

October 23, 2017

Honorable Ellen Lord  
Under Secretary of Defense for Acquisition, Technology and Logistics  
3015 Defense Pentagon  
Rm 3E1010  
Washington, DC 20301-3015

Dear Ms. Lord:

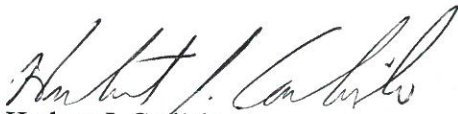
In May 2014, the National Defense Industrial Association (NDIA) presented to the Undersecretary of Defense (Acquisition, Technology & Logistics) a report on the growing cyber threat to U.S. defense industrial base. In a follow-on action, with coordination and support from several Office of the Secretary of Defense (OSD) organizations, including Ms. Kristen Baldwin's office, NDIA formed a joint working group charged with providing specific ideas for implementing the recommendations in the original report and developing an integrated approach across government agencies to address this rapidly escalating problem.

The Cybersecurity for Advanced Manufacturing Joint Working Group (CFAM JWG) focused on the protection of manufacturing networks from cyber-attacks in the defense industrial base. The group identified ways for the Department of Defense (DoD) and its prime contractors to assist manufacturers, particularly small and medium enterprises (S&MEs) to improve cybersecurity.

With this letter I am pleased to transmit to you the report from this Joint Working Group. The recent release of Presidential Executive Order 13806 "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States" (21 July 2017) makes this White Paper both timely and appropriate.

As you know from your previous association, NDIA is committed to assist the DoD and the defense manufacturing industry in securing the nation's manufacturing infrastructure from cyber-attacks and cyber espionage. We are pleased to support the important mission of your organization.

Sincerely,



Herbert J. Carlisle  
General, USAF (Ret.)  
President and CEO