The Chemours Company
1007 Market Street
PO Box 2047
Wilmington, DE 19899

302-773-1000 t
chemours.com

August 3, 2015

VIA ELECTRONIC MAIL

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce, Room 2099B
14th Street and Pennsylvania Avenue NW
Washington, D.C. 20230

Re: Revisions to Definitions in the Export Administration Regulations; RIN 0694–AG32

To whom it may concern:

The Chemours Company appreciates the opportunity to submit comments regarding the proposed Revisions to Definitions in the Export Administration Regulations published in the June 3, 2015, Federal Register. The proposed changes seek to "enhance clarity and ensure consistency" with the ITAR. While Chemours supports efforts to harmonize and streamline the regulations, we are particularly concerned about sections 734.13(6), 734.18(a)(4), 734.18(b), and 734.18(c). These sections outline the conditions which make (or do not make) a transfer of technical data or information an export by means of Information Technology (IT) systems requiring access codes, passwords, etc. We caution that the proposed changes to these sections would cause significant resource and financial burden on industry.

A. <u>Proposed Change to §734.13(6)</u>

The proposed language of this section provides:

> "(6) Releasing or otherwise transferring decryption keys, network access codes, passwords, 'software' or other information with 'knowledge' that such provision will cause or permit the transfer of other 'technology' in clear text or ''software'' to a foreign national."

Our interpretation of the text as written is that, after releasing decryption keys, network access codes, passwords, etc., the mere possession of the decryption keys, network access codes, passwords, etc., would not necessarily "cause" a transfer of technology in clear text to a foreign national. However, possession of the decryption keys, network access codes, passwords, etc., would *"permit"* a transfer of technology in clear text to a foreign national despite the owner of the technical data specifically prohibiting their use and access.

Proposed §734.13(6) would severely limit the industry practice of offshore outsourcing of computer systems management and is contrary to current BIS guidance. Current BIS guidance allows computer systems to be managed by restricted foreign nationals provided they do not access and read the files stored in the computer systems. This restriction is customarily a requirement of the service contract with the service provider and the activities performed by IT specialists are monitored or tracked. Additionally, because some information is also business confidential, there are business reasons to have the appropriate contractual terms denying access to files and to strictly enforce compliance with those terms.

Moreover, at a BIS webinar on June 10, 2015, it was stated that proposed §734.13(6) is not a change to BIS guidance and policy regarding foreign computer system management. However, the proposed language does describe a departure from current BIS guidance. If BIS intends to retain the current policy, we suggest that the phrase, "or permit" be omitted from the proposed text of §734.13(6).

B. Encryption in §734.18(a)(4), §734.18(b), and §734.18(c)

These sections describe "end-to-end" encryption as an acceptable way to transmit technical data without creating an export. Encryption of documents poses significant challenges for industry. Maintaining encryption capability adds the required task and expense of maintaining encryption certificates, including tracking expiration dates, funding new certificates and running the implementation process, which may include coordinated testing internally and with business partners to ensure access is not compromised.

Software that generates documents (e.g., Microsoft Word, Microsoft Excel, etc.) are constantly being upgraded and changed by the developer. After several software versions, the encryption keys are incompatible with the document and the document can no longer be accessed. Additionally, when a company is sold or merges with another company, the encryption keys for the company are changed. Again, documents previously encrypted become inaccessible.

If the primary concern is the security of technical data associated with "600 series" items, we submit that encryption should be limited to that particular technical data and not be applied to the entire EAR.

C. Implementation Implications of §734.13(6)

There would be two ways to implement §734.13(6) as written: encryption or separation of controlled technical data into computer systems managed by nationals who fulfill NLR requirements for the control level of the technical data. Some of the encryption issues have been discussed above in Section B. In addition, because encryption would have to be manually applied to each document, retrofitting encryption to documents already stored in computer systems managed by restricted foreign nationals would be a mammoth undertaking due to the massive number documents. Thus, separation of technical data into a separately managed computer system is the only practical way to comply with §734.13(6) as proposed.

Such separation of computer systems would be costly to implement and maintain. Without greater detail regarding programming requirements, we roughly estimate that costs to analyze, create separate computer domains, and move technical data to the correct domain, to be in the tens of thousands of dollars and possibly over one hundred thousand dollars. Additional significant costs will be incurred with the maintenance of separate systems staffed by U.S. or EU personnel. It will roughly increase computer systems costs by 3 to 5 times or hundreds of thousands of dollars above current levels. The increased costs represent the differential between U.S. and EU pay scales and those found in alternative countries. Costs of separating computer systems would also be driven by the size and complexity of the computer systems. Systems include servers (usually local), applications, databases, and back-up systems. The time needed to implement separation would be significant. If required, we estimate needing twelve (12) months to fully separate computer systems.

For the foregoing reasons, Chemours submits that the proposed definition changes discussed in these comments would cause significant burdens on industry and would change current BIS guidance and policy for computer systems management. Therefore, Chemours urges BIS to consider our suggested change to proposed §734.13(6). Thank you for your consideration of these comments. Please do not hesitate to contact me if you have any questions at 302-773-1318.

Sincerely,

/s/ PEDRO DE LA TORRE

Pedro de la Torre
International Trade Counsel &
Global Compliance Officer
The Chemours Company