MEMORANDUM FOR ALMAJCOM/DRU/FOA (CONTRACTING)  
ALMAJCOM/DRU/FOA A6 AND SUBORDINATE CIOS  

SUBJECT: Leveraging Cyberspace Infrastructure Planning System (CIPS) and Enforcement of  
Trade Agreements Act (TAA) Requirements to Enhance Network Security  

The communications and contracting communities, amongst others, are working closely  
to secure our IT supply chain and defend our systems against intrusions and exploitation. Our  
efforts need to start with careful review and approval of our IT requirements prior to purchase  
and must continue through strict evaluation of offerors in accordance with authorities under the  
Trade Agreements Act (TAA) to contribute to this goal.  

The TAA governs trade agreements negotiated between the United States and other  
countries under the Trade Act of 1974. Pursuant to Federal Acquisition Regulation (FAR)  
Subpart 25.4, the Trade Agreements Act provides the authority for the President to waive the  
Buy American statute and other such provisions in order to obtain eligible products from  
countries that have signed an international trade agreement with the United States, or that meet  
certain other criteria, such as being a least developed country. TAA applies to all IT related  
purchases such as our Network-Centric Solutions (NETCENTS) program, Government Purchase  
Card (GPC) purchases, and other IT vehicles.  

Cyber and Communications squadrons are advised that we have received recent reporting  
that highlights the efforts of nation states to attempt to infiltrate our supply chain and the items  
we procure in order to enable their cyber exploitation of our missions. A key concept for  
protecting our Air Force Networks is requirements discipline through utilization of the  
Cyberspace Infrastructure Planning System (CIPS) for all IT requirements, regardless of dollar  
value. Then coupled with our strict compliance with TAA in regards to IT procurements, which  
is more critical than ever and just one way we contribute to the fight.  

Utilizing the CIPS requirements process ensures the proposed solutions/products sought  
for purchase are secure and approved by the Communications Squadron prior to contract award.  
You and your team will need to ensure products/solutions being requested at your  
base/installation are on the approved products list, are compatible with our network architectures,  
are purchased from the original manufacturer or an authorized reseller and the technologies are  
ot developed or hosted in suspect countries. You are on the front lines of cyber defense for our  
warfighters in the field! You make a difference with the choices you make on how and where to  
procure IT!  

Warranted Contracting Officers are reminded to strictly evaluate offers in accordance  
with DFARS Subpart 225.4 and 225.5 as well as obtain appropriate certification in accordance  
with DFARS 252.225-7020 when procuring IT related items, regardless of the contract tool  
utilized. Further, you and your team can help by ensuring our best value determinations for IT
related products not only include a price, but a clear and defendable TAA waiver used IAW DFARS.

For cyber or network security related questions, please contact your base/command information security manager or the Chief Information Security Officer at 703-697-1303. Please direct any contracting questions to Ms. Beatrice Torres, SAF/AQCA at 703-545-9090 (DSN 865-9090) or beatrice.b.torres.civ@mail.mil.

WILLIAM MARION, SES, USAF
Deputy Chief Information Dominance and Deputy Chief Information Officer

CASEY D. BLAKE, Major General, USAF
Assistant Secretary (Acquisition)