China has acquired proprietary technology and early-stage ideas through legal transfers and industry relationships to gain access to research fields, experts, and key enabling industrial processes that, over time, erode the U.S. Air Force's long-term competitive advantages. China requires foreign entities, including U.S. companies conducting business within China, to incorporate as a Wholly Foreign Enterprise (WFOE) or enter into a joint venture with a local Chinese partner. These entities are subject to China's laws governing personal information, company data, and intellectual property. U.S. companies conducting business in China, or that have shared information with a Chinese company, may be unwittingly providing non-publicly available, proprietary, or personal information to the Chinese government.

2021 Counterespionage Law
Mandates that Chinese nationals cooperate with national security agencies. Article 9 requires Chinese organizations to collaborate with the Chinese Communist Party (CCP) national security agencies to monitor staff and students with access to sensitive information when they work or travel overseas, to protect Chinese interests. Businesses are compelled to work with national security agencies to train staff and students on counterespionage techniques and to provide them with counterespionage equipment and facilities.

2021 Anti-Foreign Sanctions Law
 Allows Beijing to take retaliatory measures against persons or entities instigating or implementing sanctions against China. For global companies, complying with Western sanctions would mean violating Chinese law and facing counter-sanctions and liabilities. Retaliatory targets include spouses, relatives, and coworkers of those deemed responsible for sanctions.

2021 Personal Information Protection Law
Mandates U.S. companies operating in China to locally store all personal information that is collected and produced. Non-Chinese companies must agree to a Chinese government-formulated data handling contract. Personal information is broadly defined to include video, voice, or image data.

2017 Cybersecurity Law
Requires that data is stored in China and that Chinese public security and intelligence services are given access to investigate incidents through on-site inspections, including spot-testing critical information infrastructure.

2015 National Security Law
China's comprehensive national security legislation. Provides the enabling legal infrastructure broadly covering China’s security apparatus. The law contains 84 articles and 7 chapters. Chapter 6 defines obligations of citizens and corporations and broadly defines national security as the relative absence of international or domestic threats to the state's power to govern and the capacity to protect security in a sustainable manner.

1993 Company Law
Requires all Chinese companies to establish and maintain an active organization of the CCP to carry out Party activities. This ensures CCP knowledge and direction regardless of whether a company is a state-owned enterprise.

2021 Special Administrative Measures for Foreign Investment
Chinese businesses in certain sectors must receive government clearance before they can list their shares in overseas markets. Foreign investors must not participate in the operation and management of the companies, and their holdings are capped at 30%. The sectors include compulsory education, news organizations, and rare-earth minerals.

2021 Data Security Law
Companies processing "important data" are subject to periodic security reviews. This law reinforces compliance with Chinese officials, who are authorized to obtain data. Companies must obtain Chinese government approval to release any data stored in China to any foreign judicial or law enforcement agencies, regardless of where the data originated from.

2021 Network Product Security Vulnerability Reporting Law
Jointly published with the Ministry of Public Security (MPS). Mandates vulnerability reporting to the Chinese Ministry of Information and Technology within 48 hours. The law covers network product suppliers, operators (broadly defined), and cybersecurity platforms.

2020 Hong Kong National Security Law
U.S. citizens and companies are exposed to penalties and criminal fines for violations deemed a threat to Chinese national security. Includes activity that "inches authoring anti-PRC, Government opinion articles or calling for sanctions."

2017 National Intelligence Law
Article 7 obligates Chinese individuals, organizations, and institutions to support national intelligence work. Article 14 gives the Chinese intelligence agencies the authority to demand such cooperation.

Author: OS Center Technology Protection
Product ID: 04057
Serial: TP-0134-22
Feedback: afosicon-productionmanagement@ua.mil/subject= 40507

UNCLASSIFIED
<table>
<thead>
<tr>
<th>Chinese Law</th>
<th>Implications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2021 Personal Information Protection Law</strong></td>
<td>U.S. companies operating in China must locally store all personal information that is collected and produced. Non-Chinese companies must report to a Chinese government-formulated data handling contract. A security review by state authorities is required for cross-border transfers of personal information. Personal information is broadly defined to include video, or images depicting a person. It also includes fines up to 50 million RMB (~7.2 million USD) or 5% of an organization's annual revenue for the previous year, revocation of operating permits, or negative Chinese national credit score systems.</td>
</tr>
<tr>
<td><strong>2021 Data Security Law</strong></td>
<td>Companies processing “important data” are subject to periodic security reviews. This law reinforces compliance with Chinese authorities, who are authorized to obtain data. Companies must obtain PRC’s approval to release any data stored in China to any foreign judicial or law enforcement agencies, regardless of where the data originated from. Companies found in violation of regulations concerning “core data” face penalties of up to 10 million RMB (~1.56 million USD), the forced shutdown of their businesses, and potential criminal liabilities. Companies found in violation of regulations concerning “important data” face penalties of up to 5 million RMB (~780,000 USD).</td>
</tr>
<tr>
<td><strong>2021 Counterespionage Law</strong></td>
<td>Strengthens existing national security laws. Mandates that Chinese nationals cooperate with the PRC national security agencies to monitor staff and students who may engage in activities that harm national security interests. Requires sensitive information when they work or travel overseas, to protect Chinese interests. Businesses are compelled to work with national security agencies to train staff and students on counterespionage techniques and to provide them with counterespionage equipment and facilities.</td>
</tr>
<tr>
<td><strong>2021 Network Product Security Vulnerability Reporting Law</strong></td>
<td>Jointly published with the MPS. Mandates vulnerability reporting to the China Ministry of Information and Technology within 48 hours. The law covers network product suppliers, operators (broadly defined), and cybersecurity platforms. See Chinese Malicious Cyber Activity: <a href="https://www.cisa.gov/uscit">https://www.cisa.gov/uscit</a> China.</td>
</tr>
<tr>
<td><strong>2021 Anti-Sanctions Law</strong></td>
<td>Allows Beijing to take retaliatory measures against persons or entities instigating or implementing sanctions against China. Forbids defining malicious actors as “those that interfere with Chinese interests. Businesses are compelled to work with national security agencies to train staff and students on counterespionage techniques and to provide them with counterespionage equipment and facilities.</td>
</tr>
<tr>
<td><strong>2021 Special Administrative Measures for Foreign Investment Access</strong></td>
<td>Chinese businesses in certain sectors must receive government clearance before they can list their shares in overseas markets. Foreign investors must not participate in the operation and management of the companies, and their holdings are capped at 30%. The sectors include compulsory education, news organizations, and rare-earth minerals.</td>
</tr>
<tr>
<td><strong>2020 Biosecurity Law</strong></td>
<td>Treats biosecurity as an element of national security, putting all related work under the National Security Commission of the Communist Party. The law covers enhanced penalties for violations and gives the Chinese state sovereignty over all human genetic resources.</td>
</tr>
<tr>
<td><strong>2020 Hong Kong National Security Law</strong></td>
<td>U.S. citizens and companies are exposed to penalties and criminal fines for violations deemed a threat to national security. Includes activity that “inches authoring anti-PRC Government opinion articles or calling for sanctions”</td>
</tr>
<tr>
<td><strong>2017 Cryptocurrency Law</strong></td>
<td>Requires that data is stored in China that is related to Chinese national security and information services are given access to investigate incidents through on-site inspections, including spotting critical information infrastructure.</td>
</tr>
<tr>
<td><strong>2017 National Intelligence Law</strong></td>
<td>Article 7 obligates Chinese individuals, organizations, and institutions to support national intelligence work. Article 14 gives the Chinese intelligence agencies the authority to demand such cooperation.</td>
</tr>
<tr>
<td><strong>2016 National Defense Transportation Law</strong></td>
<td>Article 40 stipulates that the People’s Liberation Army (PLA) may station military representatives in areas where relevant transportation enterprises are located. Transportation enterprises are mandated to provide convenience for the military representatives to carry out their work. China. Companies participating in overseas projects are obligated to host and collaborate with PLA units at the request of the Chinese government.</td>
</tr>
<tr>
<td><strong>2015 National Security Law</strong></td>
<td>China’s comprehensive national security legislation. Provides the enabling legal infrastructure broadly covering China’s security apparatus. The law contains 84 articles and 7 chapters. Chapter 6 defines obligations of citizens and corporations and broadly defines national security as the relative absence of internal or domestic threats to the state’s power to govern and the capacity to protect security in a sustainable manner.</td>
</tr>
<tr>
<td><strong>2013 Company Law</strong></td>
<td>Requires all Chinese companies to establish and maintain an active organization of the CCP to carry out Party activities. This ensures CCP knowledge and direction regardless of whether a company is a state-owned enterprise.</td>
</tr>
</tbody>
</table>

(U) FBI Outreach & Liaison Tool; 07 FEB 2022; (U) PRC Laws Impacting U.S. Business Operations with PRC Enterprises; Citated portion is unclassified; Overall document is unclassified.  
(U) CSIS.org; 30 AUG 2021; (U) How the Data Security Law Sets the Stage for the Tech Industry in China and Beyond; https://www.csis.org/blog/strategic-technologies-blogs/how-data-security-law-sets-stage-tech-industry-china-and-beyond; Accessed 23 AUG 2022; The Center for Strategic and International Studies (CSIS) is a U.S. bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world’s greatest challenges.  
(U) FBI; LBR 220405006; 05 APR 2022; (U) China: 2021 Counterspying Likely Increases Risk to U.S. Intellectual Property; Citated portion is unclassified; Overall document is unclassified.  
(U) Covington & Burling, LLP; 09 DEC 2020; (U) China Enacts Biosafety Law; www.cov.com; Accessed 14 JUN 2022; Covington & Burling is an international law firm that opened in Washington D.C. in 1919.  
(U) FBI Outreach & Liaison Tool; 07 FEB 2022; (U) PRC Laws Impacting U.S. Business Operations with PRC Enterprises; Citated portion is unclassified; Overall document is unclassified.  
(U) CSIS.org; 25 JUN 2020; (U) Who Benefits from China’s Cybersecurity Laws? https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws; Accessed 22 AUG 2022; The Center for Strategic and International Studies (CSIS) is a U.S. bipartisan, nonprofit policy research organization dedicated to advising practical ideas to address the world’s greatest challenges.  