From: "Hoydysh, Dan" <dan.hoydysh@unisys.com>
To: PublicComments@bis.doc.gov
Date: Mon, Feb 7, 2011 7:31 PM

Comments Attached

Dan Hoydysh I Director Global Public Policy I Government Relations I O: 703.439.5193 I M: 202.210.7310

Unisys Corporation I 11720 Plaza America Drive I Tower III I Reston, VA 20190
UNISYS

Imagine it. Done.

February 7, 2011

Sent via email to: publiccomments@bis.doc.gov

Regulatory Policy Division
ATTN: Notice of Inquiry -- CCL
Bureau of Industry and Security
Room 2705
U.S. Department of Commerce
Washington, DC 20230

RE: Federal Register: December 9, 2010 (Volume 75, Number 236)

Commerce Control List: Revising Descriptions of Items and Foreign Availability

On behalf of the Computer Coalition for Responsible Exports ("CCRE"), we are submitting these comments in response to the above-referenced notice. CCRE is an alliance of American computer companies and allied associations established to inform policy makers and the public about the nature of the computer industry—its products, technological advances, and global business realities.

CCRE strongly supports the export control reform initiative launched by President Obama. The President's decision to modernize the export control system is a major step forward in improving the international competitiveness of American companies and workers, and their ability to innovate while effectively protecting national security. American information technology companies and workers are primed for export expansion and need the Administration to move forward quickly in applying its new control criteria to information technology.

CCRE's members include Dell, Inc., Hewlett-Packard Company, IBM Corporation, Intel Corporation, Unisys Corporation, Information Technology Industry Council, and TechAmerica. CCRE has a long history of cooperation with the U.S. government on security-related technology issues, and it is committed to providing the Administration with the information its needs to develop effective and modern export controls.

Sincerely,

Dan Hoydysh
Chairman, CCRE

A Roadmap for Modernizing Export Controls on Information Products and Technology

CCRE has three specific recommendations for helping the Administration modernize information technology export control that are consistent with national security.

As explained in detail below, these recommendations are based on the fundamental policy conclusions reached by government experts and the reality of global advances in technology; and none of these recommendations require new legislative authority.

These recommendations are supported by a long history of policy reports over the last two decades confirming that the U.S. export control system is outmoded and counterproductive in achieving fundamental national security, foreign policy and economic objectives. Most recently, in 2009, the National Research Council of the National Academy of Sciences concluded:

> *The export controls .... that were crafted to meet conditions the United States faced over five decades ago now quietly undermine our national security and our economic well being.* Beyond "Fortress America", National Security Controls on Science and Technology in a Globalized World

In a speech earlier this year on export controls, Secretary of Defense William Gates emphasized that:

> *... an overly broad definition of what should be subject to export control ... make[s] it more difficult to focus on those items and technologies that truly need to stay in this country. We need a system that that dispenses with the 95% of the easy cases and lets us concentrate on the remaining 5 percent.*

****

1. **Remove performance-based controls on commercial scalar computers and associated technology.** (*Existing foreign policy and nuclear non-proliferation controls would remain in effect.)

This recommendation is based on almost a decade of research and findings by government experts. As highlighted below, these findings have all concluded that access to computing power is so widely available that U.S. export controls on commercial computers are no longer effective and undermine our technology competitiveness and national security.

2001 -- Office of the Deputy-Under Secretary of Defense (Science and Technology): Export Control of High Performance Computing: Analysis and Alternative Strategies

> *After evaluating a number of alternative hardware control strategies, we concluded that it is no longer feasible to control high performance computer hardware. Instead we recommend a focus on protecting our software used specifically for national security purposes.*

2002 – Wassenaar Arrangement

> *With the concurrence of the US, digital computers are removed from the Wassenaar "Sensitive" and "Very Sensitive" lists, reflecting multilateral agreement that computer systems are not "essential for the development, production, use or enhancement of the most advanced conventional military capabilities ..."*

2006 - Under Secretary of Defense, Acquisition, Technology and Logistics Pentagon: Militarily Critical Technologies List

> *Except at the leading edge of the art (large vector supercomputers ...) access to raw computational performance can no longer be effectively controlled.*

The ineffectiveness of US computer export controls in denying access to high levels of computing power is underscored by the fact that foreign computing capability far exceeds US control thresholds. The chart below compares computing power available from Chinese (Lenovo, Dawning, Inspur) and Russian (T-Platforms) companies and the current U.S. export control threshold for computing power. The chart is based on the November 2010 Top500 List of Supercomputers.

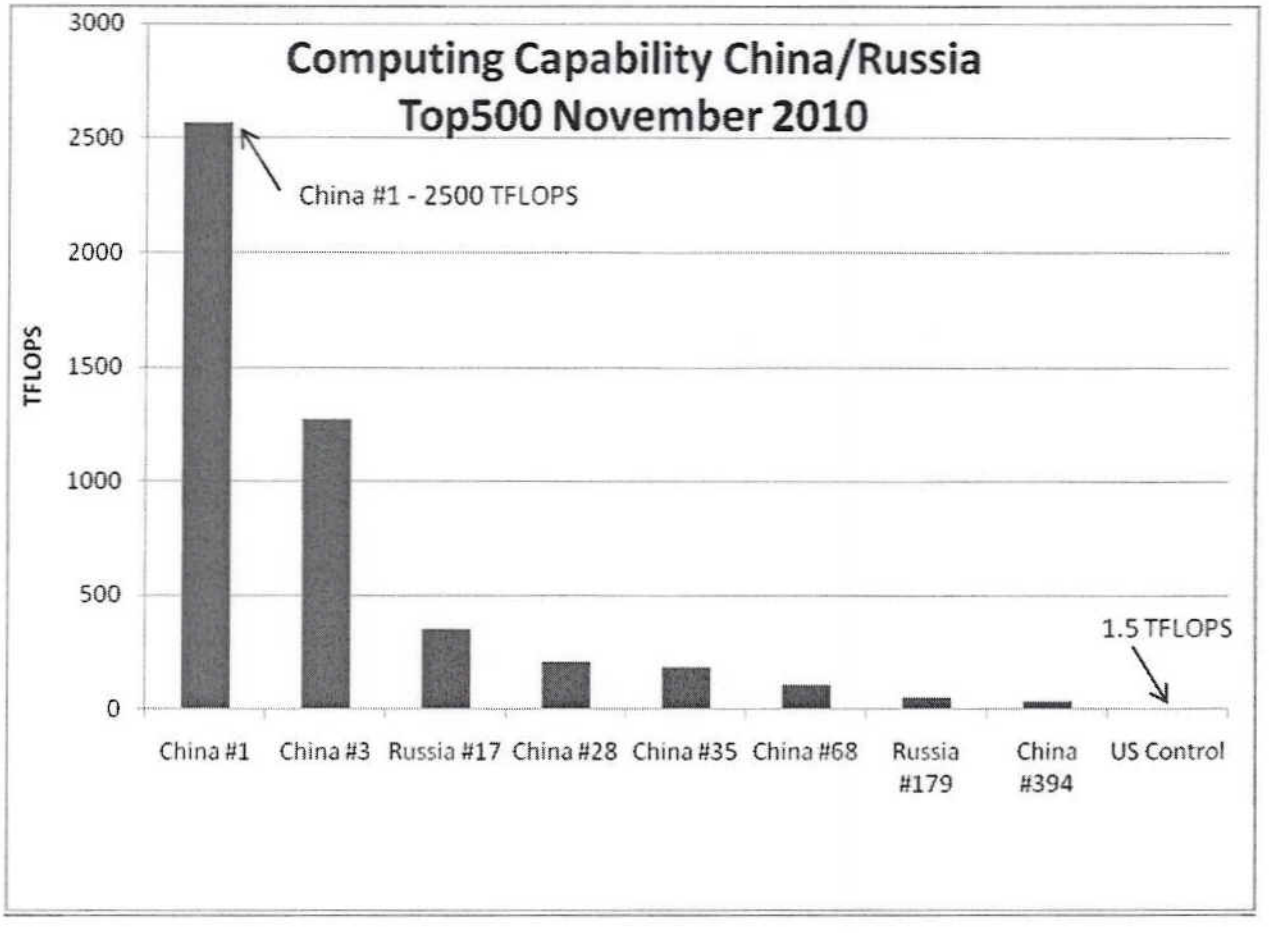
According to the Top500 list, China has the world's fastest supercomputer located at the National Supercomputing Center in Tianjin that can perform over 2,500 trillion operations per second (TFLOPS) -- that is more 1,500 times more power than the current 1.5 TFLOPS US computer export control threshold. China also has the second fastest system rated at over 1,200 TFLOPS. The Russian T-Platforms system, which is the 17th most powerful in the world, is rated at 350 TFLOPS -- more than 200 times the power represented by the US control threshold.

TFLOPS is an industry standard metric for approximating the number crunching capability of computer systems. Actual performance depends on the problem being solved, the software and other architectural factors. However, TFLOPS is recognized as a useful method for comparing computing performance.

Both the Chinese and Russian systems were assembled from widely available commodity motherboards, microprocessors, inter-connects, and open source software. Therefore, US export controls have not and

cannot prevent end users outside the US from developing and accessing computing power that far exceeds the US control threshold.

Moreover, since 2002, there have been no effective multilateral controls on scalar high performance computer systems because the Wassenaar Arrangement, with the consent of the United States, removed computer hardware from both the "Sensitive List" and "Very Sensitive List", of dual-use items. Removal for these lists signifies multilateral agreement that computer hardware is not directly related or essential to the creation of a critical, substantial or significant military- or intelligence-related advantage.



2. Create a practical exception for intra-company sharing of technical information/data and equipment to support the development of new IT products services that does not impose conditions similar to individual or bulk licenses.

The sharing of knowledge within the global operations of U.S. information technology companies is essential to spur innovation and maintain the U.S. industry's global competitiveness and technological

leadership. Technology sharing is at the heart of the industry's 21st century research and development activities, and is fundamental to the industry's world-wide manufacturing and services network.

Over the last decade, government and private sector experts have concluded that the development of information technology is critical to U.S. national and economic security, and that the current export control system undermines U.S. technological leadership.

1999 -- Department of Defense: Defense Science Board Task Force on Globalization and Security

> *[g]lobalization's most significant manifestation is the irresistible leveling effect it is having on the international military-technological environment in which DOD must compete...DOD is relying increasingly on the U.S. commercial advanced technology to push the technology envelop and enable the Department to 'run faster' than its competitors.*

2007 – Department of Commerce Deemed Export Advisory Committee, <u>The Deemed Export Rule in the Era of Globalization</u>

> *In the present environment, most scientific and technologic knowledge and items will not be denied to enemies even by a perfect United States control regime: They will simply be obtained from others.*

Given the global nature of research and development, if U.S. information technology companies continue to be restricted in the sharing of technology within their own operations, there is a serious risk of stifling the U.S. military's rate of technological advancement as well as the industry's international competitiveness. The modernization proposal described above will promote the development of U.S. information technology by facilitating the sharing of technology **within** U.S. companies, both in the United States and overseas. By limiting the sharing to **only** U.S. company operations, the ENC-type license exception will also protect national security interests.

Because U.S. information technology companies already apply a wide-range of internal security measures in both their U.S.-based and foreign-based operations, the risk of misappropriation of technology has been substantially reduced: (a) prescreening employees prior to hiring; (b) employee completion of non-disclosure agreements; (c) internal compliance programs and employee education; (d) physical security measures; (e) computer network security to restrict and monitor access to company restricted databases; (f) content classification of company data and "need to know" access restrictions; and (g) internal audits that verify company policies and programs are being implemented.

These types of business and security practices effectively limit the ability the rogue foreign national employees to access and transfer technical data outside the U.S. enterprise. Preventing corporate intellectual property from misappropriation, regardless of its export control status, is an interest that

industry has in common with the government.

3. **Remove encryption controls on products and components that are, or will be, widely available or deployed, do not contain encryption as their primary function, or are not peculiarly responsible for creating a military- or intelligence-related advantage. Remaining encryption controls should consist of: (A) applying export controls only to a narrow positive list of encryption items; (B) decoupling the export approval process from items where only product information is needed by the U.S. government; (C) expanding mass market treatment to include any item with encryption-related capability that is, or will be, widely available or deployed, whether through retail or other channels; (D) conferring mass market treatment on components with encryption capability that are designed for use in a mass market product, even if the components themselves are not mass marketed; and (E) expanding "ancillary encryption" treatment to include information technology and communications products and components which do not contain encryption as a primary function.**

U.S. export controls on commercial grade encryption are now so outmoded they are undermining U.S. national security as well as the economic competitiveness of American companies producing software applications and commodity products with cryptographic-related functions.

President Obama recognized the critical importance of modernizing export controls on encryption in particular when he spoke earlier this year at the Export-Import Import Bank's Annual Conference:

"First, we're going to streamline the process certain companies need to go through to get their products to market—products with encryption capabilities like cell phones and network storage devices. Right now, they endure a technical review that can take between 30 and 60 days, and that puts that company at a distinct disadvantage to foreign competitors who don't face these same delays."

The Obama Administration has since affirmed that the recent rule implementing this process-based reform "is the first step in the President's effort to reform U.S. encryption export controls to enhance national security by ensuring the continued competitiveness of U.S. encryption products, reducing paperwork requirements for less sensitive encryption items, making the process for submission more efficient, updating the control parameters for controlled encryption items and addressing the impact of export controls on electronic components having encryption functionality. The U.S. Government will also review other issues related to encryption controls, in keeping with national security requirements and multilateral regime commitments."

The revisions requested present an approach more attuned to the current technology landscape. Data storage, computing, data transmission, and networking products increasingly require the security features that standard commercial encryption provides. As more devices are networked, there is ubiquitous need for standard commercial encryption features in everyday computing and

telecommunications devices so as to protect personal data and property. Indeed, the President's cyber security goals are unattainable without them. For example, the semiconductor industry is currently moving toward utilizing encryption features in standard commercial products. Without reform, these products will find themselves re-controlled when they incorporate the encryption features, and we would head towards the exact opposite result from the one sought by the President and his national security team.