



Updated Hong Kong Business Advisory

Issued: September 6, 2024

Title: Amendment to the July 2021 Business Advisory on Risks and Considerations for Businesses Operating in Hong Kong

Introduction

The U.S. Department of State, the U.S. Department of the Treasury, the U.S. Department of Commerce, the U.S. Department of Agriculture, and the U.S. Department of Homeland Security are issuing this amendment to the [July 2021 Hong Kong Business Advisory](#) to highlight new and heightened risks associated with actions undertaken by People’s Republic of China (PRC) and Hong Kong Special Administrative Region (SAR) authorities. These risks could adversely affect U.S. companies that operate in the Hong Kong SAR of the PRC (Hong Kong). This amended advisory highlights the potential reputational, regulatory, financial, and, in certain instances, legal risks to U.S. companies operating in Hong Kong.

Businesses, individuals, and other persons, including academic institutions, media organizations, research service providers, and investors (hereafter “businesses and individuals”) that operate in Hong Kong, or have exposure to U.S.-sanctioned individuals or entities, should be aware of changes to Hong Kong’s laws and regulations that have been issued since the previous advisory in 2021 and could adversely affect businesses and individuals operating in Hong Kong.

In particular, similarities between Hong Kong's and the PRC's national security laws, combined with Hong Kong's diminishing autonomy from the central government of the PRC, create new risks for businesses and individuals in Hong Kong that were previously limited to mainland China (see the 2023 [Investment Climate Statement](#) for China and [Hong Kong](#) for further details).

This evolving legal landscape includes the enactment of the 2020 Law of the People's Republic of China on Safeguarding National Security in the Hong Kong SAR (National Security Law, or NSL), as well as the Safeguarding National Security Ordinance (SNS Ordinance), which was enacted in March 2024 under Article 23 of Hong Kong's Basic Law.

The SNS Ordinance contains broad and vague provisions regarding the criminalization of "colluding with external forces," activities involving "state secrets," and "espionage," among other acts, that could affect or impair routine business activities in, or travel to, Hong Kong. Further, Hong Kong officials have stated that provisions in the SNS Ordinance apply extraterritorially. These statements followed the August 2023 and December 2023 issuance of "bounties" and arrest warrants by Hong Kong police for 13 pro-democracy advocates living outside Hong Kong, including a U.S. citizen and others residing in the United States. The vaguely-defined nature of the law and previous government statements and actions raise questions about risks associated with routine activities that may violate the NSL and/or the SNS Ordinance, such as: due diligence research on government policy or local clients; analysis of local or mainland economic conditions or firms; maintaining connections with local and international government officials, journalists, or non-governmental organizations; and data management, protection, and transmission to and within Hong Kong.

The Department of State encourages U.S. citizens traveling to or residing in the Hong Kong SAR to consult the [Travel Advisory](#).

Background on Hong Kong's Economic Status

Hong Kong's economic system retains many distinctions from that of mainland China, such as free and open trade, a higher degree of internet freedom, negligible tariff and non-tariff barriers, and well-protected property ownership and intellectual property rights. Although Hong Kong is part of the PRC, Hong Kong maintains a separate common law legal system for commercial and civil litigation. Hong Kong maintains the Hong Kong International Arbitration Centre (HKIAC), which offers alternative dispute resolution services for commercial disputes. It also maintains a separate currency and separate regulatory structures to supervise companies operating in the territory. Hong Kong continues to exercise independent authority in the implementation of commercial agreements, administers a separate customs territory, sets a monetary policy autonomously from the PRC, and has maintained its own representation in many international organizations and multilateral entities, including the Asia-Pacific Economic Cooperation, the Financial Action Task Force, and the World Trade Organization.

However, as noted in the [Business Advisory issued in July 2021](#) and the Department of State's [Hong Kong Policy Act Report in 2024](#), the PRC's imposition of the NSL in Hong Kong in June 2020 led to major structural changes that significantly reduced Hong Kong's autonomy and undermined human rights and fundamental freedoms.

The SNS Ordinance poses additional risks for businesses and individuals, and it should be considered in the broader context of actions undertaken by PRC and Hong Kong authorities in attempts to apply Hong Kong's national security laws extraterritorially to suppress civil society and free expression and peaceful assembly. As a result, risk factors that were formerly limited to mainland China are now also a concern in Hong Kong and could affect commerce, trade, and seemingly routine individual commercial activities in Hong Kong.

Background on the SNS Ordinance

Following a limited public comment period, Hong Kong's Legislative Council fast-tracked enactment of the [SNS Ordinance](#) in March 2024, introducing several vaguely defined criminal offenses, including: (1) offenses in connection with state secrets and espionage; (2) external interference endangering national security; and (3) acts with seditious intention. The SNS Ordinance adopts a definition for "state secrets" and sets forth elements of "espionage" that are similar to updated PRC national security and counter-espionage laws enacted in mainland China in 2023 and 2024.

The SNS Ordinance broadly defines "national security" to include threats not only to Hong Kong's sovereignty and territorial integrity, but also to its political regime, "the welfare of the people, sustainable economic and social development, and other interests of the state."

Further, many provisions of the SNS Ordinance purport to apply extraterritorially to: any Hong Kong resident who is a PRC citizen for their activities outside of Hong Kong; any firm registered in Hong Kong; and any company outside of Hong Kong that has a place of business in Hong Kong. Additionally, some offenses, such as the unlawful disclosure of state secrets, purport to apply to anyone outside of Hong Kong, regardless of nationality.

Under similar laws to those recently enacted in Hong Kong, PRC authorities in mainland China appear to have broad discretion to deem a wide range of documents, data, statistics, or materials to be state secrets and to detain and prosecute foreign nationals for alleged espionage. Following the enactment of these similar laws in the PRC, there has been increased PRC scrutiny of foreign firms, such as professional service and due diligence companies, operating in mainland China. PRC security personnel could detain U.S. citizens while inside mainland China or subject them to prosecution for conducting research or accessing publicly available material.

Hong Kong authorities have already [charged six people](#) under the SNS Ordinance for "seditious" posts to a Facebook group, with police alleging that the posts were intended to provoke hatred against the government. Since the NSL's enactment in 2020, Hong Kong authorities have used existing

national security laws to arrest over 200 people suspected of violating national security provisions, and formally charged more than 100 of them.

SNS Ordinance Provisions Relevant to Business Interests

While the SNS Ordinance has not been used to prosecute any businesses in Hong Kong as of the date of this publication, national security police raids of newspaper *Apple Daily* and parent company *Next Digital* in 2020 and 2021 ultimately forced the company's closure and liquidation after the arrest of company founder Jimmy Lai and several Next Digital executives for allegedly violating the NSL. PRC and Hong Kong authorities may attempt to use broadly defined offenses in the SNS Ordinance to prosecute individuals or businesses for engaging in routine business activities, including: lobbying to influence government decision-making; conducting market analysis or research that relies on Hong Kong government data; engaging in due diligence or accountancy operations; or publishing analysis or commentary through the media, NGOs, or think tanks, so long as Hong Kong authorities determine that these activities threaten national security.

Several specific provisions of the SNS Ordinance set forth broadly defined offenses, listed below, that are particularly relevant to business operations because they may implicate certain routine business activities.

1. **Theft of State Secrets and Espionage**: The SNS Ordinance provisions regarding "state secrets" and "espionage" are modeled on the PRC's Safeguarding State Secrets Law and the Counter-Espionage Law. Clauses 32, 33, and 35 of the SNS Ordinance codify offenses for unlawfully acquiring, possessing, and disclosing "state secrets," the last of which is punishable by up to 10 years in prison. Clause 34 makes it an offense to unlawfully possess state secrets when leaving Hong Kong, which is punishable by up to seven years in prison. Clause 29 vaguely defines "state secrets" to include information concerning, among other things:
 - the economic or social development of China or the Hong Kong SAR;

- the technological development or scientific technology of China or the Hong Kong SAR; and
 - the relationship between PRC Central Authorities and the Hong Kong SAR.
2. **External Interference Endangering National Security**: Clause 52 of the SNS Ordinance provides that “collaborat[ing] with an external force to do an act” with “intent to bring about an interference effect” and using “improper means when doing the act” is an offense. Under Clause 53, an “interference effect” appears to broadly encompass influencing the Central People’s Government, executive authorities of the Hong Kong SAR, legislative councilors, election outcomes (specifically the casting of votes), and judicial procedures, as well as prejudicing the Hong Kong SAR’s relationship with the PRC or the relationship between the Hong Kong SAR/PRC and any foreign country.
 3. **Acts with Seditious Intention**: Clause 24 makes it an offense to: perform an act or utter a word that has a seditious intention; with knowledge that a publication has a seditious intention, print, publish, sell, offer to sell, distribute, display, or reproduce the publication; or import a publication that has a seditious intention. Under Clause 23 of the SNS Ordinance, “seditious intention” includes “an intention to bring a Chinese citizen, Hong Kong permanent resident or a person in the HKSAR into hatred, contempt or disaffection” against the PRC’s “fundamental system of state” or state institutions, or against various offices of the Central Authorities in Hong Kong.
 4. **Sabotage Endangering National Security**: Clause 49 of the SNS Ordinance makes it an offense to damage or weaken a “public infrastructure” with the intent to endanger national security or with recklessness as to whether national security would be endangered. Such offenses are punishable by up to 20 years imprisonment; punishment may be increased to life imprisonment if a person commits the same act but “colludes with an external force” to do so. The SNS Ordinance defines “external force” to include companies that

have directors who are “under an obligation” to act “in accordance with the directions, instructions or wishes” of the government of a foreign country.”

In light of examples of the extra-territorial assertion of the existing NSL and some SNS Ordinance provisions, Hong Kong authorities may also seek to apply SNS Ordinance provisions extraterritorially to prosecute activities that take place outside of Hong Kong.

Continued Risks for Businesses and Individuals Operating in Hong Kong under the NSL, SNS Ordinance, and Other Laws:

Individuals have been arrested under the NSL in Hong Kong for various reasons, including: publishing newspaper articles; participating in democratic processes; expressing an opinion regarding the government or the Chinese Communist Party; and attending public gatherings. Penalties for offenses under the NSL, which applies to any individual in Hong Kong, can include criminal fines and imprisonment, including life imprisonment in certain circumstances. In addition, the NSL states, among other things, that “an incorporated or unincorporated body, such as a company or organization which commits an offense” under the NSL, may be subject to a criminal fine and to having its operations suspended or its license or business application revoked “if the body has been punished for committing an offense” under the NSL.

Only judges specially appointed by the chief executive may oversee NSL cases. The NSL established an Office for Safeguarding National Security (OSNS) in Hong Kong. It is staffed by PRC security services and not subject to the jurisdiction of the Hong Kong authorities, including its judiciary. Rather than Hong Kong courts, the OSNS is empowered to exercise jurisdiction over certain cases brought under the NSL. The NSL also established a new Committee for Safeguarding National Security, led by the chief executive and accountable to the PRC. As of May 2024, at least 100 people have been found guilty in cases designated as involving national security, and only two have been acquitted. The NSL authorizes the mainland PRC judicial system

to take over any national security-related case at the request of the Hong Kong government or the OSNS. To date, this provision has not been used, though Hong Kong authorities have threatened to invoke it.

The Hong Kong authorities have arrested individuals under a colonial era sedition law for publishing books, articles, and posting material on social media it deems seditious. In September 2023, police invoked a colonial era law prohibiting the “import[ation of] seditious publications” for the first time to charge a man who received 18 copies of “Sheep Village,” a children’s picture book a Hong Kong court previously ruled was seditious. Hong Kong authorities also arrested individuals for social media activity that took place outside of Hong Kong. The SNS Ordinance updated the colonial era sedition law and increased the penalty from two to seven years, or ten years if the alleged offense involves an “external force.”

Hong Kong authorities have arrested foreign nationals under the NSL, including one U.S. citizen. Those arrested may have travel documents confiscated and may be prevented from departing Hong Kong. Additionally, the Hong Kong Legislative Council amended Hong Kong immigration law in 2021, and the amendment could potentially allow Hong Kong authorities to place exit bans on individuals seeking to depart the country, including non-residents. As of May 2024, police have carried out at least 237 arrests for alleged “national security offenses.” Police have used the NSL extraterritorially to issue arrest warrants for individuals residing abroad, and in 2023, the Hong Kong government offered cash rewards of over \$128,000 per person for information leading to the arrest of 13 democracy advocates living in the United States, the UK, and Australia, including a U.S. citizen.

Heightened Risks Regarding Surveillance and Data Privacy

Businesses operating in Hong Kong face privacy-related risks, including electronic surveillance without warrants and the surrender of data to authorities. The NSL introduced, and the SNS Ordinance compounded, the risk that PRC and Hong Kong authorities may use expanded legal authorities to collect data from businesses and individuals in Hong Kong for actions that

may violate “national security” or constitute “theft” of a “state secret.” Hong Kong authorities have, to date, interpreted “national security” to include: participating in primary elections; other political activity specifically protected by the Basic Law; posting opinions on social media; and meeting with members of the diplomatic community. While Hong Kong maintains a separate regulatory framework from mainland China for how businesses, individuals, and government authorities collect, handle, and use data in Hong Kong, the NSL and the SNS Ordinance appear to grant Hong Kong law enforcement broad authorities to conduct wiretaps or electronic surveillance with the approval of the chief executive, rather than the courts, in national security-related cases.

In light of these risks, some foreign businesses with operations in Hong Kong have reportedly requested their non-Hong Kong staff to leave their laptop computers and mobile phones in their home offices prior to traveling to Hong Kong due to security concerns. Other foreign firms have removed automatic access to internal global databases for Hong Kong-based staff without prior corporate approval due to similar data security concerns, or have separated their Hong Kong-based operations from their existing corporate structure altogether.

Heightened Risk Regarding Free Expression and Access to Information

Businesses that rely on free and open press may face restricted access to information. Imposition of the NSL and enactment of the SNS Ordinance have further limited the exercise of free expression, notably by members of the press, especially for expression which may be viewed as critical of the Hong Kong or mainland government. For example, Hong Kong authorities forced the closure of several media outlets, including *Apple Daily* and *Stand News*, and seized property from both privately held entities. Authorities continue to prosecute staff of these media outlets under the NSL and on sedition charges. In response to increased risks posed by the NSL and the SNS Ordinance, some international news outlets have reduced Hong Kong-based staff. Radio Free Asia decided to close its Hong Kong bureau completely. Additionally, in May 2024, a Hong Kong court issued an

injunction relating to the song “Glory to Hong Kong,” which banned people from “broadcasting, performing, printing, publishing, selling, offering for sale, distributing, disseminating, displaying or reproducing” the song with “seditious intent.”

The NSL and its implementing regulations granted extensive powers to police to order the blocking and removal of content by message publishers, platform service providers, hosting service providers, and network service providers. While Hong Kong authorities do not generally disrupt access to the open internet, there have been several reports by international media outlets that the Hong Kong police, exercising powers granted by the NSL, have required internet providers to block access to certain websites or to block certain accounts.

The SNS Ordinance also adds new risks for businesses and individuals that engage in certain forms of economic and market research and could potentially limit access to important economic data. This may include economic and business analysts, market researchers, and credit rating analysts, as well as the firms that employ them, particularly firms that conduct due diligence research on Hong Kong or PRC authorities, as well as those who consult with foreign government officials, departments, and agencies as part of their routine operations. Likewise, the SNS Ordinance's provisions related to the publication of "false or misleading" statements could present potential risks for the routine work of foreign press, research and academic institutions and think tanks, foreign banks and financial institutions, and other foreign businesses. For example, the SNS Ordinance added a new “espionage” offense, which says “if a person colludes with an external force to publish to the public a statement of fact that is false or misleading” it could be punishable by up to 10 years in prison.

Other Heightened Risks

Under laws related to anti-doxing, Hong Kong authorities could fine or arrest locally based staff of online platforms that do not comply with user information or content takedown orders. The law allows the Office of the

Privacy Commissioner for Personal Data to seize and access any electronic devices in premises being searched without a warrant if authorities suspect a doxing-related offense was or could have been committed.

Hong Kong authorities froze bank accounts of former lawmakers, civil society groups, and other political targets. The government froze assets belonging to several suspects in NSL- and sedition-related trials. In December 2023, according to the South China Morning Post's online news site myNEWS, the Hong Kong government amended Article 43 of the NSL to allow the government to freeze assets of suspects involved in national security cases until legal proceedings conclude, removing an earlier limit that capped the period at two years unless the High Court authorized an extension.

Key U.S. Authorities for the Imposition of Sanctions and Other Financial Risks

Individuals and entities should also be aware of potential consequences under U.S. law of certain types of engagement with sanctioned persons.

The United States government has imposed sanctions measures and visa restrictions that target persons involved in certain conduct related to Hong Kong; the legal authorities for such measures remain unchanged from the [Hong Kong Business Advisory published in July 2021](#).

In addition to accounting for these sanctions measures and visa restrictions, U.S. persons and others subject to U.S. jurisdiction operating in [or with a connection to] Hong Kong should be aware of sanctions risks related to other malign behavior involving Hong Kong-based individuals and entities including activities related to supporting Russia's defense industrial base, manufacturing and distribution of fentanyl and other illicit drugs and their precursor chemicals, procurement facilitation for Iran's ballistic missile and unmanned aerial vehicle program, and the shipment of Iranian liquefied petroleum gas to U.S.-designated terrorist group Hizballah.

The PRC and Hong Kong have become significant transshipment points for dual-use goods re-exported to Russia to support Russia's military-industrial base and its continued aggression against Ukraine. The United States and international partners have imposed sanctions and export controls that have severely restricted Russia's ability to import many of the items that directly support its war against Ukraine. As a result, Russia is increasingly using third countries and jurisdictions such as Hong Kong to evade sanctions and continue its procurement of certain critical items. U.S. persons and others subject to U.S. jurisdiction should ensure that their Hong Kong related business does not violate the sanctions and export control prohibitions designed to frustrate Russia's continued aggression against Ukraine. U.S. export controls extend to foreign persons engaging in transactions involving items subject to U.S. controls, including items produced outside the United States destined to Russia or restricted parties in Hong Kong or elsewhere.

The United States and international partners have published multiple advisories, including detailed lists of red flags, to notify the public about Russian sanctions evasion and to support sanctions and export control compliance efforts. In addition, on June 12, 2024, the U.S. Department of the [Treasury updated the definition](#) of Russia's defense industrial base under [Executive Order 14024, as amended](#), to include all persons blocked pursuant to that order, among others. The United States may impose sanctions on any foreign financial institution conducting or facilitating significant transactions or providing any service involving persons blocked under this authority. As of August 30, 2024, the U.S. Department of Commerce has imposed restrictions on exports, reexports, in-country transfers, and foreign-produced items to 174 unique parties in Hong Kong as well as 11 addresses identified through their inclusion on Commerce's Entity List.

Hong Kong may become a financial hub for persons supporting PRC-based chemical and pharmaceutical companies that are complicit in the proliferation of illicit drugs, including fentanyl precursor chemicals and associated manufacturing equipment. On June 20, 2024, the U.S. Department of the Treasury's Financial Crimes Enforcement Network ([FinCEN](#)) [issued a supplemental advisory](#) urging U.S. financial institutions to

increase vigilance in identifying and reporting suspicious activity associated with Mexico-based transnational criminal organizations and their illicit procurement of fentanyl precursor chemicals and manufacturing equipment from PRC-based suppliers and their chemical brokers. This supplemental advisory builds off of the related 2019 FinCEN advisory and alerts U.S. financial institutions of the risks of transactions related to the sale or purchase of fentanyl precursor chemicals and manufacturing equipment, including: the use of shell and front companies; money transfers through banks, money services businesses, and online payment processors; and payments in virtual currency.

Hong Kong is one of the pathways often used to circumvent U.S. export controls related to PRC semiconductor manufacturing equipment. Since October 2022, the U.S. Department of Commerce published a series of interim final rules imposing controls on advanced computing and supercomputing items and semiconductor manufacturing equipment to limit the PRC's ability to engage in activities that would pose significant threats to U.S. national security and foreign policy.

Furthermore, U.S. and non-U.S. persons alike should be aware of the applicability of U.S. sanctions and export control laws to individuals and entities located in Hong Kong, as set out in more detail, for example, in the Department of Commerce, Department of the Treasury, and Department of Justice [Tri-Seal Compliance Note: Obligations of foreign-based persons to comply with U.S. sanctions and export control laws.](#)

As noted in the July 2021 advisory, U.S. persons should continue to be aware of the prohibitions under U.S. sanctions authorities and the civil and criminal penalties that may result in a failure to comply. OFAC continues to encourage U.S. persons and [to the extent their activities implicate U.S. sanctions authorities] foreign entities, including foreign financial institutions, to employ a risk-based approach to sanctions compliance.

In addition, on December 23, 2020, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) removed Hong Kong as a separate

destination under the Department's Export Administration Regulations (EAR) pursuant to [Executive Order 13936](#). Accordingly, all items subject to the EAR that are destined for export, reexport, or transfer (in country) to or from Hong Kong are treated as exports, reexports, or transfers (in country) to or from the PRC.

Risks for Businesses with Exposure to Sanctioned Hong Kong or PRC Entities or Individuals, and for Businesses that Adhere to U.S. Sanctions

Businesses operating in Hong Kong may face retaliation and countermeasures in the PRC for adhering to sanctions imposed by the United States and other countries. Hong Kong authorities officially recognize UN sanctions, but not U.S. sanctions, and Hong Kong's financial sanctions regime is governed by its two ordinances on UN sanctions and UN anti-terrorism measures. Rules issued by the PRC's Ministry of Commerce (MOFCOM), including rules issued under the Law of the People's Republic of China on Countering Foreign Sanctions and the PRC's 2015 National Security Law, do not apply in Hong Kong. To date, the PRC Countering Foreign Sanctions Law has not been adopted or implemented under Hong Kong's separate legal system.

Although no individuals or companies appear to have been subject to retaliatory measures or civil liability in Hong Kong for adhering to U.S. sanctions to date, there is some risk that the SNS Ordinance may be used to target businesses or individuals involved in facilitating or advocating for sanctions that target Hong Kong officials. The SNS Ordinance codified a new offense with a maximum penalty of 10 years in prison for "unlawful harassment of persons handling cases or work concerning national security," including judges and prosecutors. An individual commits this offense if that individual uses words, makes communications, or does an act that is "intimidating, abusive, or offensive" with the intent to cause alarm, distress, psychological harm, or harm that causes the other person to be concerned for that person's safety, well-being, or damage to that person's property.

Accordingly, businesses operating in Hong Kong may face conflicting jurisdictional requirements and liability in connection with sanctions compliance efforts. Failure to adhere to U.S. sanctions can result in civil and criminal penalties under U.S. law. Companies with questions about sanctions compliance obligations may contact OFAC at the link [here](#).

Due Diligence

Human Rights Due Diligence

The United States encourages U.S. companies that operate in Hong Kong to undertake heightened human rights due diligence. Resources include: the [UN Guiding Principles on Business and Human Rights](#); the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct; the International Labor Organization publication “[Combating Forced Labor: A Handbook for Employers and Business](#)”; and the Office of the High Commissioner for Human Rights guide on [The Corporate Responsibility to Respect Human Rights](#). Additional resources are available from multi-stakeholder efforts such as the [Global Network Initiative](#).

Compliance Due Diligence for Sanctions and Export Controls

Persons engaging in activities subject to OFAC regulations should consult OFAC’s website, which contains detailed information on sanctions programs, including key elements of any sanctions compliance program, see “[A Framework for OFAC Compliance Commitments](#).” Businesses and individuals engaging in export transactions involving items subject to the EAR should consult BIS’s website, which contains detailed guidelines on export controls, including key elements of any export controls compliance program, see “[Export Compliance Guidelines: The Elements of an Effective Export Compliance Program](#).”

In addition to sanctions and export controls compliance, U.S. financial institutions are required to comply with the Bank Secrecy Act (BSA) and its implementing regulations administered by FinCEN. BSA requirements

generally include establishing anti-money laundering programs and complying with certain recordkeeping and reporting requirements, including the obligation to file currency transaction reports and report suspicious activity. The reporting generated by these obligations is essential to detecting, investigating, and deterring criminal activity. U.S. financial institutions are expected to take a risk-based approach to identify, assess, and mitigate their money laundering and terrorist financing risks, including a consideration of the risks that arise from the geographic focus of the U.S. financial institution or of its customers. For further information, financial institutions should refer to FinCEN-issued press releases, regulations, advisories, and guidance as to their obligations under the BSA. Financial institutions may face civil enforcement as well as potential criminal penalties if they fail to comply with their BSA obligations.

Disclaimer: We will provide an updated, accessible version of this document soon. You may write to eap-press@state.gov to request an accessible alternative version of this information.