

美国商务部发布新的拟议法规：云计算服务供应商“客户识别计划”之规范

作者：袁帅琦 *王晚一对本文亦有贡献。

引言

2024年1月29日，美国商务部发布拟议法规，旨在向美国基础结构即服务（Infrastructure as a Service, IaaS）提供商提出验证其外国客户身份的新要求，即，实施“客户识别计划”。该拟议规则是建立在特朗普时代的行政命令（2021年1月19发布的《采取更多措施应对重大恶意网络活动引发的国家紧急状态》行政命令）与美国现任拜登政府对安全人工智能开发和使用的努力（2023年10月30发布的《安全、可靠和可信的人工智能开发和使用》行政令）基础之上的。拟议法规目前尚处于评论阶段，各方提供评论的截止日期为2024年4月29日。

本文从法规的主要内容、法规的合规要求与执法，以及生效后可能产生的影响为大家作以如下简要的总结与解析。

1. 拟议法规的主要内容——实施“客户识别计划”的规范与要求

本次拟议法规适用的对象为美国IaaS提供商和经销商。法规要求美国IaaS提供商、美国经销商（U.S. Reseller）实施“客户识别计划”（Customer Identification Program, CIP），用于核实外国客户以及“客户获益人”的身份。另外，拟议法规要求美国 IaaS 提供商以及美国经销商只能和实施符合要求的CIP的外国经销商（Foreign Reseller）合作，因此法规的CIP要求延伸至外国经销商。

美国IaaS提供商是指提供IaaS产品和服务的美国公民、美国合法永久居民、根据美国法律或于美国境内任何司法管辖区组建的实体（包括外国分支机构）或位于美国的任何人。美国IaaS提供商不包括美国实体的外国子公司。而经销商是指持有IaaS产品或服务“账户”的，将其获得美国IaaS产品或服务全部或部分提供给第三方的实体或个人。

针对拟议法规所要求实施的CIP，覆盖的对象不仅包括客户，还包括对客户有实质控制的或持有客户25%及以上所有权利益的个人和实体（获益人）。当美国IaaS提供商和美国经销商通过所要求的程序确认客户以及其所有的获益人均均为美国人时，该客户所持有的账户不受本次拟议法规的管辖。

拟议法规要求CIP包括如下主要程序和措施：（1）信息收集的程序。信息包括客户及其受益人的姓名、地址、每个客户账户的支付方式和来源、电子邮件地址和电话号码，以及用于访问或管理账户的IP地址等；（2）确认美国客户；（3）确认与核实外国账户所有者和外国受益人身份的程序，其中还包括了无法核实客户身份时，供应商应采取的步骤、相关的补救措施和问题管理措施；（4）记录保存的程序；（5）要求外国经销商实施CIP，且要求当美国IaaS提供商在收到表明外国经销商未能维护或实施的证据时，须在30日内终止转售关系；（6）对CIP实施更新的程序。目前拟议的法规建议相关方于法规生效后的一年内建立起所要求的CIP。

2. 拟议法规的主要内容——就人工智能训练向美国商务部提交报告的要求

拟议法规要求，美国IaaS提供商与美国经销商对与其交易的外国人进行训练有可能用于恶意网络活动的潜在能力的大型人工智能模型的行为，向商务部部长提交报告。当外国经销商发现该等行为时，需要向美国IaaS提供商提交此类报告，由美国提供商将这些报告提供给美国商务部。报告应至少包括以下内容：外国人的身份信息、确认符合定义的大型人工智能模型训练的存在、商务部要求提交的其他信息。

目前法规拟议就“具有可用于恶意网络活动的潜在能力的大型人工智能模型”的定义为任何具有两用基础模型技术条件的人工智能模型，或具有其他令人担忧的技术参数并且可被用于协助或自动化恶意网络活动的人工智能模型，包括但不限于社会工程学攻击、漏洞发现、拒绝服务攻击、数据中毒、目标选择和优先排序、虚假信息或错误信息的生成和/或传播，以及远程指挥和控制等。

3. 拟议法规的主要内容——授权美国商务部采取“特殊措施”

本次拟议法规还授权美国商务部对“大量外国人员提供美国IaaS产品用于恶意网络活动，或有大量外国人员直接获取美国IaaS产品用于恶意网络活动”的情形可以自行启动调查，评估相关证据，并且决定是否实施特别措施。如果商务部部长确定有证据表明应实施特别措施，将在《联邦纪事》上发布决定。可能采取的特别措施包括：（1）针对某些外国司法管辖区内的客户、潜在客户或账户持有者实施于美国IaaS提供商处开设或维持帐户（包括经销商帐户）的限制或附加条件；（2）针对某些特定的外国人实施在美国IaaS提供商处开设或维持帐户（包括经销商帐户）的限制或附加条件。

4. 拟议法规的合规要求与执法

根据拟议法规，任何违反本建议规则的人都可能根据《国际紧急状态经济权力法案》（International Emergency Economic Powers Act, IEEPA）承担民事或刑事处罚责任。本次拟议法规明确增加了合规要求与执法章节，列出了民事和刑事处罚，以及可能导致处罚的具体行为。违规行为会导致民事或刑事处罚，很大程度上取决于违规行为的性质。例如，故意或蓄意违反这些法规的规定可能会导致刑事处罚，而无意违反则更有可能导致民事处罚。

根据拟议规则，每次违反行为的最高民事处罚金额不超过 250,000 美元（可根据通胀率进行调整），或者是作为违反行为基础的交易金额的两倍，以两者中金额较高者为准。而刑事处罚则包括，应对违法者处以不超过 100 万美元的罚款，如果是自然人，则可处以不超过 20 年的监禁，或两者并罚。

5. 拟议法规的主要内容——实施“客户识别计划”的规范与要求

本次拟议的法规旨在防止“外国恶意网络行为者”利用美国IaaS产品窃取美国知识产权和敏感数据、进行间谍活动、训练对美国关键基础设施进行网络攻击的大型人工智能模型。“今天的规则让外国恶意网络行为者注意到我们正在采取行动阻止他们使用我们自己的云基础设施破坏我们的国家安全利益。”美国商务部工业和安全局副局长艾伦·埃斯特维兹（Alan Estevez）评论道。

而美国商务部部长吉娜·雷蒙多在接受路透社采访时的评论则进一步彰显了美国试图通过该拟议法规限制中国进行人工智能大模型训练。“我们不能让中国或我们不希望的人访问我们的云服务来训练他们的模型。”同时，雷蒙多又暗示该举措对美国目前对中国高科技芯片出口管制措施进行补充的目的：“我们对芯片实行出口管制……美国正在竭尽全力阻止中国获得他们想要的计算能力来训练他们自己的（人工智能）模型，但如果他们绕过这一点使用我们的云服务来训练他们的模型，那又有什么用呢？”

整体而言，目前拟议法规的限制措施与范围较为克制。首先，该拟议法规并不是直接的针对云计算的出口管制措施或是向外国客户提供美国云计算服务的禁止措施。其次，拟议法规限制的主体范围没有扩大至“美国IaaS提供商与经销商”的外国子公司。云服务采购是目前没有足够的资金自建人工智能计算中心的一些中国用户获取云计算资源的重要方式。拟议法规如果生效，所实施的CIP要求以及强制要求美国IaaS提供商报告非美国实体使用其资源训练大型语言模型的情况，可能会阻碍国际合作，进而导致一些中国采购云计算服务与产品的用户被美国切断供给。在美国针对中国高算力GPU严格出口管制的情况下，进一步影响大模型训练进度。本次拟议法规还在评论阶段中，最终生效的法规可能会有内容上的实质性改变，从而产生更进一步的可能不利影响。

2024-01-31

