# 美國商務部新訂雲端基礎架構式服務業者建立外國客戶身份識別程序規則草案

曾泓霖 編譯

**摘要**

今（2024）年 1 月 29 日，美國商務部所屬工業暨安全局提出一項規則草案，加強對美國雲端服務供應商；特別是針對基礎架構式服務供應商的監管，該規則草案旨在保護美國國家安全，針對外國客戶可能利用該服務進行網路惡意活動的行為進行規範。此舉亦可認為係美國擔憂中國可能利用基礎架構式服務來規避美國新半導體出口管制措施所採取之應對手段。該規則草案要求美國基礎架構式服務供應商建立客戶身份識別程序——即「認識客戶」要求，以識別、評估與追蹤使用該服務的外國客戶。規則草案並要求，美國基礎架構式服務供應商於其外國客戶利用美國雲端計算服務以訓練進行網路惡意活動之人工智能模型時，須向美國工業暨安全局報告該情事。然美國工業暨安全局此舉亦招致利害關係人對於規則草案可能侵害隱私權或效益不彰等擔憂，故該規則草案之後續發展，仍待持續關注。

（取材資料：Brian J. Egan et al., *Know Your Cloud Customer: Commerce Department Proposes to Regulate Foreign Access to US IaaS Products,* SKADDEN (Feb. 13, 2024), https://www.skadden.com/insights/publications/2024/02/know-your-iaas-customer.）

美國商務部工業暨安全局（Bureau of Industry and Security, BIS）於今（2024）年 1 月 29 日提出一項規則草案[1]，要求基礎架構式服務（Infrastructure as a Service, IaaS）供應商應對外國客戶之身分進行驗證[2]。此舉將為雲端計算技術之出口管制措施奠定基礎，其旨在嚇阻中國違反先進半導體技術管制之行為[3]。

以下先簡介規則草案之提案背景及內容，並講述規則草案之涵蓋範圍及具

[1] Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities, 89 Fed. Reg. 5698 (Jan. 29, 2024) (to be codified at 15 C.F.R. pt. 7).
[2] *Id.* at 5698.
[3] Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections, Bureau of Industry and Security, 88 Fed. Reg. 73458 (Oct. 25, 2023) (to be codified at 15 C.F.R. pt. 732, 734, 736, 740, 742, 744, 746, 748, 758, 770, 772, and 774) at 73458.

體要求，接著說明目前專家及產業界對此提案之評論，最後做一結論。

## 壹、提案背景

2021 年 9 月 24 日，美國商務部依據「針對重大惡意的網路活動採取進一步行動」之第 13984 號行政命令，發布制定法規之預先通知（Advance Notice of Proposed Rulemaking, ANPRM），以徵求公眾對於履行該行政命令所制定之相關規則的意見[4]。

緊接著，美國總統以「人工智慧的安全、發展與應用」之第 14110 號行政命令，下令商務部應要求美國的 IaaS 供應商需確保外國經銷商主動驗證外國用戶之身份[5]。第 14110 號行政命令亦賦予商務部權限，使其得要求美國的 IaaS 供應商，於外國人以訓練可能用於網路惡意活動之大型人工智慧模型為目的而購買、使用其服務時，須通報美國商務部[6]。

參考公眾意見後，BIS 於今年 1 月 29 日提出履行第 13984 號行政命令第 1、2、5 條及第 14110 號行政命令的規則草案[7]。該規則草案為針對雲端服務實施出口管制以防止中國遠端取用先進技術晶片之作法，奠定基礎。此舉主要回應美國產業界之擔憂，即中國或可透過 IaaS，遠端取用原先受到出口管制的先進技術晶片，令其即便未實際持有該等晶片，亦得將之用於訓練供軍事用途之大型人工智慧模型[8]。

## 貳、提案內容

### 一、IaaS 之定義與範圍

規則草案之適用對象為「美國 IaaS 供應商」，其將 IaaS 定義為「提供消費者處理、儲存、網路或其他基礎運算資源之免費或付費服務或產品，使消費者能夠安裝與運行非預先定義（predefined）之軟體，包括操作系統與應用程式[9]。」

其中，「美國 IaaS 供應商」涵蓋任何美國人（U.S. Person），包括銷售 IaaS 服務之外國實體的美國子公司，以及銷售這些服務的美國經銷商[10]。雖然美國 IaaS

[4] Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities, 89 Fed. Reg. at 5698.
[5] *Id*.
[6] *Id*.
[7] *Id*.
[8] Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections, Bureau of Industry and Security, 88 Fed. Reg. at 73462.
[9] Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities, 89 Fed. Reg. at 5701.
[10] *Id*. at 5700.

業者的外國子公司不在此定義範圍之內[11]，美國 IaaS 供應商仍需要確保其外國經銷商實施「客戶身份識別計劃（Customer Identification Program, CIP）」[12]。

## 二、客戶識別程序

規則草案之第二部份要求美國 IaaS 供應商制定並保有書面的 CIP，以建立外國用戶之個人帳戶的識別與驗證程序[13]，即「認識客戶（Know-Your-Customer, KYC）」要求[14]。在實施 KYC 要求時，美國 IaaS 供應商至少需要蒐集並更新其外國帳戶持有人之姓名、地址、付款方式、款項來源、電子郵件地址、電話聯絡方式以及 IP 位址等資訊[15]。在草案規則下，美國 IaaS 供應商得將公司規模、提供的服務類型及相關風險納入考慮，建立具彈性且對商業營運負擔最小的 KYC 程序[16]。

然而，根據規則草案，BIS 可能在美國 IaaS 供應商及其外國經銷商遵循特定條件時，豁免其 KYC 要求：

第一種豁免管道為，實施經 BIS 批准之「防止 IaaS 服務濫用計劃」（Abuse of IaaS Products Deterrence Program, ADP）[17]。該計劃要求美國 IaaS 供應商採取類似 KYC 的機制來對客戶進行驗證、監控 IaaS 服務的使用情況，並識別、解決與報告潛在之網路惡意活動[18]。

其中，公私部門合作係另一項 BIS 用於評估是否得以豁免的條件。若美國 IaaS 供應商或美國 IaaS 產品的外國經銷商透過參與業界團體，一同開發與維護隱私保護相關的數據共享與分析，以便更好地偵測網路惡意活動，則可能豁免於 KYC 要求[19]。

同時，若美國 IaaS 供應商或美國 IaaS 產品的外國經銷商自願與執法部門合作，提供有關網路惡意活動之資訊及證據，亦可能藉此取得 BIS 豁免[20]。

根據以上豁免條件，KYC 之豁免程序為： BIS 與國防部長、司法部長、國土安全部長及國家情報局局長或其認為適當之行政部會首長協商後，將做出裁定以決定是否免除美國 IaaS 供應商與其外國經銷商之 CIP 要求[21]。然，為持續得到

[11] *Id*. at 5703.
[12] *Id*.
[13] *Id*.
[14] *Id*. at 5698.
[15] *Id*. at 5703.
[16] *Id*.
[17] *Id*. at 5704.
[18] *Id*. at 5730.
[19] *Id*. at 5731.
[20] *Id*.
[21] *Id*. at 5732.

豁免，美國 IaaS 供應商或美國 IaaS 產品的外國經銷商有義務持續更新資訊，以應對不斷變化的威脅形勢，並且必須在其 ADP 出現重大偏誤或變化時通知 BIS[22]。同時，BIS 有權隨時撤銷 CIP 要求的豁免，包括在實施特別措施的情況下[23]。

此外，根據規則草案，美國 IaaS 供應商需將可能被用於訓練網路惡意活動的大型人工智能模型或改變現有 IaaS 用途之外國交易回報給 BIS[24]。

## 三、特別措施

根據規則草案，BIS 可以採取兩項特別措施以防止 IaaS 服務遭到濫用：其中一項為，對於位在擁有大量美國提供之 IaaS 服務的外國地區，並將該服務用於網路惡意活動之外國人或其代理人，禁止於 IaaS 服務提供者處開設帳號或對帳號之開設施加限制[25]；第二項特別措施為，若 IaaS 供應商代理或為外國人開設或維持帳戶，而此外國人被發現提供用於網路惡意活動的美國 Iaas 產品，或由已知之使用美國 IaaS 服務於網路惡意活動之外國人，建立或持有 IaaS 帳戶之行為，BIS 可予以禁止或施加限制[26]。

# 參、產業界與相關專家對規則草案之質疑

## 一、管制措施之必要性

對於中國遠端取用先進技術晶片之能力所帶來之威脅，是否如 BIS 所認定，已達到需要控管之程度，數個業界團體對此提出質疑。美國資訊技術產業協會（Information Technology Industry Council, ITI）認為，遠端取用 IaaS 所獲取之計算能力，並不能與直接使用實體晶片相比[27]。此外，目前訓練大型軍民用途之人工智能基礎模型，需要成千上萬與高效能網路連接的晶片，以及其他專業基礎設施如冷卻設備才能達成[28]。若個人實際持有受管制的晶片，則確實得透過將該晶片與其他晶片物理上串聯並建立一個叢集，以用於訓練雙重用途的人工智能基礎模型[29]。然而，IaaS 客戶沒有這種能力，因為他們只能取用晶片之計算能力，而

---

[22] *Id*.
[23] *Id*. at 5732.
[24] *Id*. at 5725.
[25] *Id*. at 5732.
[26] *Id*.
[27] *ITI Comments on Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use*, INFO. TECH. INDUS. COUNCIL (Jan. 17, 2024), https://downloads.regulations.gov/BIS-2022-0025-0077/attachment_1.pdf.
[28] *Id*.
[29] *Id*. 叢集是指使用多部小型電腦，透過區域網路或廣域網路「合體」成為較大型的分散式運算架構電腦。部署叢集指在提高單台電腦效能及可用性。*Cluster Computing: An Advanced Form of Distributed Computing*, GIGABYTE (Jan. 11, 2022), https://www.gigabyte.com/Article/cluster-computing-an-advanced-form-of-distributed-computing-a-tech-guide-by-gigabyte.

不是獲取晶片本身[30]。

## 二、管制措施之有效性

美國喬治城大學研究機構（Center for Security and Emerging Technology）之研究員指出，如果 BIS 意圖通過 IaaS 供應商，控制國內用戶或終端用戶透過 IaaS 取用晶片，則 KYC 規則將有效加強對 IaaS 供應商的出口管制[31]。然而，中國客戶可能會試圖掩蓋其位置或身份，因此規則草案的有效性，將取決於 IaaS 供應商是否投入 KYC 規則的實踐，對此，標準化或改進 IaaS 供應商的 KYC 實踐情形，或將提升管制的有效性[32]。

## 三、管制措施在隱私權保護上的疑慮

提案規則之措施引發了許多隱私上的疑慮，包括 IaaS 供應商是否能在不違反其他國家隱私法規的情況下，向美國政府提供客戶之詳細資訊[33]。美國科技貿易管制聯盟（Technology Trade Regulation Alliance）指出，IaaS 用戶通常會認為其使用於 AI 訓練的數據數量或類型、參數數量以及訓練 AI 模型的方法為敏感且受專利權保護的資訊，因此 IaaS 用戶可能不願意提供此類資訊[34]。再者，IaaS 用戶對於限制 IaaS 供應商存取其客戶資料有著強烈的商業利益。此係基於 IaaS 用戶在保護具敏感性之企業資料上普遍具有共識，且可能需遵循其他隱私法規[35]。

## 肆、結語

美國 BIS 此次提出規則草案的目標，在於強化美國在雲端計算服務之防線，以防止美國企業直接或間接幫助海外之網路惡意活動。該規則草案下，針對 IaaS 服務供應商之 KYC 要求，雖對於維護美國國家安全以及達成管制目的上有其政策重要性，但其於實施上將面臨許多困難。同時，IaaS 服務供應商亦需承擔龐大的法遵成本以及面臨技術上之挑戰，對於 IaaS 服務供應商來說，潛在的解決方案或為向 BIS 尋求實施 KYC 之豁免。由於該規則仍在徵求公眾意見之階段，各界之評論與質疑是否將影響規則草案之發展方向，有待後續觀察。

---

30 *Id*.
31 Jacob Feldgoise & Hanna Dohmen, *CSET Response to October 17, 2023 AC/S IFR_Request for Public Comment*, THE CTR. FOR SEC. AND EMERGING TECH. (Jan. 17, 2024), https://cset.georgetown.edu/wp-content/uploads/CSET-Response-to-October-17-2023-AC_S-IFR_Request-for-Public-Comment.pdf.
32 *Id*.
33 Brett Fortnam, *BIS 'Know-Your-Customer' Rule Seen as Precursor to Cloud Controls*, INSIDE U.S. TRADE, Vol. 42, No. 7, Feb. 16, 2024.
34 *Id*.
35 *Id*.