United Technologies Corporation
1101 Pennsylvania Avenue, N.W.
10th Floor
Washington, D.C. 20004-2545

United Technologies

Submitted Via Email

August 3, 2015

Ms. Hillary Hess
Director, Regulatory Policy Division
Office of Exporter Services
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
Washington, D.C. 20230

Attn: RIN 0694–AG32

Re: Proposed Rule; Comments on Revisions to Definitions in the Export Administration Regulations (80 Fed. Reg. 31505, June 3, 2015)

Dear Ms. Hess:

United Technologies Corporation ("UTC")[1] appreciates the opportunity to submit these comments to the Bureau of Industry and Security ("BIS") on the proposed amendments to the Export Administration Regulations ("EAR") regarding various definitions in order to clarify the scope of activities and information that are covered within these definitions and to harmonize the definitions with the International Traffic in Arms Regulations ("ITAR"). Most significantly, this proposed rule introduces new sections that would exclude from the definitions of export, reexport and transfer (in-country) the electronic transmission and storage of unclassified technical data abroad provided the technical data is sufficiently secured to prevent unauthorized access by foreign persons. The Directorate of Defense Trade Controls ("DDTC") concurrently published proposed amendments to the ITAR to align and harmonize these definitions, including largely parallel treatment concerning the electronic transmission and storage of technology abroad.

UTC supports the objectives of the BIS and DDTC proposed rulemakings to clarify, harmonize and update, wherever possible, common or similar terms and definitions to facilitate enhanced compliance, promote consistency, and reduce regulatory burdens. In particular, we believe the agencies' proposals to address the electronic transmission and storage of technical data are critically important to achieving these objectives. The business and information technology ("IT") environment in which global companies operate has changed profoundly over

[1] UTC is a global, diversified corporation based in Hartford, Connecticut, supplying high technology products and services to the aerospace and building systems industries. UTC's companies are industry leaders, among them Pratt & Whitney, Sikorsky, UTC Aerospace Systems, UTC Building & Industrial Systems, and United Technologies Research Center.

the past two decades. Increased use of electronic modes of collaboration and communication – such as email, web-based portals, networked shared drives, cloud computing, globally connected enterprise resource planning, engineering and manufacturing systems, etc. – has enhanced greatly the ease and frequency of information sharing. In this environment, the physical (geographic) location of information is less relevant than the security conditions governing access to the information. We strongly encourage and support changes to the regulations that recognize these new global business paradigms and evolve relevant EAR and ITAR definitions, policies, and practices to ensure an effective, harmonized export control regulatory system for the 21st century.

A. § 734.18 Activities that are not exports, reexports or transfers – transmission and storage of technical data and software

UTC supports the addition of EAR § 734.18 describing activities that are not exports, reexports or retransfers and, therefore, do not require authorization from BIS. We commend DDTC and BIS for their proposals to address through regulatory changes some of the longstanding and challenging issues facing industry with regard to compliance with export controls when transmitting, storing and managing technical data (and software) in electronic environments. We fully agree with the principle that in an electronic environment, the standards for defining an export, reexport or retransfer, i.e., a controlled event, should focus on the conditions of *access* to the controlled data and software and not just the physical (geographic) location of the digital bits as they move (in motion) or are stored (at rest). The proposed carve-out in paragraph (a)(4) for sending, taking or storing technical data and software that is secured using cryptographic means is a positive step forward.

Encryption is one instrument in UTC's toolset of security measures to secure and prevent unauthorized access to sensitive and proprietary information, including export-controlled data. UTC primarily uses encryption-based tools in high-risk areas such as securing portable media (e.g., laptops, phones, external storage devices, etc.) and certain transmissions within or outside the company network (e.g., Virtual Private Network ("VPN"), Managed File Transfer, etc.). Encryption is applied through security tools in different ways to achieve data protection, whether the underlying data files are encrypted, or the "pathway" for transmitting data or the electronic "container" for storing data is encrypted. In addition, UTC's IT security program employs various other robust data protection measures based on the nature of the IT system or application, technical and performance requirements, and cost of deployment. The tools include logical access controls such as single or multi-factor authentication, password protection with password length and complexity protocols, and other access restrictions. Logical access controls (as opposed to encryption) are heavily used in IT environments in which data is at rest, such as servers, databases, enterprise IT applications.

1. Clarify the Definition of End-to-End Encryption

Paragraph (a)(4)(ii) requires that technical data or software is secured using end-to-end encryption, which is defined in paragraph (b) as "the provision of uninterrupted cryptographic protection of data between an originator and an intended recipient…" The definition goes on to state that "it involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient…" Such uninterrupted protection can be achieved by

encrypting the underlying data files (i.e., the data is not in clear text and is unreadable without the key) or encrypting the transmission pathway or storage device (i.e., the pathway or device is encrypted, and data moving through the pathway or stored on the device cannot be accessed without the decryption key). It is not clear if the proposed definition requires encryption of the data content or permits encryption protection of the pathway or container.

UTC submits that requiring the data itself be encrypted is an overly narrow application of the concept, and is not a widespread practice for securing data at rest (stored) in IT systems. UTC recommends that BIS revise § 734.18(b) to read as follows:

> (b) *Definitions.* For purposes of this section, 'end-to-end encryption' means the provision of uninterrupted cryptographic protection of data between an originator and an intended recipient, including between an individual and himself or herself. It requires that the originating party encrypt the data or otherwise prevent access to the data through cryptographic means to keep that data secured until received by the intended recipient, where the means to access the data in readable form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

The following examples illustrate uses of encryption to secure the pathway or storage media. UTC requires all laptop computers maintain Full Disk Encryption of the hard drive. The entire hard drive is encrypted, so all data and software stored on the hard drive is protected end-to-end although the data files themselves are not encrypted. The employee to whom the laptop is assigned can unencrypt the device by logging into the laptop using their unique network ID and password. Similarly, U.S. person employees on international travel may use a secure VPN connection (i.e., an encrypted tunnel) to access data stored on servers in the United States. Another scenario involves backing up data from a server onto some form of portable electronic media and storing the physical back-up media offsite for disaster recovery purposes. The storage media is encrypted before it is provided to an offsite storage vendor, and remains encrypted at every point during storage unless and until the originator needs to recover the information. We encourage DDTC to clarify the proposed end-to-end encryption standard to encompass cryptographically securing the channel for transmission or the storage medium.

2. <u>Allow Cryptographic Means that are Similarly Effective to FIPS 140-2</u>

The proposed carve-out for transmitting or storing technical data using end-to-end encryption requires that the cryptographic modules be compliant with the National Institute for Standards and Technology ("NIST") Federal Information Processing Standard Publication 140-2 ("FIPS 140-2") or be secured using other "similarly effective cryptographic means." As BIS recognized, although FIPS 140-2 is a widely recognized cryptographic standard used in Federal Government procurement in the United States and for other uses abroad, companies may use hardware and software products that may not be certified to FIPS 140-2 but achieve equivalent encryption-based information security.

As noted above, UTC uses a broad tool set with a variety of solutions to ensure information security for sensitive enterprise data during transmission and at rest. UTC believes

it is important to allow companies the flexibility to use alternate encryption solutions (software and hardware modules) across their IT environment that may not be certified to FIPS 140-2 but provide comparable effectiveness.[2] It would be the responsibility of the exporter to determine equivalent effectiveness. We urge BIS to maintain the proposed language allowing for use of "similarly effective cryptographic means" to secure data and software in transit or at rest, and have recommended that DDTC adopt the same approach in its final rule.

In addition, we understand that an encryption product may lose its certification in certain circumstances, such as when a security flaw is detected. Such flaws are normally patched rapidly, but the product may have to go through a re-certification process. A cryptographic product that is deployed and in use should not be considered ineligible under the carve-out if it temporarily loses FIPS certification but is recertified within a certain period of time (i.e., one year). Likewise, if a product needs to be re-certified to meet a revision of the standard, it should continue to remain eligible.

3. Other Challenges Involving the Transmission, Storage and Management of Technical Data in IT Environments

In explaining the proposed exclusion for certain encrypted data, BIS cites two examples where controlled technical data may be electronically routed through or stored on foreign servers unbeknownst to the original sender. Specifically, the case of email that might transit a foreign country's Internet service infrastructure in route to its intended and authorized destination, and the use of mass data storage (cloud storage) where the controlled data may be stored on servers physically located in a foreign country(ies). There are many other examples involving the electronic movement, storage and access to technical data, driven by the business imperatives for international collaboration across a global IT infrastructure. Although the proposed exclusion of certain encrypted data and software from the definitions of export, reexport and retransfer may not directly address these examples, we encourage DDTC and BIS to consider these scenarios as they develop a final rule and in their ongoing review and update of controls as part of the Administration's Export Control Reform initiative.

- IT datacenter provider hosts servers containing ITAR or EAR data outside the United States. Datacenter employees have physical access to the servers abroad, but cannot access the data stored on the servers due to logical access controls. Database maintenance and other functions requiring access to the data are performed remotely by U.S. persons.

- IT system application hosted on a server in the United States and utilized by non-U.S. subsidiaries. UTC business unit uses an enterprise manufacturing execution system ("MES") to document, control and manage the manufacturing process and work-in-

[2] We understand that FIPS 140-2 establishes a Cryptographic Module Validation Program (CMVP), where third-party accredited laboratories perform validation testing of cryptographic modules (both hardware and software). We also understand NIST maintains validation lists of modules/implementations that receive validation certificates. If the requirement for FIPS 140-2 conformity is retained, we urge DDTC to provide explicit guidance on use of the validation lists to confirm that specific encryption products are certified.

process on the factory floor. The MES application is hosted on a server located in the U.S. Non-U.S. subsidiaries of the business unit engaged in the aftermarket maintenance, repair and overhaul of the company's products use the MES system to create, maintain and execute certain repair processes constituting non-U.S. technical data. The data is created and managed wholly outside the U.S., and personnel at the non-U.S. subsidiary only have access to their repair plans in the MES system. Likewise, business unit personnel in the United States cannot access the data (the MES application employs user-level security controls). In this scenario, non-U.S.-origin data, which is not accessed or in any way manipulated in the U.S., should not fall under jurisdiction of the U.S. export control regulations solely because the servers are physically located in the U.S.

B. § 734.3(b), Note to (b)(3) Items subject to the EAR

In a final rule published in June 2014, BIS added a sentence to the definition of "technology" to clarify that "technology" also includes specific information necessary for operation, installation, maintenance, repair, overhaul, refurbishing, or other terms specific in Export Control Classification Numbers ("ECCNs") on the Commerce Control List ("CCL") that control "technology."[3] BIS also added Note 2, which stated that "technology" not elsewhere specified on the CCL is designated as EAR99. The preamble stated that note did not change the definition but, together with the new sentence, was intended to provide "additional guidance on the application of the definition based on current BIS practice and past interpretive guidance BIS has provided[.]" BIS now proposes to add a Note to EAR § 734.3(b)(3) to make explicit that information that does not meet the definition of "technology" is not subject to the EAR. UTC appreciates this clear statement regarding BIS' change in practice and brings to your attention two situations that are impacted by this shift.

First, in a final rule published in August 2014, BIS added ECCN 0A998 to control specific oil and gas exploration items, including data.[4] This entry is specifically intended to control information that does not meet the definition of "technology." In the preamble to this rule, as well as in Q18 of BIS' Frequently Asked Questions for the Russia Sanctions, BIS states that this data is a "commodity." However, with this new note, companies with data classified as ECCN 0A998 would likely determine that their data would not meet the definition of "technology" and conclude that such data is not subject to the EAR. It would be inconsistent to determine otherwise in the clear face of the new language.

Second, UTC notes that the Office of Foreign Assets Control's definition of "informational materials" largely relies upon whether an item is subject to the EAR. This new note potentially creates a situation where information that is of a technical nature but not "technology" and not publicly available would be considered "informational materials" and, therefore, eligible for export to a sanctioned country without a license.

---

[3] Corrections and Clarifications to the Export Administration Regulations; Conforming Changes to the EAR Based on Amendments to the International Traffic in Arms Regulations. 79 Fed. Reg. 62612 (June 5, 2014). The sentence added by the June 4 rule is currently designated as Note 1 to the definition of "Technology."

[4] Russian Oil Industry Sanctions and Addition of Person to the Entity List. 79 Fed. Reg. 45675 (Aug 6, 2014).

C. § 734.20 Definition of Permanent and Regular Employee

On October 31, 2013, BIS published updated guidance on its website regarding deemed reexports of technology in order to harmonize with certain ITAR definitions as part of Export Control Reform.[5] In Section V.D of this guidance, BIS referenced DDTC's definition of "regular employee" in ITAR § 120.39 and defined the phrase "permanent and regular employee" for purposes of the EAR. UTC notes that BIS has now included a definition for "permanent and regular employee" in EAR § 734.20(d)(2). We also note use of this term in EAR §750.7(a), as well as a slightly different construction - "*bona fide* regular and permanent employee" – in EAR §§734.20(b)(2) and (c)(2). UTC recommends consistent use of the defined term and also that the term be changed to "regular employee" in all instances because it: (1) maximizes harmonization with the ITAR; and (2) is more accurate because individuals hired by a staffing agency are included and such contract labor are not permanent.

DDTC published a proposed rule in May 2015, which modified its definition of "regular employee" by clarifying that the phrase "long term" indicates that contractual relationship is intended to be one year or longer.[6] UTC commented that DDTC include the phrase "or other contract employee provider" after each reference to "staffing agency" because it reflects DDTC's current interpretation.[7] UTC also proposed that DDTC include a Note at the end of the definition to clarify that the contractual relationship can be with the individual, the staffing agency, or other contract employee provider because a company would be more likely to enter into a contract with the staffing agency or contract employee provider, rather than the individual. Consistent with our comments to DDTC and to further harmonize the definitions in the ITAR and EAR, UTC recommends that BIS revise EAR § 734.20(d)(2) to read, as follows:

(2) "*Regular employee*" means an individual who:
(a) is permanently and directly employed by the company, or
(b) is in a long-term (*i.e.,* 1 year or longer) contractual relationship with the company where the individual:
(i) works at the company's facilities or at locations assigned by the company (such as a remote site or on travel);
(ii) works under the company's direction and control;
(iii) works full time and exclusively for the company;
(iv) executes a nondisclosure certification for the company; and
(v) where the staffing agency or other contract employee provider that has seconded the individual (if applicable) has no role in the work the individual performs (other than providing that individual for that work) and does not have access to any "technology" other than where specifically authorized by a license or other approval.

---

[5] Updated BIS Guidance Regarding the Treatment of Dual and Third Country Nationals with Respect to Deemed Reexports of Technology or Source Code Subject to the EAR (Oct. 31, 2013). *See* https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-reexport-guidance1.

[6] Amendment to the International Traffic in Arms Regulations: Registration and Licensing of U.S. Persons Employed by Foreign Persons, and other Changes. 80 Fed. Reg. 30001 (May 26, 2015).

[7] Section 3.9 of DDTC's *Guidelines for Preparing Electronic Agreements* states that individuals can be hired through staffing agencies "or other contract employee providers."

Note to paragraph (d)(2): The contractual relationship can be with the individual, the staffing agency or other contract employee provider.

D. §§ 734.13 Export, 734.14 Reexport

UTC understands that the intention of EAR §§ 734.13(a)(6) and 734.14(a)(4) is to make the provision of the means of access (*e.g.,* providing decryption keys, passwords, network access codes, etc.) to encrypted data an "export" or "reexport." For consistency, UTC recommends that BIS utilize the same word construction from the definition of "technology" in §§ 734.13(a)(6) and 734.14(a)(4). This would also align better with the proposed counterpart provisions in ITAR §§ 120.17(a)(6) and 120.19(a)(4).

BIS has maintained a long-standing position of drawing a distinction between actual access and potential access. UTC understands that BIS intends to retain this distinction, as BIS explains that the "mere act of providing physical access to unsecured "technology" will not, however, be a controlled event…." However, the current proposal defines an export (and reexport) to be the provision of the means of access with "knowledge" that it "will cause or permit" the transfer of controlled technology. UTC believes that this phrasing is confusing and appears to undercuts BIS' existing position. First, it is unusual for BIS to include a knowledge standard outside of catch-all, end-use or end-user controls. Second, the language does not account for whether the recipient has accessed the controlled technology and "permit" may include situations where the foreign national has the ability to access the "technology" but does not.

The distinction between DDTC's and BIS' position on access is important and UTC believes it merits sufficient explanation directly in the EAR. Therefore, UTC recommends that BIS revise EAR § 734.13(a)(6) to read, as follows, and that conforming changes be made to § 734.14(a)(4):

> (6) Releasing or otherwise transferring information (e.g., decryption keys, network codes, passwords) or "software," or otherwise providing access to other "technology" in clear text or "software" to a foreign national.
>
> **Note to paragraph (6):** The mere act of releasing or otherwise transferring the information (e.g., decryption keys, network codes, passwords) or "software," or otherwise providing means of access, is not a controlled event until the foreign national applies it and accesses the "technology" in clear text or "software."

In comments submitted in response to DDTC's companion rule, we encourage DDTC to adopt the BIS formulation to achieve a common, harmonized standard in this area.

E. § 740.9 Temporary imports, exports, reexports and transfers (in-country) (TMP)

1. <u>Remove additional documentation requirement for foreign nationals</u>

UTC acknowledges that existing § 740.9(a)(3)(i)(B) already includes additional recordkeeping requirements that only apply to foreign nationals. This requirement has been carried over into proposed § 740.9(a)(3)(v). UTC does not agree with this requirement because it: (1) creates a different standard for use of the exception for foreign nationals that does not apply to U.S. persons employed by the same employer; (2) is redundant to the requirement set forth in § 740.9(a)(3)(i); and (3) imposes an extra burden on the employer upon each instance of travel to document an underlying premise that has already been established – namely, that the foreign national requires the technology for their activities abroad on behalf of the employer. If there was no need for the foreign national to have the technology, the authorization would not be in place and the requirement in § 740.9(a)(3)(i) would not be satisfied. Therefore, UTC recommends that subparagraph (v) be removed.

UTC also recommends that reexports and transfers (in-country) remain in scope of the exception. Currently, EAR §740.9(a)(3) authorizes use of the exception for "exports, reexports, and transfers (in-country)." However, BIS has narrowed the scope of this exception to exports, which limits the activity to shipments/transmissions out of the United States. This change effectively excludes from its scope that which is permissible today, which will have a negative impact on U.S. person employers. The change would mean that an employee would be limited to export activity and would not be able to transfer the technology to authorized persons or travel onward to third countries with the same technology.

2. Expand scope to include foreign subsidiaries and affiliates of U.S. persons

UTC notes that EAR § 740.9(a)(3)(iii) restricts only U.S. persons to employment by the U.S. government or a U.S. person employer, with no similar restriction on foreign nationals. We believe this is an oversight and the intention is to cover both U.S and foreign national employees. This can be corrected by using the term "individual" to reference the employee in this subparagraph. However, UTC recommends that BIS expand this exemption to include foreign subsidiaries and affiliates of U.S. persons.

If the condition in subparagraph (i) is met – that the foreign national is already authorized to receive the technical data - then the U.S. Government has already determined that such person is "trusted." Accordingly, if the additional conditions in subparagraph (ii) are met with respect to use and security precautions, the risk of permitting employees of foreign subsidiaries and affiliates of U.S. persons to travel abroad with technology is no different than permitting employees who are working for U.S. affiliates to travel abroad. The U.S. person assumes responsibility as a licensee when its companies engage in activities under the U.S. person's EAR licenses in accordance with EAR § 750.7(d). Permitting foreign subsidiaries and affiliates of U.S. persons to have a similar authorization as U.S.-based affiliates for employees to travel with EAR technology under prescribed circumstances would greatly benefit global enterprises.

3. Remove requirement to encrypt technical data from security measures

UTC concurs with incorporating affirmative obligations to secure technology. In addition to export compliance considerations, use of security precautions such as firewalls, use of passwords and secure network connections are sound information security practices intended

to prevent unauthorized access to intellectual property, business proprietary information, technology and other types of confidential information. Among the types of security precautions identified in the proposed rule is encrypting the technology. UTC is unclear whether BIS' intention was that they underlying information be separately encrypted while at rest, in addition to securing the "pathway" to access the technology. UTC submits that requiring that the underlying technology also be encrypted is disproportionately burdensome. Further, if the pathway to access the technology is properly secured by use of secure network connections, firewalls, passwords and the like, separately encrypting the technology at rest should not be mandatory.

As written, § 740.9(a)(3)(ii) appears to be a proscriptive list of security techniques, requiring all to be used, which may not be effective, practical, or even necessary, depending on the application. This may not have been BIS' intent, but it is the meaning of the entry. UTC recommends revision to clarify that adequate security measures need to be used but that companies can choose which measures should be implemented.

For the reasons described above, UTC recommends that § 740.9(a)(3) be modified to read as follows:

> (a) ***
> (3) "Technology," regardless of media or format, exported, reexported, or transferred (in-country) by or to an individual who is travelling or on temporary assignment abroad subject to the following restrictions:
>
> > (i) The individual is a "regular employee" of the U.S. government or a U.S. person (including foreign subsidiaries and affiliates of a U.S. person).
> >
> > (ii) Foreign nationals may only export, reexport or receive such "technology" as they are authorized to receive through a separate license or other approval.
> >
> > (iii) The "technology" exported or reexported under this exception is to be possessed or used by the employee. Any such "technology" may be retransferred by the employee to a third party, only if there is a separate license or other approval for the third party to receive the "technology."
> >
> > (iv) Sufficient security precautions are used to prevent unauthorized access to the "technology." Such security precautions may include encryption of the "technology;" the use of secure network connections, such as virtual private networks; the use of passwords or other access restrictions on the electronic device or media on which the "technology" is stored; or the use of firewalls.
> >
> > (v) "Technology" authorized under this exemption may not be used for foreign production purposes or for defense services unless authorized through a license or other approval.

F. § 772.1 Definition of Peculiarly Responsible and Required

UTC commends BIS for the effort to clarify the interpretation of the term "required," and to harmonize the interpretation with a proposed new definition in the ITAR. However, we believe that defining "peculiarly responsible" using a "catch and release" format has serious drawbacks, and recommend that the proposed definition be deleted.

In some cases, the proposed definition "peculiarly responsible" will control more than is currently captured under the EAR's definition of "Required." The performance levels, characteristics, or functions of "technology" can be controlled higher than the commodities that result from the "technology." For example, ECCN 9E003.a.5 is "technology" for the "development" and "production" of cooled turbine blades, vanes, and tip shrouds and controlled as National Security 1. Such commodities, when part of a production 9A991.c or .d engine, are themselves 9A991.c, an AT-only control. Per the proposed item (3) release of "peculiarly responsible," because the 9E003.a.5 "development" and "production" data is used in or with the AT-only commodity, such data cannot be "peculiarly responsible" and, therefore, it cannot be "required" for 9E003.a.5. Further, per the BIS Advisory Opinion of March 25, 2014, the term "required" applies to all ECCNs controlling "technology" regardless of whether the ECCN specifically refers to the GTN or uses the term "required." As the information to design or produce the turbine components is not "required", it falls to EAR99. We believe this clearly is not the intent of the proposed definition.

The proposed definition as stated would make the General Technology Note (GTN) an empty box. The GTN controls "technology" "required" for the "development", "production", or "use" of a controlled product, even if that "technology" is applicable to a product controlled at a lower level. In order for the GTN to apply, the subject "technology" must be "required." Per the definition, if that information is used in or with (i.e., applicable to) a production AT-only item (i.e., item of lower control), the information is not "peculiarly responsible' and, therefore, not "required" per the item (3) release. Additionally, releases (4) and (6) would make information not "peculiarly responsible" and, therefore, not "required" simply by documenting contemplated applications of the technology to AT-only commodities, again making the GTN an empty box.

The proposed definition also may result in over-control of certain technologies. Consider information unique to the production of a blade meeting the temperature thresholds in 9E003.a.4, but which in unrelated with the temperature capabilities of the blade. For example, instructions for grinding off excess metal from the fir tree portion of the blade after casting. Under the current definition, such information is necessary for the production of the blade, but contributes nothing towards the ability of the blade to meet or exceed the temperature threshold that triggers control and, therefore, would not be considered 9E003.a.4 technology. Under the proposed definition, since the information is used in production of the controlled blade, it is "caught," and because it is unique to that particular blade, it would not be released. Under the proposed definition, the information would be considered "peculiarly responsible" and would be controlled under ECCN 9E003.a.4

Further, under the proposed "catch" in the definition, an item is "peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions" if it is

used in or for use in a variety of EAR activities. In this structure, the capability or lack thereof of the item to "achieve or exceed the controlled performance levels…" is replaced by the basic test of the item being "used in or for use in" various EAR activities. The capability threshold is rendered meaningless for purposes of the "catch," which would result in capturing all of the "mundane" technical data necessary to produce the part, but not "required" under the present definition. This is a significant increase in the scope of "required." Of course, much of this mundane technology would be "released" in paragraphs (1) through (6), but that would require an extensive analysis of all the technology associated with the item, which would be a significant and unnecessary additional burden over the status quo.

Additionally, the "catch-and-release" format of the proposed definition would overly complicate "specially designed." The term 'peculiarly responsible' appears in the EAR in only two places – the defined term "required" and in the 'catch' paragraph (a)(1) of "specially designed" (and subsequent clarifying notes). The effect would be that when analyzing an item against "specially designed", the 'catch' paragraph would require an additional 'catch and release' analysis of "peculiarly responsible" before moving on to the 'release' of "specially designed." To further complicate matters, the proposed "peculiarly responsible" has a catch for items (i.e., commodities, software, and technology), releases for items (1), (4), (5), and (6), and the (3) release is reserved for "information." This will greatly complicate any "specially designed" analysis. If BIS does not intend for the term "peculiarly responsible" in "specially designed" to reflect the defined term, the use of the same term in different ways will cause confusion.

The last drawback is one of style and construction. We believe a defined term ("required") should not be defined directly by yet another defined term ("peculiarly responsible.") UTC proposes maintaining the EAR's existing definition and illustrative example of "required" technology, and eliminating the proposed definition of "peculiarly responsible."

G. § 772.1 Definition of Proscribed Person

BIS has proposed a new definition for "proscribed person" as "a person who is prohibited from receiving the items at issue or participating in a transaction that is subject to the EAR without authorization by virtue of U.S. law, such as persons on the Entity List, Specially Designated Nationals, or debarred parties." UTC finds the wording to be overly broad and the illustrative examples to be potentially confusing because they appear to: (a) define a person as a "proscribed person" if they are designated on a list pursuant to *any* U.S. law, some of which may have no export control nexus; and (b) bring activity that might otherwise not be prohibited by the EAR within the scope of the EAR. For example, the Office of Foreign Assets Control is primarily responsible for designating and maintaining lists of Specially Designated Nationals ("SDNs") under the various sanctions programs it implements. U.S. persons are generally prohibited from engaging in transactions with SDNs, but these prohibitions do not extend to the provision of items subject to the EAR to SDNs by foreign persons absent a specific prohibition in the EAR. UTC notes that BIS has targeted only certain Executive Orders and SDN programs in Part 744 (*e.g.,* §§ 744.8, 744.12, 744.14). If a broader prohibition existed in the EAR to cover all SDNs, those specific provisions would not be necessary.

Although UTC would agree with such an outcome for SDNs, there are lists implemented pursuant to other U.S. laws with no nexus to export control. For example, a person listed in the Excluded Party List System (now managed by the System for Award Management) is "debarred" under U.S. law but such debarment typically pertains to government contracting or prohibits the party from receiving certain government benefits or grants for reasons that have no connection to export control laws. Absent action by BIS to debar the person or identify the person on a list managed by BIS, UTC submits that such a person is not a "proscribed party." However, this definition may create confusion due to its generic reference to "debarred parties." UTC recommends that BIS revise the definition of "proscribed person" by deleting the phrase "by virtue of U.S. law" and removing references to SDNs and debarred parties.

BIS has revised EAR § 750.7(a) to specify that a license authorizing release of technology to an entity also authorizes the release of the technology to the entity's foreign nationals who are permanent and regular employees and who are not "proscribed persons under U.S. law." As written, this language appears to impose an obligation on the license applicant to ensure that a third party's foreign nationals are not "proscribed persons." UTC objects to any requirement that an applicant must directly screen the foreign nationals of an entity that will receive technology under its license. Conducting such screening would require the entity to provide a <u>by name</u> list of such employees, and potentially additional personal information as may be needed for the applicant to verify whether a potential match is in fact a true match to a "proscribed person." Not only would this be impractical and burdensome for the applicant, it may violate the anti-discrimination, human rights and privacy laws of the countries in which those foreign nationals are resident. If the entity receiving the technology is to conduct the screening directly, EAR § 750.7(a) provides no clear statement to that effect and the entity may also be similarly constrained from conducting such screening pursuant to domestic law.

Complexities raised by this proposed language include whether an applicant is prohibited from providing technology to an entity that refuses to provide the names of its employees for screening by the applicant or refuses to screen them directly, and whether it is adequate for an entity to provide assurances that none of its employees are "proscribed parties" or some general certification regarding EAR compliance. If this change is to become final, BIS needs to provide specific guidance to industry on how this obligation is satisfied.

UTC notes that the phrase "proscribed person under U.S. law" is also used in EAR §§ 734.20(b)(2) and (c)(2). For the reasons already articulated above, UTC believes that this screening requirement will pose significant challenges for foreign persons to implement. Consistent with the changes that UTC recommends above to the definition of "proscribed person," UTC further recommends that "under U.S. law" be deleted in each instance where BIS uses the phrase "proscribed person under U.S. law" in the EAR.

H. § 772.1 Definition of Technology

Paragraph (a)(1) defines "technology" to include "information gleaned through visual inspection." UTC recommends replacing the word "gleaned" with "revealed" in order to align with the language used in the proposed definition of "release" in EAR § 734.15(a)(1). The use

of the term "glean" implies the value of the information is based on the capability of the viewer, which is unknowable and unquantifiable. The use of the term "reveal" is a more objective measure of what information is provided by the visual inspection.

In the Note to Paragraph (a)(1), because "development" stops short of serial production, the term "production" must be added, otherwise the instructions for the serial production of Y by modifying existing stocks of X would not constitute technical data under the ITAR. UTC suggests the following revision:

> NOTE TO PARAGRAPH (a)(1): The modification of an existing item creates a new item and technical data for the modification is technical data for the development or production of the new item.

Paragraph (b) defines specific types of information that do not constitute "technology," including in (b)(1) "non-proprietary general system descriptions." We recommend that the modifier "non-proprietary" be deleted, as the way a company chooses to restrict such information in non-public settings has no bearing on whether the information is technical data or not. General system descriptions may be included in various types of business documents, such as proposals, that are treated as proprietary for commercial reasons. It is understood that the term "general" may cause confusion as to the bounds of "general system descriptions," but the addition of "non-proprietary" does not provide clarification. Additionally, it should be made clear that the exclusion is not limited to "systems," as the defined term is used, but also should cover general descriptions of parts, components, accessories, attachments, firmware, software, and end-items.

* * *

For additional information, please contact the undersigned at (202) 336-7467 or peter.jordan@utc.com or Christine Lee at (202) 336-7458 or christine.lee@utc.com.

Sincerely,

Peter Jordan
Director, Senior International Trade Counsel