COVINGTON

Microsoft Office 365 and U.S. Export Controls

David Addis
Peter Lichtenbaum
Covington & Burling LLP

With contributions from:
Anne Marie Griffin
Nathan Leong
Microsoft Corporation

Microsoft Office 365 and U.S. Export Controls

December 1, 2016

This paper offers a brief overview of U.S. export control laws and regulations as they may apply to use of Microsoft Office 365, with some general guidance concerning the considerations that Office 365 customers should bear in mind to assess their obligations under U.S. export controls.

U.S. export controls are laws and regulations to control the export and transfer of items from the United States or to non-U.S. persons, in the interest of protecting U.S. national security and furthering U.S. foreign policy and other interests. U.S. export controls apply not only to traditional cross-border shipments of physical goods, but also transfers, uploads or downloads of software and data. That includes transfers, uploads or downloads of software or specific technical data using cloud-based services.

Office 365 is a cloud-based "Software as a Service" platform that includes the transmission of customer data across the Internet to and from Microsoft's cloud infrastructure and the storage and processing of customer data on Microsoft's cloud infrastructure. The focus of this paper is on Office 365-branded plans or suites intended for organizations (such as Exchange Online and SharePoint Online), rather than consumer Office 365 offerings such as Office 365 Home or Office 365 Personal. The Office 365 suite of cloud products makes use of physical infrastructure that is located inside and outside of the United States, and some Office 365 service operations personnel are non-U.S. persons who may in some cases have access to customer data. Organizations and enterprise customers may therefore need to consider whether and how U.S. export controls may apply to their organization's use of Office 365, as explained in more detail in the paper that follows. With appropriate planning, customers can use Office 365 tools and their own internal procedures to help ensure compliance with U.S. export controls when using the Office 365 platform.

1. Executive Summary

As the first step, customers should consider whether any of the data they want to use or store in the Office 365 cloud may even be subject to export controls. U.S. export controls are intended to cover specific, non-public technical information for production or development of a controlled product, and most types of customer data used or stored in the Office 365 cloud are not the kind of specific technical data that is subject to U.S. export controls. Many customers will face little or no export control risks from use of the Office 365 cloud, because most or all of their data in Office 365 is business or financial information that is simply not controlled for export at all.

Moreover, even when technical data is covered by U.S. export controls, in most cases export licensing is required only for export, reexport or transfer to a small number of countries that

are subject to U.S. sanctions. Office 365 does not have infrastructure to store or process data in any of these locations.

Where technical data subject to tighter U.S. export controls may be involved, Office 365 is configured to offer features that help mitigate the potential risk that customers may inadvertently violate U.S. export controls when uploading or downloading controlled technical data in Office 365. For example:

- For customers in North America, customer data is stored at rest in the United States, which minimizes transfer of controlled technology/technical data outside the United States. Similarly, customers in other regions (called "Geos") also have information about the places their customer data may be stored at rest, as described in the Office 365 Trust Center.

- Microsoft implements a range of policies and security practices that strictly limit access to customer data by service operations personnel, including built-in controls that grant such personnel the "least privilege" access to the service, "just-in-time" accounts that strictly limit the time for access for a limited amount of time, and controlled access to take specific actions based on a defined role and task. Customer Lockbox is an optional feature that allows the customer to approve or reject access requests to customer content during service operations by Microsoft.

- Microsoft carries out background checks on all U.S.-based employees who have the potential to access customer data, including checks against export-related lists maintained by the Departments of Commerce, State and Treasury.

- Data Loss Prevention ("DLP"), developed to help organizations protect sensitive information and prevent its inadvertent disclosure, may provide ways for some customers to limit export compliance risk. DLP tools allow customers to conduct searches using key words that may help identify controlled technical data, or tag documents or data when the customer (using its own independent process) has determined the document or data is subject to export controls. DLP tools can also be used to prevent transfer of the designated data, and/or notify individual customers of potential controls before any transfer.

- Office 365 offers end-to-end encryption features that can provide customers with significant technical measures to manage and help protect against U.S. export control risks, as enabled by the new EAR rules regarding "End-to-End Encryption" discussed in this paper.

- Microsoft offers specialized Office 365 solutions and delivery models, including the Office 365 Government Federal offering, that are designed to support ITAR and other controlled data categories.

- Microsoft is ready and able to work with customers to develop a customized "hybrid solution" that uses a mix of servers and resources on the customer's own premises together with cloud-based resources and services.

These features and the ways they can help some customers mitigate export control risk are all described in more detail in the rest of this paper. However, it is important to recognize that the nature of the Internet and cloud-based services means these measures cannot eliminate the customers' risk entirely. Accordingly, Office 365 customers should consider the summary below and carefully monitor the export control requirements for any data that they place into the Office 365 cloud to ensure compliance with U.S. export controls.

2. What are U.S. export controls?

The primary U.S. export controls with the broadest application are the Export Administration Regulations ("**EAR"**), administered by the U.S. Department of Commerce, and this paper summarizes the ways in which the EAR may impact the use of cloud-based services like Office 365.

The United States also has separate and more specialized export control regulations that govern the most sensitive items and technology. For example, the International Traffic in Arms Regulations ("**ITAR"**), administered by U.S. Department of State, impose controls on the export, temporary import, reexport and transfer of many military, defense and intelligence items (also known as "defense articles"), including related technical data. Other U.S. regulations impose export controls focused on specific industries, including nuclear energy.

Microsoft offers Office 365 options and delivery models designed to support ITAR and other controlled data categories, including the Office 365 Government Federal offering, or hybrid models, discussed in Section 5 below. This paper focuses on compliance with the EAR export controls, discussed next.

2.1. The Export Administration Regulations ("EAR")

The EAR impose controls on the export and reexport of most commercial goods, software and technology, including so-called "dual-use" items that can be used both for commercial and military purposes as well as certain defense items. The EAR broadly govern exports from the United States; reexports or retransfers of U.S.-origin items and certain foreign-origin items with more than a *de minimis* portion of U.S.-origin content; and transfers or disclosures to persons from other countries. U.S. export controls apply not only to traditional exports or transfers of commodities and hardware, but also transfers, uploads or downloads of software, and transfers or disclosures of defined "technology" and "technical data"—all core features of cloud computing services.

2.2. "Technology" / "technical data" subject to EAR export controls

In ordinary usage, "technology" may refer to hardware and software that provide technical solutions. But the EAR define the term "technology" to mean "information" only, distinct from hardware and software. More specifically, the EAR define "technology" subject to U.S. export controls as "[i]nformation necessary for the 'development,' 'production,' or 'use' of a product." (For this purpose, technical information that is only for operation of any item is not considered "use" technology unless it also provides information concerning its installation, maintenance, repair, refurbishing and overhaul.) "Technology" may take the form of "technical data" in a variety of forms, including blueprints, plans, diagrams, models, formulas, tables, manuals and instructions.

Information that is publicly available is generally not subject to U.S. export controls.

2.3. "Export" and "reexport" / "retransfer"

Under U.S. export controls, an "export" includes the actual shipment or transmission of U.S. items from the United States to another country. But exports are not limited to the traditional transportation of physical objects across national boundaries. "Exports" subject to U.S. export controls also include transfers, uploads or downloads of technology/technical data to locations outside the United States, and transfers, releases or disclosures of technology/technical data or source code to persons or locations outside the United States.

Similarly, a "reexport" or "retransfer" subject to U.S. export controls includes the actual shipment or transmission of U.S. items, software or technology from one non-U.S. country to another non-U.S. country, or in some cases the transfer of items to an unauthorized end-use or end-user.

2.4. "Deemed" exports / reexports

The EAR also control "deemed" exports and reexports. A deemed export is the release, transfer or disclosure (including oral and visual disclosures) of technology/technical data or source code to a foreign national in the United States. A deemed reexport is a release, transfer or disclosure of U.S.-origin technology/technical data or source code in one foreign country to a national of a different foreign country. Such a deemed export or reexport generally is subject to the same requirements as an export made to the home country or countries of the foreign national.

The "release" of technology or software can occur through visual inspection or electronic exchanges of information in the United States or abroad. The inspection must actually reveal controlled technology or source code to a foreign person. Accordingly, mere ability to access data without actual access, or actual access with limited exposure that is not sustained or complete enough to reveal the controlled technology or source code, would likely not constitute a "release" that results in a deemed export or reexport. In addition, new EAR rules effective September 1, 2016 now permit a company broad latitude to disclose technology to

that company's own employees without triggering deemed reexport licensing requirements, provided certain compliance measures are implemented.

For purposes of the EAR deemed export rules, a "U.S. person" is (1) an individual who is a U.S. citizen, U.S. permanent resident (*i.e.*, green-card holder), or protected individual under the Immigration and Naturalization Act; (2) a corporation, business association, partnership, society, trust, or any other entity, organization, or group that is incorporated under U.S. law; or (3) any federal, state, or local governmental entity in the United States.

A "foreign person" or "foreign national" is any person or entity that is not a U.S. person as defined above. A foreign national working for a U.S. company remains subject to U.S. export controls for potential "deemed exports" even if the foreign national is located and legally employed in the United States under a visa.

2.5. New EAR Amendments effective September 2016

New EAR rules adopted in June 2016 and effective September 1, 2016 may directly impact the use of cloud-based services. The new rules provide that "[s]ending, taking, or storing" EAR-controlled technology or software will not be considered an export, reexport or transfer that is subject to EAR regulation ***provided that*** it meets certain criteria: the technology or software must be (i) limited to information or software that is unclassified (i.e., not a government secret); (ii) secured using "end-to-end encryption" that meets NIST or equivalent standards; and (iii) not "intentionally" stored in any one of 25 designated countries.[1]

"End-to-end encryption" means that the data must not be unencrypted (i.e., in clear text) at any point between the originator's "in-country security boundary" and the recipient's "in-country security boundary," and the means of decryption must not be provided to any third-party. For example, when a customer's encrypted data is uploaded to the cloud, the customer may be the originator while the cloud provider is the recipient; when that customer downloads encrypted data from the cloud to its local "security boundary," the cloud provider may be the originator and the customer is the recipient. Where encrypted data is transferred between different nodes or "security boundaries" of the same company, or different nodes in the cloud, the originator and recipient can be the same entity.

The Commerce Department has advised that the rule is intended to have "a major positive effect on the management and use of many cloud services," and says that it "is consistent with the common practices in both the government and industry, [and] allows for desired or necessary services to be performed within security boundaries."

It is important to note that the local network within the security boundary -- the area in which decrypted/plaintext data can be processed -- must be limited to a single country, and may not

[1] Currently Russia and the "Group D:5" countries Afghanistan, Belarus, Burma (Myanmar), Central African Republic, China, Congo, Cote d'Ivoire, Cuba, Cyprus, Eritrea, Haiti, Iran, Iraq, Lebanon, Liberia, Libya, North Korea, Somalia, Sri Lanka, Sudan, Syria, Venezuela, Vietnam and Zimbabwe.

allow unencrypted data to cross national boundaries. As explained in the preamble to the BIS rule: "A consequence of this requirement is that data eligible for the carve-out must by definition be encrypted before crossing any national boundary and must remain encrypted at all times while being transmitted from one security boundary to another. This principle applies to transmissions within a cloud service infrastructure, where a transmission from one node or cloud infrastructure element to another could qualify for the carve-out provided that it was appropriately encrypted before any data crossed a national border."

The new rule also requires that the technology and software cannot be "intentionally stored" (even in encrypted form) in 25 designated countries, including China and Russia. However, the new rule expressly provides that data "in-transit via the Internet" is not treated as "stored." Thus, for example, encrypted files containing controlled technology temporarily cached on a server outside the approved list of countries while transiting the Internet could still be eligible for this carve-out.

3. Office 365 and the "cloud"

Cloud computing brings together technology solutions in new ways to deliver new efficiencies. The National Institute of Standards and Technology (NIST) defines the key features of cloud computing as customer-directed, on-demand network access to a shared pool of configurable computing resources (including networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing services can be offered in several different models: Microsoft Office 365 is an example of "software as a service (SaaS)" that allows the customer to use the provider's applications on cloud infrastructure. Other models for cloud services include "platform as a service (PaaS)," which allows the customer to deploy its own applications onto the provider's cloud infrastructure; and "infrastructure as a service (IaaS)," which allows the customer to deploy and run its own software environment, including both operating systems and applications, on the provider's cloud infrastructure.

Microsoft Office 365 is a cloud-based SaaS platform designed to help meet an organization's needs for robust security, reliability, and customer productivity with a range of software-as-a-service products, including Exchange Online, Exchange Online Archiving, Exchange Online Protection, Advanced Threat Protection, SharePoint Online, OneDrive for Business, Project Online, Skype for Business Online, Sway, Office Online, Delve Analytics, Customer Lockbox, and Yammer Enterprise. Technical descriptions of these products and their features are available on Microsoft's website at https://technet.microsoft.com/en-us/library/office-365-service-descriptions.aspx.

The Office 365 services are offered within specific regions, called "Geos." Thus Australia, the European Union, India, Japan, and the United States are each defined as a separate "Geo" for Office 365. As of the date of this paper, Microsoft stores Office 365 customer data at datacenters in the United States and in the following locations: Australia, Austria, Brazil,

Finland, Hong Kong, India, Ireland, Japan, Malaysia, the Netherlands, Singapore, and South Korea. Not all Office 365 customers' data will be stored in all of these locations, however. For example, for customers located and provisioning an Office 365 tenant in North America, their customer data will be stored in Microsoft datacenters in the United States. As another illustrative example, for customers located in Japan, their customer data in Office 365 cloud products will be stored primarily in Japan, but some data (e.g., Active Directory, Sway and Yammer) may also be stored in the United States, Hong Kong, Ireland, the Netherlands, and/or Singapore. Further information about the location of Office 365 cloud datacenters for customers located in other parts of the world is available from Microsoft at http://o365datacentermap.azurewebsites.net/. In addition, for customers who provision their Office 365 tenant in the Geos of Australia, the European Union, India, Japan, or the United States, Microsoft commits to store the following customer data at rest only within that Geo: (1) Exchange Online mailbox content, (2) SharePoint Online site content and the files stored within that site, and (3) files uploaded to OneDrive for Business. *See* Microsoft Volume Licensing Online Services Terms (Worldwide English, November 2016).

The commitments described above relate to storage of data while "at rest." By the nature of cloud computing and the Internet itself, customer data that Microsoft transfers or processes on customers' behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its affiliates or subcontractors maintain facilities. *See* Microsoft Volume Licensing Online Services Terms (Worldwide English, November 2016).

In addition, Microsoft's Office 365 cloud infrastructure is administered, both in the United States and in other locations, by service operations personnel that include nationals of many countries.

Office 365 offers robust encryption options, including "end-to-end" encryption features, to allow customers to protect the security and integrity of their data, prevent unauthorized access, and provide additional options to manage and mitigate potential U.S. export control risks, as described below.

Because Microsoft's cloud infrastructure may be physically located in foreign countries, and may be operated, maintained, and administered by non-U.S. persons, Office 365 customers should be mindful of the U.S. export controls and exceptions outlined above and their potential obligations to comply with those controls.

4. How do U.S. export controls apply to Office 365 customers?

4.1. Potential sources for export control risks

There are two main ways in which customers' use of the Office 365 cloud may implicate U.S. export controls.

First, as discussed above, Microsoft operates datacenters for the Office 365 cloud products in numerous countries around the world, for speed of access, redundancy, and reliability. When

Office 365 customers upload data to the Office 365 cloud, there is at least the potential (mitigated by the Geo framework noted above) that the data may be transferred to a server that is physically located in a country other than the United States. The transfer of customer data to a cloud server may potentially constitute an export or reexport to the country in which the server is located (subject to the carve-out or safe harbor for "end-to-end" encryption). Likewise, the download of or access to customer data stored in a United States server to a user who is physically located outside the United States may also represent an export subject to the EAR. Similarly, a "reexport" subject to U.S. export controls may arise from transfers of U.S.-origin data to or from servers in more than one location.

Second, access by service operations personnel who are foreign nationals to customer data on a cloud server could potentially lead to a "deemed export" or "deemed reexport" subject to U.S. export controls. Microsoft's datacenters and other Office 365 cloud infrastructure are administered by both U.S. and non-U.S. persons. And given the multinational nature of the Office 365 service, the diverse workforce of employees, and the importance of "follow the sun" 24/7 technical support, Office 365 service operations personnel include nationals of many countries.

While these are sources of export compliance risks, Office 365 includes features that can help mitigate and manage these potential risks, as described in the following section.

4.2. Office 365 features to manage potential export control risks

The Office 365 cloud services are structured in ways that help to manage and significantly mitigate—but may not eliminate—the potential risks that customers face under U.S. export controls.

To begin with, most types of customer data are not considered "technology" or "technical data" as defined in the EAR. Most business, financial and personal information stored and processed in the cloud has no relationship to design, development, production, manufacture or use (operation, installation, maintenance, repair, refurbishing, and overhaul) of a controlled product, and is simply not subject to export controls at all. Information that is publicly available is also not generally subject to U.S. export controls. Only specific, proprietary technical information related to an export-controlled product or process is subject to controls.

Next, for customers in North America, the Office 365 Geo framework means that customer data as described above is stored in the United States and minimizes transfer of controlled technology/technical data outside the United States. Similarly, customers in other Geos also have information to know the places their data may be stored. But as noted, given the nature of the Internet, when data is processed or in transit, there is no assurance that customer data will not be transferred to and processed in any location in which Microsoft or its affiliates or subcontractors maintain facilities.

In addition, Office 365 offers end-to-end encryption features that can provide customers with significant technical measures to manage and help protect against U.S. export control risks, as

enabled by the new EAR rules regarding "End-to-End Encryption" discussed in Section 2.5 above. Data integrity between the Office 365 security boundary and a customer's security boundary is assured by encryption, and customers have options in Office 365 to configure forced TLS encryption.[2] All traffic between Office 365 data centers is encrypted.[3] Office 365 deploys BitLocker with AES 256-bit encryption on servers that hold all messaging data, including email and IM conversations, as well as content stored in SharePoint Online and OneDrive for Business.[4] Emails within a single organization deploying Office 365 are encrypted with TLS, and traffic between an Office 365 customer and a third party deploying Office 365 are likewise encrypted.[5] Office 365 enables several customer-managed options for encrypting traffic between an Office 365 user and third parties, including Office 365 Message Encryption (which may be used to encrypt messages to any external recipient's SMTP address), Information Rights Management / Azure RMS (which encrypts content and applies usage restrictions, often within a single organization), and S/MIME (which is peer-to-peer encryption which no one, even an administrator, can view).[6] Microsoft provides detailed information about cipher suites deployed in Office 365 encryption to support a customer's determination as exporter of whether the cryptographic measures are "equally or more effective" than Federal Information Processing Standards Publication 140-2 (FIPS 140-2).[7]

Customer data is not "intentionally stored" in a non-conforming location, consistent with the new EAR rules. Microsoft discloses information about the location of Office 365 cloud datacenters at http://o365datacentermap.azurewebsites.net; none of these datacenters is located in any of the 25 Group D:5 countries or Russia that are listed in footnote 1.

Finally, Office 365 can be configured to meet the requirement that the means of decryption is not provided to any third-party, because the decryption keys or other means of decryption can be limited only to two parties: the customer and Microsoft as Office 365 cloud provider. As explained above, when a customer's encrypted data is uploaded to the cloud, the customer is the "originator" while the cloud provider is the "recipient" for purposes of the EAR rule; when

---

[2] See https://technet.microsoft.com/en-us/library/mt163898.aspx.

[3] See https://www.microsoft.com/en-us/TrustCenter/Security/Encryption and https://technet.microsoft.com/en-us/library/dn569286.aspx.

[4] See https://www.microsoft.com/en-us/TrustCenter/Security/Encryption, https://technet.microsoft.com/en-us/library/dn948533.aspx, and https://technet.microsoft.com/en-us/library/dn905447.aspx.

[5] See https://technet.microsoft.com/en-us/library/mt163898.aspx.

[6] See https://technet.microsoft.com/en-us/library/dn948533.aspx.

[7] See https://technet.microsoft.com/en-us/library/dn569286.aspx. See also https://www.microsoft.com/en-us/TrustCenter/Compliance/FIPS and https://www.microsoft.com/en-us/TrustCenter/Compliance/FedRAMP.

that customer downloads encrypted data from the Office 365 cloud to its local "security boundary," Microsoft is then the originator and the customer is the recipient.

Apart from this "end-to-end encryption" carve out or safe harbor, the use of encryption also helps protect against a potential *deemed* export (or deemed reexport), because even if a non-U.S. person has access to the encrypted data, nothing is actually revealed to non-U.S. person who cannot read or understand the data while it is encrypted and thus there is no "release" of any controlled data. Again, this may not provide complete protection against inadvertent disclosure to the extent that the data does not remain encrypted at all times.

Microsoft also implements a range of policies and security practices that strictly limit access by service operations personnel to customer data and thereby reduce—but not eliminate—Office 365 customers' potential risk under U.S. export controls. No Microsoft personnel have standing access to Customer Data stored in the Office 365 services and all access is governed by strict access control policies. Core tenets of these access control policies are Role Based Access Control (RBAC) and Just-in-time Access Controls that grant system administrator personnel the "least privilege" access to the Office 365 service that is necessary to perform specific operations. Microsoft also implements a Lockbox process under which administrators must request access for elevated privileges; if approved, they are given just-in-time accounts with high entropy passwords, access for a limited amount of time, and access to take specific actions based on a defined role.

Additionally, Microsoft offers a feature called Customer Lockbox, which is included in the Office 365 Enterprise 5 ("E5") plan and can be purchased as a separate subscription with any other Office 365 Enterprise plan. Customer Lockbox gives customers enhanced control over access by Microsoft support engineers during service operations to customer content in Exchange Online mailboxes and SharePoint Online and OneDrive for Business sites and files. In the rare instances where a Microsoft support engineer requires access to such customer content to troubleshoot and fix an issue regarding those services, Customer Lockbox allows the customer to approve or reject the access request. If the customer approves, then the engineer is able to access such customer content. Each request has an expiration time, and once the issue is resolved, the request is closed and access is revoked.

New EAR rules allow service operations employees of cloud service providers to have access (in the rare cases that might be necessary) to data stored in foreign data centers without triggering a "deemed reexport" license requirement, provided that certain screening and other compliance measures are met.

These limitations that Microsoft places on access by service operations personnel to customer data have the practical effect of reducing Office 365 customers' potential risks under U.S. export controls. And importantly, Customer Lockbox gives customers an opportunity to evaluate what data may be exposed before authorizing access by Microsoft service personnel. Customers should take note, however, that these policies are not likely to completely eliminate all the export control risks. Rather, these are tools that customers can use in combination with internal procedures to help ensure full compliance.

In addition, Data Loss Prevention ("DLP") tools included in some Office 365 plans may provide ways for some customers to limit export compliance risk. These DLP tools were developed to support compliance with privacy and other regulations and to help organizations protect sensitive information from inadvertent disclosure. Where available, DLP tools allow customers to conduct searches using key words that may help identify potentially controlled technical information. Other tools allow customers to tag documents or data, as part of the document properties associated with the document in various Office 365 products, when the customer has determined the document or data is subject to export controls. That does require the customer organization to have a process, as discussed in the next section, to identify and classify controlled technical information.

DLP policies, notifications and policy tips can be customized to notify individual users that a document or data set is potentially controlled for export before it is transferred by email, upload or download; or can be set to prevent transfer without specific authorization.

Finally, Microsoft is ready and able to work with customers interested in a customized "hybrid solution" that uses a mix of cloud-based services and resources together with resources that are based on the customers' own premises or on a partner cloud provider's premises. Many customers may find that such hybrid solutions address the export control concerns and potential risks.

5. What should I do to comply with export controls when using Office 365?

Under the EAR, when data is uploaded to a cloud server, such as the Office 365 cloud, the customer who is owner of the data—not the cloud services provider, such as Microsoft—is considered the exporter. For that reason, the owner of the data—*i.e.*, the Office 365 customer—should understand the U.S. export control implications of transferring data to the Office 365 cloud. In particular, Office 365 customers should consider, as discussed below, (1) whether the data is technology or technical data that is subject to the EAR at all, and if so, (2) how the data is classified for U.S. export control purposes, (3) where the data will physically be stored and processed, (4) the nationalities of service operations personnel who may have access to the data, and (5) whether an export license is required.

It is important to note that leveraging cloud technology need not be an all-or-nothing proposition: Many customers may find through their data classification and risk analysis that the lion's share of their data may be processed in the cloud with a small subset retained in a hybrid environment or in a server on premises.

5.1. Determine whether the data is "technical data" controlled by the ITAR

Data controlled under the ITAR or other specialized export regulations are outside the scope of this paper. However, Microsoft offers several Office 365 options for customers to choose depending on their risk assessment and particular needs with ITAR or other specialized export control obligations, including Office 365 solutions and delivery models designed to support ITAR and other controlled data categories. One of those options is the Office 365 Government

Federal offering, which is available to qualified government entities as well as to non-governmental entities who handle data subject to government regulations and requirements, subject to validation of eligibility. Please see https://technet.microsoft.com/en-us/library/office-365-government.aspx for more information about Microsoft's Office 365 Government Federal offering solutions. Another option includes alternative Office 365 delivery models across the Microsoft partner ecosystem, including the hybrid solutions noted above. Please contact your Microsoft representative to discuss available Office 365 solutions and delivery models designed to support ITAR and other controlled data categories.

5.2. Determine whether the data is "technology" or "technical data" under the EAR

As highlighted above, most data stored or shared on Office 365 is not "technology" or "technical data" subject to the EAR at all. Customers who have no "technology" or "technical data," as defined in these export control regulations, to store or use in Office 365 should not need to do anything further for export compliance.

5.3. Classify the data that may be technology/technical data

If it appears that specific proprietary technology or technical data potentially subject to the EAR may be uploaded, stored, processed or used in Office 365, the next step is to determine the appropriate Export Control Classification Number ("ECCN") for that technology or technical data. The ECCN export classification will determine the level of export controls applied to that technology. Data that meets the definition of "technology" under the EAR (specific information for development, production or use) but that is not described or covered by the criteria for any specific ECCN are given the default designation "EAR99." More information concerning the export classification process is provided at the U.S. Commerce Department's website: http://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification

5.4. Take steps to comply with the EAR

For technology subject to the EAR, the relevant ECCN, and the reasons for export control that apply to that ECCN, determine the next steps.

EAR99 or "AT" controlled ECCNs. If the ECCN indicates controls only for anti-terrorism reasons, indicated with the designation "AT," or if the technology is classified in the default EAR99 category, the EAR would not require licensing for export or reexport except to such sanctioned countries as Cuba, Iran, North Korea, Sudan, Syria and the Crimea region now claimed by Russia. Such data may be placed in or used in the Office 365 cloud, as Office 365 does not have infrastructure in these locations.

The great majority of technical data falls within these EAR99 or AT-controlled categories, and many customers may find that they have little or no technical data that is subject to more stringent controls.

Other ECCNs. For the relatively smaller proportion of technology that falls within ECCNs that are controlled for reasons other than "AT," the Office 365 customer can consider whether the relevant ECCN has a licensing requirement for export to one or more of the Office 365 server location(s) for the relevant Office 365 product(s) and Geo being used. As noted above, for example, for customers in North America, the Geo framework means that customer data is stored in the United States; and customers in other Geos also have information to know the places their data may be stored. The EAR also sets forth a number of License Exceptions that permit eligible parties to carry out a defined category or type of export transactions, subject to specified criteria and conditions, without a specific license that would otherwise be required based on the ECCN and reason for control.

1. End-to-end encryption solutions. Customers should evaluate whether the end-to-end encryption features available for Office 365 are the most appropriate tools to manage these export control risks. As discussed above, it should often be possible to develop a plan to deploy end-to-end encryption that conforms to the requirements of the EAR carve-out or safe harbor: (1) Microsoft provides information about Office 365 encryption to enable the customer to confirm it meets the specified NIST/FIPS 140-2 standard, or provides cryptographic measures that are "equally or more effective" than those standards; (2) customer data is not "intentionally" stored in a prohibited location, because Microsoft does not have data centers for permanent storage in any one of the 25 prohibited locations; (3) the customer can structure its Office 365 plans and the way it uses Office 365 to keep data encrypted between the customer's "security boundary" in a given country and the Office 365 data center "security boundary" (or between different Office 365 data centers); and (4) the means of decryption will be limited to two parties -- the customer and Microsoft -- and not available to any third-party.

2. EAR License Exceptions. Alternatively, or in addition, if the relevant ECCN does have a licensing requirement for one or more Office 365 locations designated for the relevant Office 365 product(s) and Geo being used, customers may want to consider whether any License Exception is available to authorize export without a specific license.

3. Office 365 locations in the Geo do not require licensing. If the relevant ECCN does not have any specific licensing requirement for any Office 365 server location designated for the relevant Office 365 product(s) and Geo being used, then U.S. export controls should not prevent a customer from allowing that data to be stored in or downloaded to those Office 365 locations. In light of (1) the Geo framework and Microsoft commitments to store Office 365 in the United States or in particular, known locations, (2) the end-to-end encryption deployed and configurable in Office 365 to help customers limit and control where unencrypted data is "in the clear" between in-country security boundaries; and (3) the features such as Just-in-time Access Controls and Customer Lockbox (an optional feature in some plans) that minimize access to customer data by foreign-national service operations personnel, some customers may conclude that these are reasonable compliance measures and that putting such data in the Office 365 cloud involves a low risk of export control violations, enforcement actions or penalties.

4. Alternative service models. If the customer chooses not to rely on these measures to mitigate export control risk, and the ECCN and reason for control for some technical data indicate that a specific license is required, then it would be prudent not to place or use that data in the Office 365 cloud, and to explore other possible service delivery models. Customers may consider working with Microsoft to develop a customized "hybrid solution," with some resources "on-premises" for export-controlled data, and cloud-based resources and services for other data. Alternatively, some customers may consider whether Microsoft's ITAR-compliant Office 365 Government Federal offering mentioned above may be a good solution for this technology that is subject to a higher level of EAR controls.

6. Conclusion

Not all data is subject to U.S. export controls, and Office 365 offers important features and tools to help customers manage export-control risks. Customers should carefully assess how their use of the Office 365 cloud may implicate U.S. export controls and determine whether any of the data they want to use or store in the Office 365 cloud may be subject to export controls, and if so, what controls apply. Where technical data subject to tighter U.S. export controls may be involved, Office 365 is configured to offer features that help mitigate the potential risk that customers may inadvertently violate U.S. export controls when uploading or downloading controlled technical data in Office 365. With appropriate planning, customers can use Office 365 tools and their own internal procedures to help ensure full compliance with U.S. export controls when using the Office 365 platform.

* * *