/locke-says-sprint-s-chief-was-called-about-huawei-bid-concerns.html> (last visited July 27, 2011)

<sup>4</sup> John Pomfret, “History of Telecom Company Illustrates Lack of Strategic Trust Between U.S., China.” *Washington Post*. October 8, 2010. See, <http://www.washingtonpost.com/wp-dyn/content/article/2010/10/07/AR2010100707210.html> (last visited July 27, 2011)



- What steps have you taken to make your department's critical private sector partners – and your research partners in particular – aware of threats to their technology supply chain?
- Does the Department of Defense and Energy need additional authority to interact with its private sector partners and affiliates to address supply chain threats?
- While concerns over Huawei's behavior have prevented it from gaining a significant foothold in the United States, it appears to be forming relationships with U.S. companies in order to resell its equipment here. Press reports suggest that MPAK, Force10, and SYNEX have formed partnerships to resell Huawei technology in the United States. As long as these arrangements continue, it appears they do not have to disclose their troubling relationships with Huawei. In view of Dell's announced purchase of Force10 networks, what responsibility does Dell, or any other publicly traded company have to report its relationship with Huawei – and the potential material risks that relationship may constitute – to its shareholders and organizations (including U.S. and federal and state government agencies) with whom it conducts business?

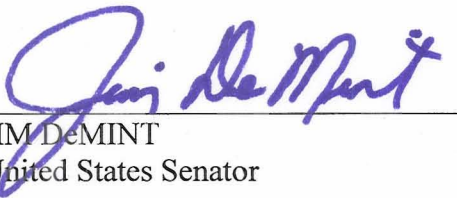
Sincerely,



JON KYL  
United States Senator



TOM COBURN, M.D.  
United States Senator



JIM DEMINT  
United States Senator



JAMES M. INHOFE  
United States Senator



SUE MYRICK  
Member of Congress

CC: The Honorable Howard Schmidt, White House Cybersecurity Coordinator  
The Honorable James Clapper, Director of National Intelligence