以“国家安全”之名：美国政府如何限制敏感数据流向中国？

作者：杨建媛 袁帅琦 吴婷 邬丹 魏依文 王晚一 *杨嘉宁对本文的写作亦有贡献

引言

- 2024年2月28日，美国总统发布《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》[1]（Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern，下称“《行政命令》”），同日，司法部下属的国家安全司也发布了一份《拟议规则制定预先通知》[2]（Advance Notice of Proposed Rulemaking，下称“《预通知》”）草案，旨在制定实施该行政令的具体计划，并征求公众意见。**目前，美国尚未对“受关注国家”通过商业交易获取美国人大量敏感个人信息进行规制，被某些美国国内的声音视为威胁美国国家安全的漏洞。**

- **中美在数据出境方面的监管有趋同态势——均立足于国家安全视角，摸索监管介入的程度及方式。**实体方面，《行政命令》立足国家安全视角，并非通常意义下的个人信息保护规范。因大量敏感个人信息、政府相关数据被认为涉及国家安全重大风险，故以数据为落脚点。程序方面，《行政命令》不会设立普遍的个案审查机制，而是制定类型化的规则，要求企业进行前置判断，并配套以合规项目、安全要求、许可等要求，间接实现了针对高风险数据出境的监管干预。

- 美国从国家安全视角限制敏感数据出境的规则早已有之。**不同于之前从“事项”出发，此次系从“数据”出发，无疑极大延展了潜在的规制范围。**但是，囿于《行政命令》上位法的授权范围，规制路径为通过对特定类别的涉数据“交易”制定普适规则，由企业自行判断特定交易是否落入规制范围。**这一规制路径直接关系到中国企业受影响的业务范围、且有别于中国的数据出境监管思路，因此，如何界定受规制的交易是重要课题。**

- 首当其冲受到《行政命令》影响的是具有**中资背景、业务中天然涉及大量敏感个人信息、已经或即将开展海外业务的企业**，直接关系到涉美业务是否还能做、是否可能因交易合作受阻而举步维艰。针对**在华外资企业**而言，反倒可以此为视角理解中国政府目前对数据出境的监管，有助于向境外总部解释建立中国法下数据出境合规机制的必要性、合理性。

章节目录

一、《行政命令》的背景与定位

2024年2月28日，美国总统拜登发布《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》（《行政命令》），限制或禁止涉及某些批量敏感个人数据或美国政府相关数据的交易，从而防止这些数据被大规模转移到"受关注国家"或所涉人员，其中包括中国（包括香港和澳门）、俄罗斯、伊朗、朝鲜、古巴和委内瑞拉。根据《行政命令》的指示，美国司法部也发布了《拟议规则制定预先通知》（《预通知》），正式邀请利益相关方于2024年4月19日前提交意见，以参与制定拟议规则。《预通知》中详细介绍了司法部目前对于拟议规则如何制定的初步想法并结合预想案例进行解释说明，此外还包括司法部希望收到评论的重点议题。

本《行政命令》展示了特朗普政府与拜登政府对相关数据安全的政策的持续关注。近年来，美国政府日益重视美国的数据被获取的问题以及由此产生的对美国国家安全的顾虑，这样的担忧也得到了国会两党的支持。特朗普曾于2019年5月15日签发第13873号行政命令《确保信息通信技术与服务供应链安全》[3]，宣布了国家紧急状态，并限制对美国国家安全构成不当威胁的、美国管辖下任何人士进行的或涉及美国管辖下任何财产的信息和通信技术或服务相关交易。拜登总统于2021年6月9日在第13873号行政命令的基础上进一步发布第14034号行政命令《关于防范外国对立方侵犯美国敏感数据的行政命令》[4]，指示建立外国对立方关联软件应用程序的评估机制，防止其对美国国家安全造成威胁（例如将应用程序用于恶意网络活动或搜集个人敏感数据）。本次《行政命令》扩大了第13873号行政命令国家紧急状态的范围，也是在第14034号行政命令基础上采取的更进一步的措施。

本次《行政命令》将充分利用司法部的职能，以填补数据安全审查方面的空白。首先，虽然《行政命令》以及《预通知》援引了很多美国商务部和财政部所适用的监管概念与机制，（例如，一般许可证和特定许可证、咨询意见、财政部指导的合规程序等）但是该《行政命令》将美国司法部作为领导机构，表明了更多关注执法的潜在意图与可能性。其次，本《行政命令》与美国国外资投资委员会（Committee on Foreign Investment in the United States，即CFIUS）在管辖权上存在一定的重合。CFIUS是美国政府的一个跨部门委员会，美国司法部作为经常审查CFIUS交易的联合牵头机构，具有对涉及敏感个人数据和政府相关数据的交易进行严格审查的经验。根据《行政命令》，司法部预计施加限制的一类交易是"投资协议"，其中涉及相关人员获得美国公司的权益。在某些情况下，受新数据限制约束的"投资协议"也将符合 CFIUS 目的的"受管辖交易"。在《预通知》中，司法部提议存在重叠管辖权时，只有当CFIUS启动正式审查并实施缓解措施时，司法部才会放弃管辖权。另一方面，本次《行政命令》在某些方面比 CFIUS 的管辖权更广泛。例如，司法部在《预通知》中建议为可识别数据量设定阈

值，该阈值低于CFIUS法规中100万个的典型阈值（例如，考虑健康数据的阈值为1,000 到 1,000,000 之间）。其次，《预通知》将扩展到不符合CFIUS目的"受管辖交易"的交易类别，例如批量数据销售、供应商协议和雇佣协议。

最后，该《行政命令》，与美国其他对外管制措施交相呼应，以国家安全的名义和机制为美国的数据安全和管控"添砖加瓦"。例如，《行政命令》对建立相关法规的指示也提到，国防部长、卫生与公共服务部长、退伍军人事务部长和国家科学基金会主任应禁止联邦拨款被用于帮助受关注国家或所涉人员获取敏感个人数据。而美国根据《2024财年国防授权法案》[5]通过被列于1260H清单禁止与美国国防部签订、续签或延长采购合同限制规定，对相关实体获取美国基因数据、其他政府相关数据进行限制。另外，该《行政命令》也反映出美国政府不断加强涉及人工智能、半导体等先进技术的方面出口管制措施的趋势。今年1月29日，商务部发布拟议法规[6]要求美国基础结构即服务（Infrastructure as a Service，IaaS）提供商验证其外国客户身份，并且就人工智能训练行为向美国商务部提交报告（详见*《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》*）。《行政命令》也同样表现出对受关注国家发展人工智能技术的担忧。具体而言，受关注国家可能会"利用批量数据推动人工智能和其他先进技术的创造和完善，从而提高其利用基础数据的能力"。

二、《行政命令》的规制范围：数据、交易、对象

基于对国家安全重大风险的考量，《行政命令》所规制的范围可以概括为：美国主体和"受关注国家"相关的"受覆盖人员"之间特定类型的"交易"，其中涉及获取"美国人的批量敏感个人数据"或"美国政府相关数据"。

为了评估《行政命令》对企业的影响、以及企业的经营活动是否受到规制，首先需要充分理解规制范围的三个维度，即数据、交易、对象。

(一) 数据：哪些数据受规制？

数据是本次规制的落脚点。《行政命令》及《预通知》明确指出了受规制的两大类数据，即"美国人的批量敏感个人信息"和"美国政府相关数据"，并进一步界定了数据类别、数量门槛、可识别性，从而限缩了受规制的数据范围。

1. 美国人的批量敏感个人信息（Americans' Bulk Sensitive Personal Data）

（1）从数据类型的角度，目前主要有如下6类敏感个人信息受到规制：

- 受覆盖的个人识别符：可被用于从数据集中识别出特定个人，或将多个数据集与特定个人关联起来。

《预通知》明确列举了该等识别符的范围，包括：政府身份证件或账户号码（如社会保险号码/SSN、驾照号、护照号），基于设备或硬件的识别符（如IMEI、MAC地址、SIM卡号），人口统计或联系信息（如姓名、出生日期、住址、电话号码、电子邮箱地址），广告识别符（如谷歌广告ID、苹果广告标识符），账户认证数据（如账户名称、密码、安全问题答案），基于网络的识别符（如IP地址、Cookie数据），通话明细数据。

- 地理位置与相关传感器数据：《预通知》目前将该数据限于"精确地理位置数据"，具体精度有待后续制定。

我们理解，地理数据不仅可以反映美国人的行踪轨迹与生活习惯，还可能直接影响物理空间层面的国家安全，因此受到特别关注。这一限制可能对地图导航、自动驾驶/智能汽车等行业产生直接影响，并且对涉及线下经营活动的更多行业产生影响。

- 生物识别标识符：《预通知》将其定义为可用于识别或验证特定个人的可测量的物理特征或行为，如人脸图像、声纹及声音模式、视网膜及红膜扫描、掌纹及指纹、步态、键盘使用模式等。

此处的"生物识别标识符"与中国法下个人生物识别信息概念类似，其通常指对自然人的身体、生理、行为等生物特征进行处理而得出的能够识别自然人独特标识的个人数据。该等信息的使用场景也较为广泛，包括人脸识别系统、语音识别系统的应用等。

- 人类组学数据：《预通知》目前将该数据限于"人类基因组数据"。

《预通知》对"人类基因组数据"的关注，与近期中国科技部对基因数据的重点关注也不谋而合。科技部目前将基因数据作为

中国人类遗传资源信息的监管重点，其包括基因、基因组、转录组、表观组及ctDNA等核酸类生物标志物等数据信息。目前涉及此类数据的中美双向流动均属于敏感领域。

- 个人健康数据：《预通知》将其定义为个人可识别健康信息，主要是指由医疗保健服务提供者等主体创建或接收的、与个人的健康状况或医疗保健服务情况相关的、可用于识别个人的信息。

此处个人健康数据内涵非常宽泛。类似的，根据中国《信息安全技术 健康医疗数据安全指南》，个人健康医疗数据被广泛理解为涉及个人过去、现在或将来的身体或精神健康状况、接受的医疗保健服务和支付的医疗保健服务费用等。

个人健康数据涉及的场景也非常多。对于医药企业而言，其不仅涉及产品开发和注册阶段可能接触和处理的受试者医疗健康信息（含去标识化的编码信息），也可能涉及产品商业化阶段，因药物警戒、不良事件、质量投诉、产品召回等事由而接触和处理的产品患者的医疗健康信息。

- 个人财务数据：《预通知》将其定义为与个人的信用卡、借记卡、银行账户等相关的数据，包括购买和支付记录；银行、信用或其他财务报告中的数据，包括资产、负债、借款和交易；信用报告或消费者报告中的数据；医保账户信息，包括接受的医疗保健服务和支付的医疗保健服务费用信息。

下列数据类型则被明确排除在规制范围之外：公开记录；个人通信；具有表达性和言论保护目的的信息或信息材料。

（2）从数量门槛的角度，"批量"敏感个人信息应在特定时间内达到特定的数量门槛（指人数或设备数）。

《预通知》基于风险路径，为各类敏感个人数据分别设置了不同的数量门槛，即：在受覆盖的数据交易发生前的12个月内的任何时间点，同一受覆盖人员在所有交易中所涉数据累计达到下列数据量（单位为美国人或美国设备）：

	人类基因组数据	生物识别标识符	精确地理位置数据	个人健康信息	个人财务数据	受覆盖的个人识别符
低	100	100	100	1,000	1,000	10,000
高	1,000	10,000	10,000	1,000,000	1,000,000	1,000,000

（3）从可识别性的角度，受规制的数据系与"可识别的"美国个人或群体相关联。是否可以通过匿名化、去标识化、假名化处理降低甚至去除可识别性，从而避免落入受规制数据？随着人工智能、大数据分析等技术的不断发展，处理后的数据变得更容易被重识别，导致受限制的数据范围可能有所扩张。《预通知》对此问题亦表达谨慎态度。

2. 美国政府相关数据（United States Government-Related Data）

（1）从数据类型的角度，目前主要有如下2类数据受到规制：

- 美国政府人员相关数据。该等人员包括美国联邦政府（包括军方）的现任或近期前任雇员、承包商、前任高级官员等类别。

- 美国政府位置相关数据。该等位置为美国联邦政府（包括军方）所控制的敏感位置。《预通知》目前将该数据限于司法部拟出台清单上的特定敏感区域的精确地理位置数据。

（2）从数量门槛的角度，美国政府相关数据没有数量门槛，即，因其敏感性质而直接落入规制范围。此类似中国法下重要数据的监管思路。

（3）从可识别性的角度，受规制的人员数据系与已识别的美国政府人员相关联或可关联，或与可用于识别美国政府人员的

数据相关联；受规制的位置数据系与美国政府位置相关联或可关联。

(二) 交易：哪些交易类型受规制？

交易是本次规制的切入点，有别于数据保护领域的监管路径。对于上述受规制的数据，《行政命令》并不要求该等数据本地化存储在美国，也不直接对数据跨境传输本身进行前置审查。受限于上位法的授权范围，《行政命令》的切入点是涉及受规制数据的“交易”。

“交易（transaction）”一词具有丰富的内涵和实践形式，是指美国主体所从事的、而外国国家及其国民享有利益的任何获取、持有、使用、传输、运输、出口或交易，统称为交易。一方面，不能排除存在“交易”被扩大解读的可能；另一方面，仍需存在特定类型“交易”这个载体才会受到规制。一个典型的问题是：直接从美国个人用户处收集个人信息的APP是否会被规制呢？

从规制的角度，交易被划分为被禁止的交易、受限制的交易、可豁免的交易。此外，本文也将探讨哪些业务活动可能不落入《行政命令》的规制范围。

1. 被禁止的交易（Prohibited Transaction）

《行政命令》及《预通知》列举了2类被禁止的交易类型：

（1）数据经纪交易：《预通知》将数据经纪定义为数据接收方不直接从个人处收集数据，而是从数据提供方（即数据经纪人）处购买、被许可访问数据。

数据经纪在美国属于合法行为，且已成为实践中盛行的产业。数据经纪人可以合法地购买、销售大量的个人数据，这种交易形态本身蕴含高风险。特别是，人工智能技术的不断进步令“大力出奇迹”成为现实，批量敏感个人数据不仅更容易被识别、被关联，其使用的目的和方式更将不断突破人类的想象空间。

（2）基因组数据交易：该等交易涉及批量人类基因组数据或可推导出该等数据的生物样本的传输。

值得一提的是，2024年1月美国国会提出了BIOSECURE法案，该法案禁止政府机构购买或使用所谓“关注生物技术公司”的生物技术设备或服务，禁止政府机构与使用这些公司产品的实体签订、续签或扩展合同，其中主要是中国的生物技术公司。被列入“关注生物技术公司”的主要原因包括，在全球范围内开展收集基因数据的活动，在多国运营基因采集点或实验室，收集了大量孕妇的基因数据等，且可接触美国市场和人群。

2. 受限制的交易（Restricted Transaction）

《行政命令》及《预通知》列举了3类受限制的交易类型，我们理解，其核心逻辑是受覆盖人员（比如中国企业）能否通过该等交易而接触、获取美国敏感数据。

（1）供应商协议：该类协议涉及产品和服务的提供，《预通知》中重点列举了云计算服务（包括IaaS、PaaS、SaaS）。典型示例是外国公司在为美国公司提供技术服务过程中可能接触受规制的数据，如软件开发、技术服务、数据存储及处理服务。次典型示例是外国公司与美国公司开展内涵更多元的业务合作过程中可能接触受规制的数据，例如：旅游产品预订平台吸纳美国酒店入驻，从而获取美国人敏感信息，该平台可能被认为系SaaS服务提供者。

（2）雇佣协议：《预通知》指出该类协议包括董事、执行、运营等多个层面的雇员，并强调外国人员入职美国公司后因工作性质而有权限访问受规制的数据。以人员入手进行规制，可视为监管精细化的体现，也在一定程度上体现了涉国家安全数据领域的监管趋势。

（3）投资协议：《预通知》指出该类协议系就美国的不动产或法律实体取得直接或间接的所有权利益或相关权利，并强调被投资对象应掌握或可接触受规制的数据。同时，《预通知》排除了公开交易证券、微量股权等投资类型。

3. 可豁免的交易（Exempt Transaction）

对于被禁止或受限制的交易，《行政命令》及《预通知》还列举了可被豁免的类型，包括：

（1）金融服务、支付处理、监管合规所附带的数据交易：例如，银行业、资本市场或金融保险服务，在电商平台购买商品或服务产生的支付数据等。

（2）美国跨国公司内部业务运营所附带的数据交易：例如，用于人力资源管理、工资支付、税费支付、外部审计、风险管理等目的。

（3）美国政府及其承包商、雇员和受赠者的公务：例如，联邦政府资助的健康和研究活动。

（4）美国联邦法律或国际协议所要求或授权的交易：例如，旅客名单信息、国际刑警组织请求、公共卫生监测。

4. 可能不落入规制范围的业务活动

《行政命令》的规制逻辑是指定特定类型的交易，而非对数据相关的所有交易或活动进行普遍限制。因此，中国企业需要评估自己的涉美业务活动是否落入《行政命令》的规制范围。

实践中一种常见的业务模式是，中国企业面向美国市场推出产品，以to C类APP出海为例，并在APP运营过程中直接收集并处理美国用户的个人数据。我们理解，直接从个人用户处收集数据的行为似乎不会直接落入上述受规制的交易类型，且《情况说明》也明确表示不会直接禁止任何特定的APP。但需要注意的是，APP出海运营不仅包括与个人用户的交互，还涉及与诸多供应商、合作方（包括美国实体）的合作，而该等合作则有可能落入受规制的交易类型，从而影响APP在美国市场的运营。

我们理解，判断中美企业之间的合作是否受规制的一个核心标准是，该等合作是否会导致中国企业获得受规制的数据。例如，向中国企业销售数据集，或使用中国企业的云服务，会大概率导致中国企业获得数据。相反地，美国应用商店上架中国APP，则只是为中国企业从美国用户处获取数据提供了前提与可能性，但上架本身并不会直接导致中国企业获得数据。

又比如，对于医药行业而言，在跨境产品引进、全球合作开发，以及国际多中心临床试验等背景下，中国医药企业可能需要获取受规制数据，如在中国药品开发和上市申报需要依赖于美国的临床试验数据，或者在临床试验中需要纳入美国人作为受试者，该等临床数据可能涉及受规制的数据类型（如个人健康数据、人类组学数据、生物识别标识符等）。如本文所述，涉及该等跨境项目或业务的企业亦需要监测和评估相关数据流动是否可能受到规制。

(三) 对象：哪些国家、实体、人员受规制？

对于上述受规制的数据及交易，《行政命令》并未施加普遍性的限制，而是有差别地挑选出存在所谓引发国家安全重大风险的特定国家及相关人员。《行政命令》及《预通知》所辐射的对象，可从受关注国家、受覆盖人员、经由第三国再出口这三个角度予以理解。

1. 受关注国家（Countries of Concern）

《行政命令》所规制的对象是可能引发美国国家安全重大风险的外国政府，并将由司法部决定该等国家名单。目前，司法部在《预通知》中指明了6个“受关注国家”，即：中国（包括香港和澳门）、俄罗斯、伊朗、朝鲜、古巴、委内瑞拉。

2. 受覆盖人员（Covered Persons）

《行政命令》及《预定通知》指定了禁止或限制美国主体与之交易的“受覆盖人员”的范围，分为如下5类。其核心逻辑是，如果该等人员获取数据，出于法律或实践原因，则数据将处于受关注国家（政府）可获取的境地。

（1）受关注国家所拥有、控制、受其管辖或指示的实体；

《预通知》进一步解释了该类实体的范围，包括：1由受关注国家直接或间接掌握50%或以上所有权的实体；2根据受关注国家的法律注册成立的实体；3主要营业地位于受关注国家的实体；4由各类受覆盖人员直接或间接掌握50%或以上所有权的实体。

由是观之，不仅是中国国资控股企业、以及更广泛意义上的中国企业会受到规制，而由中国企业控股的外国公司也会受到规制，且可能对外国公司的股东进行穿透。

（2）作为（1）类实体的雇员或承包商的外国主体/非美国主体（包括个人或实体）；

（3）作为受关注国家的雇员或承包商的外国主体/非美国主体（包括个人或实体）；

（4）主要居住在受关注国家所辖领土内的外国主体/非美国主体（包括个人或实体）；

（5）被司法部长认定具有下述情形的任何主体（包括个人或实体）：“受关注国家所拥有、控制、受其管辖或指示”、“代表或声称代表受关注国家或其他受覆盖人员行事”、或“故意造成或指示（直接或间接地）违反《行政命令》或其相关法规”。这一额外授权有可能进一步扩大受覆盖人员的潜在范围。

3. 经由第三国再出口（Re-Export）

除了直接将受关注国家、受覆盖人员作为规制对象，《行政命令》及《预通知》还关注到了实践中可能发生的规避情形，并将规制范围进一步延伸至经由第三国再出口的情形。

例如，如果美国主体与规制对象之外的第三国人员进行数据经纪交易，则要求美国主体通过协议约束第三国人员，限制其将获取的数据转售或提供给受关注国家及受覆盖人员。

三、《行政命令》的规制手段与合规路径

《行政命令》及《预通知》并未提出普遍性的、前置性的个案审查要求，而是设定类型化的规制范围，并在相当程度上交由美国主体自行识别受规制的风险、自行采取措施以符合安全要求。此外，司法部一方面通过许可方式放行风险可控的受规制交易，减小经济影响；另一方面，在有风险的特定情形下，辅以尽职调查、记录保存、报告、审计等进一步合规措施。

(一) 在内部执行“合规项目（Compliance Program）”

《行政命令》及《预通知》并未对数据跨境流动本身、或受规制的交易本身提出普遍性的、前置性的个案审查要求，而是通过“类型化”的立法方式，圈定了受到规制的数据、交易、对象的类型，并交由企业进行自我评估。

参照OFAC实施IEEPA经济制裁项目的方式，《行政命令》及《预通知》要求美国主体（包括企业及个人）在内部自行建立并执行“合规项目”。合规项目系根据美国主体的自身特点与风险进行设计，综合考虑其规模、复杂程度、产品和服务、客户及相对方、地理位置等因素。

美国主体在业务运营过程中，如果通过合规项目自行识别出受规制的交易，则依法停止交易、或采取安全措施、或申请许可（详见下文）。对于不确定的情形，美国主体还可以向监管机构征求其咨询意见（advisory opinions），即主动询问拟开展的特定交易是否落入规制范围。

不同于事前审查，《行政命令》及《预通知》通过合规项目为企业提供了一定程度的交易自主性。如果发生违法行为，司法部会开展执法行动，并考虑合规项目的充分性。

合规项目的义务承担方为美国主体，而中国企业作为交易相对方，可能在与美国主体的交易过程中遭遇美国主体的内部评估，并被要求提供相关的信息和配合。

(二) 满足“安全要求（Security Requirement）”

《行政命令》及《预通知》规定了被禁止、受限制的交易类型，以及对应的后果：

1. 被禁止的交易：该类交易直接被禁止，除非经监管机构许可；

2. 受限制的交易：如果满足“安全要求”，则被允许交易；如果不满足“安全要求”，则被禁止交易，除非经监管机构许可。

安全要求本质上是为了降低受关注国家、受覆盖人员通过交易获取受规制数据的风险。国土安全部等监管机构将首先设定安全要求，然后由交易主体采取相应措施以符合安全要求。

《预通知》目前列举的安全要求主要包括组织措施、数据屏蔽与最小化、隐私保护技术、逻辑和物理访问控制、阻止未经授权的访问、设置独立审计员等方面。我们理解，上述措施与美国现有的网络安全与隐私保护框架、乃至世界范围内典型的数据合规措施有较多共通之处。对企业而言，搭建、执行一套完善的网络安全与数据合规体系，正日渐成为多个法域、多个监管领域的共同要求。

(三) 获得“许可（License）”

对于被禁止的交易、受限制的交易（且未满足安全措施），司法部等监管机构有权签发许可，例外地放行该等交易。许可分为两种类型：

（1）一般许可：司法部可以主动为受规制的交易提供类型化的许可、并公开发布，从而允许美国主体开展该等交易。司法部可能在一般许可中向适用主体设定额外的要求，例如，向监管机构提交报告和声明。

（2）特定许可：美国主体可以主动为特定交易申请特定许可，司法部将在个案审查后作出决定，并可能为特定许可设置额外的要求，例如，持续提交报告、确保交易所涉数据被删除等。

(四) 采取其他合规措施

《行政命令》和《预通知》表示不会为美国主体的交易创设普遍性的尽职调查、记录保存、报告、审计等合规义务，但司法部可能考虑建立一套基于风险的合规方案，在特定情形下施加合规义务。

1 . 尽职调查及记录保存：司法部考虑将主动的尽职调查及记录保存要求作为开展受限制的交易、取得一般许可或特定许可的一项条件，具体包括“了解你的供应商”、“了解你的客户”等内容。

2 . 报告：司法部考虑将主动的报告要求作为特定美国主体开展受限制的交易、取得一般许可或特定许可、识别被禁止交易的一项条件。举例说明目前受到特殊关注的情形：一个美国主体从事受限制的云计算服务、或根据许可开展数据经纪交易，且受关注国家或受覆盖人员直接或间接拥有其25%以上的股权。

3. 审计：司法部考虑设立审计要求，作为受限制的交易符合安全要求、或受规制的交易符合许可条件的举措。

4 . 调查与执法配合：司法部考虑要求美国主体在调查与执法中提供配合，可能包括就受规制交易保存完整记录、并提供完整信息。

2024-03-08