



FBI

COUNTERINTELLIGENCE STRATEGIC PARTNERSHIP INTELLIGENCE NOTE (SPIN)

SPIN: 15-007

SEP 2015

(U) Chinese Talent Programs

(U) INTRODUCTION

(U) Chinese Talent Programs are a vital part of Chinese industry. Talent programs recruit experts to fill technical jobs that drive innovation and growth in China's economy. National, provincial, and municipal talent recruitment programs provide opportunities for experts to work in industry and academic organizations supporting key areas deemed critical to China's development. The talent programs recruit experts globally from businesses, industry, and universities with multiple incentives to work in China. Associating with these talent programs is legal and breaks no laws; however, individuals who agree to the Chinese terms must understand what is and is not legal under US law when sharing information. A simple download of intellectual property (IP) or proprietary information has the potential to become criminal activity.



(U//FOUO) The large number of foreign students, researchers, scientists, and professionals in the United States, combined with current technological capabilities, allows foreign governments to contact and recruit individuals with the hopes to acquire advanced technology without research costs. While the majority of the population are law abiding individuals, anyone has the capability to acquire information. The theft of information can come from current or former employees, business partners, consultants, contractors, temporary hires, foreign agents, suppliers, or even vendors who have access to proprietary information.

(U) Recruiting these individuals allows China to:

- (U//FOUO) Gain access to research and expertise for cutting edge technology
- (U//FOUO) Benefit from years of scientific research conducted in the United States supported by US Government grants and private funding
- (U//FOUO) Severely impact the US economy.

(U) The goal of this SPIN is to provide an overview of the potential threats posed by the Chinese Talent Programs.

(U) CHINA'S TWELFTH FIVE-YEAR PLAN

(U//FOUO) China's National People's Congress approved a new national development program that will last for the next five years. These Five-Year Plans emphasize higher quality growth by determining themes and targets to ensure long-term prosperity. China is currently on its Twelfth "Five-Year Plan" covering 2011 to 2015, which focuses on the following:

1. **New Energy:** Nuclear, wind, and solar power
2. **Energy Conservation and environmental protection:** Energy reduction targets
3. **Biotechnology:** Drugs and medical devices
4. **New Materials:** Rare earths and high-end semiconductors
5. **New Information Technology:** Broadband networks, Internet security infrastructure, and network convergence
6. **High-end equipment manufacturing:** Aerospace and telecom equipment
7. **Clean energy vehicles**

(U) Among the plan's goals is the transformation of China from a manufacturing hub to a world leader in innovation, which will be partly met by an increase in highly skilled workers from 114 million to 180 million by 2020. Additionally, the Chinese Government spending on talent development is expected to increase from 10.75 percent of the country's gross domestic product (GDP) to 15 percent by 2020, which is approximately \$1.3 trillion based on the 2014 China GDP. China's talent development program acts as a vehicle to achieve the Five Year Plan's goals.

(U) THOUSAND TALENTS PROGRAM

(U//FOUO) China's most prominent national talent recruitment program is the "Recruitment Program of Global Experts," which is commonly known as the Thousand Talents Program. It focuses on identifying key national-level organizations and associated personnel involved in implementation and management.

(U) Its goal is to recruit ethnic Chinese experts from Western universities, research centers, and private companies to boost China's national capabilities in the science and technology (S&T) fields and to move China forward as an innovative nation. The program also implemented sub-programs for both young and foreign (non-ethnic Chinese) experts.

(U//FOUO) Originally, this program had a five-to-ten year goal of recruiting 2,000 professionals worldwide who could lead innovation and pioneering work in key technologies, and promote the development of emerging industries. However, this program expanded its scope -- recruiting far more than the initial goal of 2,000 individuals -- and extended its life through at least 2020.

(U) In order to be eligible as a candidate for the Thousand Talents Program, an individual must be in a field of study the Chinese Academy of Science (CAS) deems critical or meet the following criteria:

- (U) Expert or scholar with full professorship in a prestigious foreign university or research and development (R&D) institute
- (U) Technical managerial professional in a senior position at an internationally known company or financial institution
- (U) Entrepreneur holding IP rights or key technologies and possesses overseas experience

**(U) HUNDRED TALENTS PROGRAM**

(U//FOUO) The Hundred Talents Program was launched in 1994 and was China's first overseas-oriented program to recruit high-level talent. The program is exclusively designed for cultivating scientific research personnel at CAS and focuses on attracting a younger talent pool.

(U//FOUO) The primary goal of the program is to cultivate a group of leaders in their areas of specialty to work at various CAS organizations. Although focused on recruiting overseas Chinese, the Hundred Talents Program will accept applicants who are currently in China. These domestic-based applicants must demonstrate internationally-recognized expertise. Most of the Hundred Talents selectees have become "chief scientists" of various 973 Program (National Basic Research Program) projects; "responsible persons" on 863 Program (National High Technology R&D Program) projects; associated with Project 111, which recruits the world's top researchers and scholars regardless of nationality or ethnic origin to work with Chinese universities; directors of state key laboratories or CAS key laboratories; or have taken high-level leadership positions within CAS institutes or offices. Selectees of this program are given 600,000 RMB (about \$99,000) for resettlement costs and two million RMB (about \$330,000) in startup funding for research.

**(U) OTHER TALENTS PROGRAMS**

(U//FOUO) The Innovative Talent Promotion Program is another Chinese Government-sponsored program. This program's ultimate goal is to create a cadre of world-class scientists and entrepreneurs who will lead technological innovation and allow China to compete internationally in S&T and strategic emerging industries.

(U//FOUO) The Thousand Youth Talents Program for Distinguished Young Scholars is a development program for young talent. Top candidates are sent to first-class universities overseas to study. These individuals are groomed into business professionals needed for the future development of China.

(U//FOUO) Lastly, there are programs that seek to develop entrepreneurial talent by focusing on building an internationally competitive corporate management cadre. The program plans to cultivate entrepreneurs with "world foresight, strategic thinking, pioneering spirit, and operating capability," and it sets a goal of having 10,000 talented personnel in management who have expertise in strategic planning, capital management, human resources management, finance and accounting, law, etc.

(U) THREAT TO US BUSINESS AND UNIVERSITIES

(U//FOUO) Chinese Talent Programs pose a serious threat to US businesses and universities through economic espionage and theft of IP. The different programs focus on specific fields deemed critical to China, to boost China's national capability in S&T fields. These subject matter experts often are not required to sign non-disclosure agreements with US entities, which could result in lost of unprotected information that jeopardizes contracts or research funding. One of the greatest threats toward these experts is transferring or transporting proprietary, classified, or export-controlled information, or IP, which can lead to criminal charges.

(U//FOUO) The threat not only targets businesses or universities but potentially targets the researchers or scientists themselves. The technology researched or developed not only costs millions of dollars but costs years, if not decades to develop. Additionally, the theft of information or IP creates a risk that someone else could take credit for the researcher's efforts. The information stolen can be recreated, resold or claimed by others, which in turn will cost the originator credibility and potential funding for future endeavors.

(U) Theft of intellectual property is an increasing threat to organizations and can go unnoticed for months or even years. In today's society, technology affords easier access to every aspect of academia and business. Some of these tools have become effective for recruiting, such as social media. Social media websites often display large amounts of personal data, such as who an individual works for, phone numbers, known associates, previous jobs, and locations. Additionally, websites like LinkedIn have full resumes, detailing the history of an individual's achievements and accomplishments.

(U) The FBI assesses each year the United States loses billions of dollars due to technology transfer. While it is important to conduct collaborative research, it is vital for the survival of US businesses and universities that they protect their information and mitigate lost or stolen information.

(U) Areas of Interest for Recruitment:

- Information Technology
- Biotechnology
- Aerospace
- Materials & Manufacturing
- Sensors & Optics
- Energy & Environment
- Basic Sciences

**(U) MEDICAL CENTER OF WISCONSIN**

(U) **Zhao, J. Hua** – (DPOB: 1971, China) In February 2013, Zhao, a research assistant at Medical College of Wisconsin (MCOW) under Professor Marshall Anderson, stole three vials of C-25, a compound patented by Anderson and used in his cancer research. Security footage examined during an internal investigation revealed Zhao entering Anderson's office and leaving shortly after.

(U) Zhao was reprimanded previously for placing laboratory data on his personal computer. The internal investigation found research data on C-25. Zhao claimed the data would be used to conduct further studies at Zhejiang University.

He was ordered to remove the data from his computer and place it on an MCOW computer. Additionally, MCOW discovered a posting by Zhao on an Internet site called Researchgate indicating he discovered a cancer fighting compound he wanted to bring back to China.

(U) In March 2013, Zhao was arrested. In addition to the 384 files found on Zhao's personal computer relating to Anderson's research was an application to the National Natural Science Foundation of China that provides funding for many talent programs and to a Chinese foundation claiming he invented C-25 and requesting funding for additional research. This application was an exact translation of the grant application written by Professor Anderson several years earlier. It was also determined that Zhao accessed his MCOW computer remotely on the day he was suspended and attempted to delete the files he stole relating to C-25. Zhao was convicted to time served in August 2013.

(U//FOUO) Zhao had a previous history of disregarding the appropriate handling of university property and had full access to Professor Anderson's lab. His access allowed him the ability to walk in and out of the lab at his own discretion to steal the vials of C-25 and laboratory data. Had C-25 not been patented by Anderson, Zhao could have claimed and patented the cancer-fighting compound for himself. Additionally, Zhao's LinkedIn profile indicated he held a position at Zhejiang University, which has ties to the Thousand Talent Program.

(U) DUKE UNIVERSITY

(U) **Liu, Ruopeng** – (DPOB: 1983, China) In 2006, Liu, a graduate student at Duke University, worked in the laboratory a US researcher studying metamaterials. Liu had full access to the researcher's lab, which conducted basic and fundamental research. While working for this researcher, Liu arranged meetings between the researcher's lab and Cui Tie Jun, a Chinese program manager associated with Project 111 (focused on basic science and advanced technology by recruiting the best international experts to China to study from). The idea behind this connection was to share ideas, however, the US researcher eventually realized most of the ideas were coming from his lab.

(U) Over the next few years, he discovered pictures and information related to his research used to market a business started by the Liu. The business originally seemed plausible to him, because he knew Liu was applying for positions with Massachusetts Institute of Technology, which tends to favor faculty members who also have an entrepreneurial bent. The information marketed by Liu attracted a Chinese technology company. Additionally, Liu invited two Chinese visitors associated with CUI's lab from Southeast University to visit the lab. The visitors took photographs of all the equipment in the lab, including the make and model, which in turn were used to reproduce the lab in China.

(U) In 2009, the US researcher received a book entitled *Metamaterials: Theory, Design, and Applications* by Cui, Liu, and the researcher that was published in the United States. Unknowingly, the researcher had in fact signed off on some forms and received multiple e-mails regarding the book by relying on Liu's interpretation. At the same time, Liu, Cui, and another Chinese individual collaborated on a research idea based on a paper regarding carpet-cloak theory later published in 2009 in an issue of *Science*. Located in the article is a footnote acknowledging the support from Innovation Technology, National Science Foundation, National Basic Research Program (973) of China, National Science Foundation of Jiangsu Province, and Project 111.

(U) While the researcher's lab does not conduct restricted research, it receives funding from the US Department of Defense and US Intelligence Community. Since the research was not restricted, there were no rules against or restrictions on the lab's collaborative research efforts. Liu did not have to sign a non-disclosure agreement. Liu moved back to China after the researcher retracted his recommendation for Liu's employment at Princeton with Dr. Stephen Chou, the head of the nanotechnology laboratory. Liu has reportedly established a research institution in Shenzhen.

(U//FOUO) By convincing the US researcher to collaborate with Cui, Liu was able to freely share information and invite visitors to the lab. Although this was not restricted research, the metamaterials research could have both military and civilian applications. The US researcher risked his research by allowing visitors to come into his lab without personally looking at their background and being too trusting of his scientific relationship with Liu.

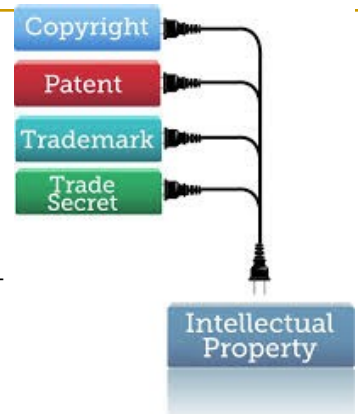
(U) HOW TO PROTECT YOUR ORGANIZATION

(U) The first step to protecting your business or university is to identify the threat.

- Who would benefit from your information, processes, or strategies?
- Who are your competitors?
- Have individuals been unusually interested in what you do?

(U) The next step is to identify proprietary or trade secrets or IP. This includes, but is not limited to the manufacturing process, financial information, list of suppliers and customers, chemical formulas, marketing strategies, and R&D data. By understanding the threat and your business or university's critical technologies, it can help you identify methods in which they can be easily stolen. Theft, bribery, espionage, blackmail, hacking, and electronic intercepts are just some of the different methods individuals may use to steal trade secrets.

- (U) Have professors, students, and employees sign non-disclosure agreements.
- (U) Identify foreign personnel who are sponsored by professors/employees.
- (U) Understand agreements between international organizations and US businesses and universities.
- (U) Identify and label or mark IP or sensitive data that is most important to US businesses and universities.
- (U) Identify methods in which professors and employees are contacted (for example, e-mail, social media, conferences) and educate them on what solicitation looks like.
- (U) Report any incidents or concerns to your security office and local FBI field office.



(U) If you wonder about the safety of your research or intellectual property, or the legality of your interactions with China, ask yourself the following questions. If any of the answers concern you, or you would like additional information, please contact your local FBI Strategic Partnership Coordinator or FBI field office.

- (U) Do you collaborate with anyone who is currently in China?
- (U) Do you have any publications? If so, in which journals and with whom? Which institutions are they associated with?
- (U) What type of funding do you have to conduct your research? Where do you obtain your funding?
- (U) Do you belong to any professional societies? If so, which ones and where are they based?
- (U) Do you travel regularly to China? Is it for business or pleasure or both? How long do you stay in China during these trips? Are you working with anyone in China on your research during this time?
- (U) How do you maintain contact with your laboratory in the United States while in China? Do you contact it via computer (login to laboratory site)?
- (U) Do you plan to return to China permanently? What will you do for employment?
- (U) Where did you attend school? What type of degrees did you earn? How did you apply for a fellowship, post-doctoral position, guest researcher or other employment with your current employer? Did someone you know refer you to this lab, university, or principal investigator?
- (U) What type of research do you conduct? What are the applications of this research? Do you expect to get a patent from this research?
- (U) With whom are you working at your laboratory? Do you collaborate with individuals from other research institutions in the United States or abroad?

Sources

(U) KPMG; China's 12th Five-Year Plan: Overview; 2011; <http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf>; accessed 04 March 2015.

(U) Online Article; Chinese Academy of Science: Thousand Talents Program; 2012; <http://englishucas.ac.cn/JoinUs/Pages/default.aspx>; accessed 04 September 2014.

(U) OSC Analysis 14-024; accessed 06 March 2015.

(U) Wang, Huiyao; China's National Talent Plan: Key Measures and Objectives; 2010; <http://www.brookings.edu/research/papers/2010/11/23-china-talent-wang>; accessed 06 March 2015.

(U) Robertson, John; Investigating Intellectual Property Crime; 2010; https://intranet.fbinet.fbi/ccrsb/CyD-old/CCS/CCU-3/CCTF_Document_Library/2010%20CCTF%20Conference%20Presentation%20Materials/IPR%20Presentation.ppt; accessed 09 March 2015.

This product was prepared by the FBI Strategic Partnership Unit (CD-4F). Please provide any questions or comments to your local Strategic Partnership Coordinator (SPC) or CD-4F at Strategic_Partnerships@ic.fbi.gov.