Office of Financial
Sanctions Implementation
HM Treasury

Financial Sanctions Notice

09/12/2025

Cyber

Introduction

1. The Cyber (Sanctions) (EU Exit) Regulations 2020 (S.I. 2020/597) ("the Regulations") were made under the Sanctions and Anti-Money Laundering Act 2018 ("the Sanctions Act") and provide for the imposition of financial sanctions, namely the freezing of funds and economic resources of persons who are have been involved in cyber activity which undermines, or is intended to undermine, the integrity, prosperity or security of the United Kingdom or a country other than the United Kingdom; directly or indirectly causes, or is intended to cause, economic loss to, or prejudice to the commercial interests of, those affected by the activity; undermines, or is intended to undermine, the independence or effective functioning of an international organisations or a non-government organisation or forum whose mandate or purposes related to the governance of international sport or the Internet; or otherwise affects a significant number of persons in an indiscriminate manner.

2. On 09 December 2025 the Foreign, Commonwealth and Development Office updated the UK Sanctions List on GOV.UK. This list provides details of those designated under regulations made under the Sanctions Act. A link to the UK Sanctions List can be found below.

3. Following the publication of the UK Sanctions List, information on the Consolidated List has been updated.

Notice summary

4. The following entries have been added to the Consolidated List and are now subject to an asset freeze:

- INTEGRITY TECHNOLOGY GROUP INCORPORATED (Group ID: 17246)
- SICHUAN ANXUN INFORMATION TECHNOLOGY CO., LTD. (Group ID: 17247)

What <u>you</u> must do

You must:

i. check whether you maintain any accounts or hold any funds or economic resources for the persons set out in the Annex to this Notice and any entities owned or controlled by them;

ii. freeze such accounts, and other funds or economic resources;

iii. refrain from dealing with the funds or economic resources or making them available directly or indirectly to or for the benefit of designated persons unless licensed by the Office of Financial Sanctions Implementation (OFSI) or if an exception applies;

iv. report any findings to OFSI, together with the information or other matter on which the knowledge or suspicion is based. Where the information relates to funds or economic resources, the nature and quantity should also be reported.

5. Information received by OFSI may be disclosed to third parties in accordance with provisions set out in the Information and Records part of the regulations and in compliance with applicable data protection laws.

6. Failure to comply with UK financial sanctions legislation or to seek to circumvent its provisions may be a criminal offence.

Ransomware and Sanctions

Making or facilitating a ransomware payment risks exposing those involved to civil or criminal penalties where such payments are made to designated persons.

7. OFSI, in partnership with other HM Government organisations has published guidance on sanctions and ransomware, which includes information on the impact of ransomware payments, cyber resilience and HM Government's approach to enforcement.

8. Guidance on ransomware and sanctions can be found here: https://www.gov.uk/government/publications/financial-sanctions-faqs.

Further Information

9. Copies of recent notices, UK legislation and relevant guidance can be obtained from the Cyber financial sanctions page on the GOV.UK website: https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases.

10. The Consolidated List can be found here: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets.

11. The UK Sanctions List can be found here: https://www.gov.uk/government/publications/the-uk-sanctions-list.

12. The Compliance Reporting Form can be found here: https://www.gov.uk/guidance/suspected-breach-of-financial-sanctions-what-to-do.

13. For more information please see our financial sanctions guidance: https://www.gov.uk/government/publications/financial-sanctions-faqs.

Enquiries

14. Non-media enquiries about the implementation of financial sanctions in the UK should be addressed to:

    Office of Financial Sanctions Implementation
    HM Treasury
    1 Horse Guards Road
    London
    SW1A 2HQ
    ofsi@hmtreasury.gov.uk.

15. Non-media enquiries about the sanctions measures themselves should be addressed to: fcdo.correspondence@fcdo.gov.uk.

16. Media enquiries about how financial sanctions are implemented in the UK should be addressed to the Treasury Press Office on 020 7270 5238.

17. Media enquiries about the sanctions measures themselves should be addressed to the Foreign, Commonwealth & Development Office Press Office on 020 7008 3100.

ANNEX TO NOTICE

FINANCIAL SANCTIONS: CYBER

THE CYBER (SANCTIONS) (EU EXIT) REGULATIONS 2020 (S.I. 2020/597)

ADDITIONS

Entities

1. **INTEGRITY TECHNOLOGY GROUP INCORPORATED**
   Name (non-Latin script): 永信至成科技集团股份有限公司
   a.k.a: Integrity Tech **Address:** Room 103, Block 6, No. 9, Fenghao East Road, Haidian District, Beijing, China. **Other Information:** (UK Sanctions List Ref): CYB0113. (UK Statement of Reasons):The Secretary of State considers that there are reasonable grounds to suspect that Integrity Technology Group Incorporated (Integrity Tech), formerly Beijing Integrity Technology Group (BITG), has been involved in relevant cyber activity, in that it provided support for and engaged in the commission, planning or preparation of such activity, and supplied technology that could contribute to the commission of relevant cyber activity. Integrity Tech controlled and managed a botnet covert network consisting of over 260,000 compromised devices worldwide and supplied access to this network enabling unauthorised access to and interference with information systems and data which targeted UK public sector IT systems. Such activity that Integrity Tech was involved in, undermined, or was intended to undermine, the integrity, prosperity or security of the United Kingdom or a country other than the United Kingdom. (Website): https://www.integritytech.com.cn **Listed on**: 09/12/2025 **UK Sanctions List Date Designated:** 09/12/2025 **Last Updated:** 09/12/2025 **Group ID:** 17246.

2. **SICHUAN ANXUN INFORMATION TECHNOLOGY CO., LTD**.
   Name (non-Latin script): 四川安洵信息技术有限公司
   a.k.a: (1) Anxun Information Technology Co., Ltd. (non-Latin script: 安洵信息技术有限公司) (2) i-Soon **Other Information:** (UK Sanctions List Ref): CYB0114. (UK Statement of Reasons):The Secretary of State considers that there are reasonable grounds to suspect that Sichuan Anxun Information Technology Co., Ltd. (i-Soon) has been involved in relevant cyber activity, including being responsible for, engaging in and providing support for malicious cyber activity that resulted in the exploitation of previously unknown vulnerabilities and gaining unauthorised access to over 80 foreign government and private business networks. In addition, i-Soon facilitated and supported a wider ecosystem of China-based information security companies, enabling actual or attempted unauthorised access to and interference with information systems and data, which targeted UK public sector and private industry IT systems through, namely, researching, exploiting and sharing of vulnerabilities. This malicious activity undermined or was intended to undermine the integrity, prosperity or security of the United Kingdom or a country other than the United Kingdom. **Listed on:** 09/12/2025 **UK Sanctions List Date Designated**: 09/12/2025 **Last Updated**: 09/12/2025 **Group ID:** 17247.

Office of Financial Sanctions Implementation

HM Treasury

09/12/2025