STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Brandon Tower, Special Agent, Federal Bureau of Investigation, being duly sworn, state as follows:

A. Affiant's Training and Experience.

I am a Special Agent with the Federal Bureau of Investigation. I have been employed by the FBI since October 2019. I have been trained by the FBI to investigate federal criminal activity and to protect the security interests of the United States. Since March 2020, I have been assigned to a squad focusing on intelligence threats from the People's Republic of China. As part of that unit, I am responsible for detecting, deterring, and frustrating the efforts of Chinese intelligence agents and agencies. As an FBI Special Agent, I have training in the preparation, presentation, and service of criminal complaints and arrest and search warrants. Prior to joining the FBI, I was a criminal prosecutor in the Suffolk County District Attorney's Office in Boston, Massachusetts for five years.

The facts in this affidavit are based on my personal observations, my training and experience, and information obtained from other witnesses and law enforcement agents. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

B. The U.S. Department of Defense and Classified Information.

The U.S. Department of Defense is a U.S. executive branch agency tasked with providing military forces needed to deter war and protect the security of the United States. National security information constitutes information owned by, produced by, produced for, and under the control of the United States government that relates to the conduct of foreign relations or the national defense. Pursuant to Executive Order 13526 and its predecessors, national security information corresponds to three possible classification levels:

> Information is classified as TOP SECRET if the unauthorized disclosure of that information reasonably could be expected to cause *exceptionally grave damage* to the national security that the original classification authority is able to identify and describe.
>
> Information is classified as SECRET if the unauthorized disclosure of that information reasonably could be expected to cause *serious damage* to the national security that the original classification authority is able to identify and describe.
>
> Information is classified as CONFIDENTIAL if the unauthorized disclosure of that information reasonably could be expected to cause *damage* to the national security that the original classification authority is able to identify and describe.

Only individuals determined to be eligible by an appropriate U.S. government official can lawfully access classified information. Such an individual is required to sign an approved non-disclosure agreement, receive a security clearance, and possess a "need to know" the classified information. The storage of classified information must be in an approved facility and container commensurate with its classification level.

Classification markings represent the usual means of communicating the need to protect classified national security information. Classified documents typically contain banners on the top and bottom stating the highest level of classification and any additional controls associated with the materials, as well as markings relating to the information contained in each paragraph. In addition to classification markings, classified information at times contains dissemination markings which restrict the distribution of the information. These markings include "NF" or "NOFORN" meaning, "No Foreign Dissemination." The NOFORN marking denotes a limitation to disseminate the information only to U.S. persons.

C. The People's Republic of China Intelligence Services.

The PRC Intelligence Services is a general term that encompasses both the civilian and military components of Chinese intelligence programs. More specifically, civilian intelligence collection is handled by the Ministry of State Security ("MSS"). The MSS's

role is similar to the FBI and the Central Intelligence Agency combined under one intelligence directorate responsible for counter-intelligence, foreign intelligence, and political security. The MSS consists of a central ministry, provincial state security departments, and municipal state security bureaus, such as the Beijing State Security Bureau and the Shanghai State Security Bureau.

The MSS and its regional bureaus are tasked with identifying and influencing the foreign policy of other countries, including the United States. The MSS and its bureaus seek to obtain information on political, economic and security policies that may affect the PRC, foreign intelligence operations directed at the PRC, and biographical profiles of foreign politicians and intelligence officers. Additionally, the MSS and its bureaus are tasked with conducting clandestine and overt human source operations, of which the United States is a principal target for the PRC's intelligence gathering.

MSS operations use trained intelligence case officers, as well as non-professional collectors referred to as "cut-outs" or "co-optees," which are trusted persons used to create a compartment between members of an operation to enable them to pass material and/or messages securely. A cut-out or co-optee can operate under a variety of covers, posing as diplomats, journalists, academics, or business people both at home and abroad. These individuals are tasked with spotting, assessing, targeting, collecting, and running sources that have access to classified, proprietary, and sensitive information that the government of the PRC can utilize for an economic, political, or military advantage.

The PRC Intelligence Services use state-owned enterprises ("SOE") and their employees to collect intelligence information from human sources. An SOE is a legal entity that undertakes commercial activities on behalf of an owner-government. SOE's may have different types of legal status, including being a formal part of government or being a business with a state as a regular or dominant stockholder. While they may also have public policy objectives, SOEs are differentiated from other forms of government agencies or state entities that are established to pursue purely non-financial objectives. The role of the Chinese Communist Party ("CCP") in SOEs has varied at different

periods but has increased during the rule of CCP General Secretary Xi Jinping, with the CCP formally taking a commanding role in all SOEs as of 2020.

PRC Intelligence Services source operations tend to originate inside the PRC, where the intelligence services prefer to meet with assets. To facilitate continued meetings inside the PRC, the PRC Intelligence Services will arrange and/or pay for travel and expenses. The intelligence services are known to pay their sources not only in cash, but also through other means, including business considerations or other types of assistance within the PRC.

D. Background Information About JOSEPH DANIEL SCHMIDT.

Beginning in January 2015, and continuing to early January 2020, JOSEPH DANIEL SCHMIDT (herein after, "SCHMIDT") was an active duty soldier in the U.S. Army. SCHMIDT ultimately rose to rank of Army Sergeant. On January 8, 2020, SCHMIDT completed his term of service and transitioned to the Inactive Ready Reserves.

SCHMIDT's primary assignment during his active duty was to the 109th Military Intelligence Battalion at Joint Base Lewis-McChord ("JBLM"), located in Pierce County, Washington. SCHMIDT was assigned to a Human Intelligence ("HUMINT") squad as a HUMINT Collector and ultimately became a Team Leader of other HUMINT Collectors. In this role, SCHMIDT supervised HUMINT collection operations and the production of intelligence reporting, analysis, and the dissemination of intelligence products. SCHMIDT's work directly supported the Indo-Pacific Command, the U.S. Department of Defense's geographic combatant command that covers the Pacific Ocean and Indian Ocean region, including the PRC.

As a HUMINT Collector and Team Leader, SCHMIDT attended various intelligence-related trainings, including: Advanced and Basic Leader Courses; Counterintelligence Collections; Human Intelligence Collector; Human Intelligence Operation Management; and Human Intelligence Tradecraft. SCHMIDT also attended the Defense Language Institute Chinese-Mandarin training.

While on active duty, SCHMIDT had access to classified intelligence collection and reporting systems, including SECRET databases that are utilized for research, reporting, and Army organizational information. SCHMIDT was given access to Secret Internet Protocol Router Network ("SIPRnet") and Sensitive Compartment Information Facility ("SCIF") space at JBLM. SIPRnet is a computer system containing information classified up to SECRET, while SCIF spaces can contain information classified up to the level of TOP SECRET.

During his tenure with the Army, SCHMIDT was granted a TOP SECRET and Sensitive Compartment Information ("SCI") security clearance. SCHMIDT was read out of SCI accesses on December 17, 2019, although his TOP SECRET clearance remained active. SCHMIDT received a briefing on how to handle and protect classified information. In consideration of being granted access to classified information, SCHMIDT entered into a non-disclosure agreement with the Army on March 23, 2015.

E. SCHMIDT's Communications and Cloud Storage Facilities.

SCHMIDT was the user of various communications and cloud storage facilities that he used during and in furtherance of the criminal activities alleged in the Indictment filed in this case. I have obtained subscriber records from Google, Microsoft, and Apple related to each of these facilities and other information that connects SCHMIDT to each of the accounts, as summarized below:

Gmail account 1 was subscribed to in the name of "Joe Schmidt." In January 2018 and April 2019, SCHMIDT provided Gmail account 1 to the Army as his email address. Gmail account 1 also has a Google account associated with it.

Gmail account 2 was subscribed to in the name of "Joey Schmidt" and lists Gmail account 1 as the recovery email address for the account. According to records obtained from U.S. Customs and Border Protection, SCHMIDT used Gmail account 2 to make travel reservations for his trips to the PRC, as discussed below. Gmail Account 2 also has a Google account associated with it.

Outlook account 1 was subscribed to in the name of "Joseph Schmidt." Outlook account 1 was listed on SCHMIDT's resume posted on his open source LinkedIn page prior to the page's deletion.

Yahoo account 1 was subscribed to in the name of "Joey Schmidt." On multiple occasions, Yahoo account 1 appeared to be a forwarding address for Gmail account 2.

Apple iCloud account 1 was subscribed to in the name of "Joseph Schmidt" with a listed address of "JBLM, Washington." Gmail account 1 and Gmail account 2 were listed as the email addresses for the user of Apple iCloud account 1.

F. SCHMIDT's Historical Travel to the PRC.

During November and December of 2017, while on active duty with the Army, SCHMIDT took personal leave and traveled to the PRC. In April 2017, SCHMIDT emailed himself a copy of the Chinese visa application he filled out prior to his trip, on which he stated: "I plan to travel to China every New Year to learn about Chinese culture… I would like to travel to China many times over the course of the next ten years. I want to learn as much about China's culture and history as I can, and so I plan to travel to China annually." SCHMIDT identified his employer as "Department of Defense Army" and his current occupation as "soldier."

SCHMIDT submitted at least two additional leave requests to the Army for the stated purpose of traveling to the PRC between August 2017 and April 2018. For reasons unknown, SCHMIDT did not take any of these trips.

On February 22, 2019, SCHMIDT conducted the following search in the Google internet browser: "[I]f it doesn't stop im [sic] going straight to china. I'm not taking anymore [sic] of this because someone literally thought I looked funny after they spiked my drink."[1] FBI agents have interviewed Army personnel familiar with SCHMIDT and have not been able to learn any information relating to the context of this Google search.

[1] This Google search – and the others referenced in this affidavit – was recovered from the stored historical records in SCHMIDT's Google accounts.

On January 14, 2020, six days after he transitioned to inactive duty status, SCHMIDT departed the United States on a flight itinerary destined to Beijing. On January 18, 2020, SCHMIDT returned to the United States from Qingdao Airport in China.

G. SCHMIDT Travels to Turkey in February 2020.

On February 9, 2020, Schmidt departed the United States and traveled to Istanbul, Turkey. SCHMIDT returned to the United States on March 2, 2020. While in Turkey, SCHMIDT engaged in activities relevant to the charges in the Indictment filed in this case, as detailed below.

Between February 17, 2020, and February 29, 2020, SCHMIDT conducted internet research about defection from the United States and countries that do not have extradition treaties with the United States. Specifically, SCHMIDT conducted the following searches in the Google internet browser and/or visited the following web pages through Google:

- Searched "chinese consulate"
- Searched "soldier defect"
- Searched "chinese embassy"
- Visited "http://istanbul.china-consulate.org/tur"
- Searched "iranian consulate"
- Searched "iranian embassy"
- Visited web page: "Chinese Consulate-General in Istanbul (Turkey)"
- Searched "chinese.consulate number doesn't go through"
- Searched "turkey extradition military defection"
- Searched "countries that dont extradite"
- Searched "can [specified U.S. Person] be extradited"
- Searched "can you be extradited for treason"
- Searched "iran visa"

- Searched "afghanistan visa"
- Searched "pakistan resident visa"
- Searched "russian visa costs"
- Searched "countries with most negative relations with US"
- Visited web page: "Ten Countries That Hate America Most – 24/7 Wall St"
- Searched "chinese embassy Istanbul"
- Searched "how did [specified U.S. Person] defect"
- Visited: "They wanted me gone: [specified U.S. Person] tells of whistleblowing"
- Searched "chinese embassy"
- Searched "what is china's intelligence agency"
- Visited: "https://en.m.wikipedia.org/wiki/Ministry_of_State_Security_(China)"
- Searched "subreddit spying"
- Visited on Reddit: "looking_for_a_subreddit_about_spy_stuff"
- Searched "russian embassy Istanbul"
- Visited web page: "Consulate General of Russia in Istanbul, Turkey"

On February 24, 2020, SCHMIDT used Gmail account 1 to send the following email to the pubic email address for the Chinese Consulate in Istanbul:

> Hello,
>
> My name is Joe Schmidt. I am a United States citizen looking to move to China. I currently reside in Istanbul, and am trying to set up an appointment at the consulate in Istanbul.
>
> I also am trying to share information I learned during my career as an interrogator with the Chinese government. I have a current top secret clearance, and would like to talk to someone from the Government to share this information with you if that is possible.
>
> My experience includes training in interrogation, running sources as a spy handler, surveillance detection, and other advanced psychological operation

> strategies. I would like to go over the details with you in person if possible, as I am concerned with discussing this over email.
>
> I'm sorry for using English, but I want to make sure that I do not miscommunicate. Please contact me at your earliest convenience if I can set up a time to meet with you.
>
> Thank you,
>
> Joe Schmidt

On February 26, 2020,[2] SCHMIDT created a Word document entitled, "Important Information to Share with Chinese Government." The document was recovered from SCHMIDT's Apple iCloud account. As described further below, the Army has determined that this document contains a variety of classified information that relates to the national defense.

On February 26, 2020, SCHMIDT conducted a Google search for "chinese military papers." That same day, SCHMIDT used Outlook account 1 and Yahoo account 1 to send several identical emails to email addresses associated with the *People's Daily*, *China Daily*, and Phoenix Television.[3] The emails stated:

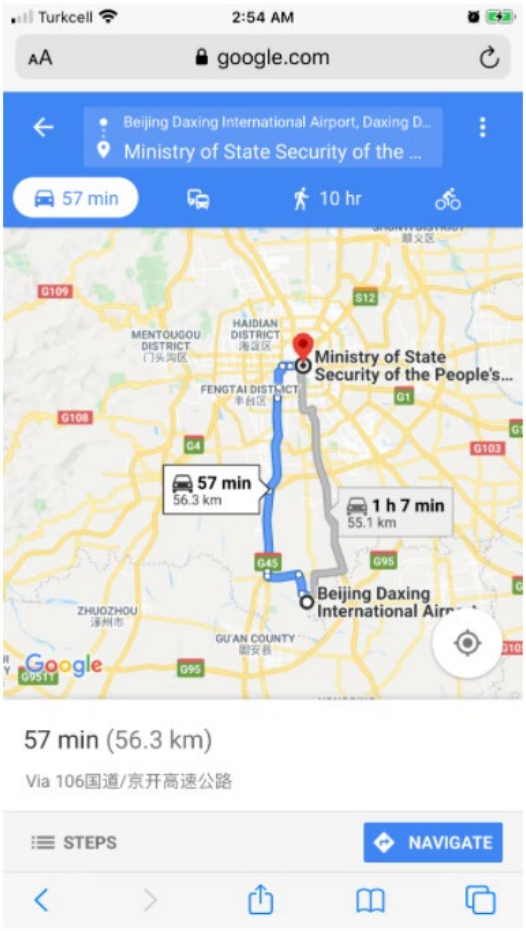
> Hey sorry to write this in English. I am not a native Chinese speaker so I lose a lot in translation. I'm just writing you to check and see if you would be interested in using any of my military stories in your paper. I have several years experience in military intelligence, and I think your audience would be very interested in reading some of these. Let me know if that's a possibility. Thanks!

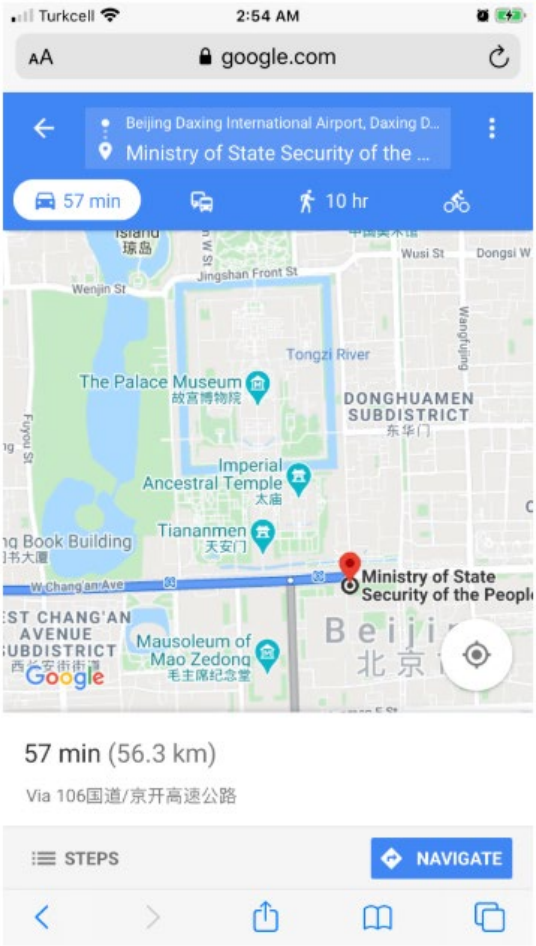
---

[2] For the purposes of this affidavit, I have used the date of the historical records' creation and/or transmission as of UTC time.

[3] I know from FBI investigations that *The People's Daily* is a newspaper owned by the Central Committee of the Chinese Communist Party. In 2020, the United States Department of State designated the *People's Daily* a foreign mission of the PRC government. The *China Daily* is an English-language newspaper owned by the Publicity Department of the Chinese Communist Party. Per open sources, Phoenix Television is a PRC state-owned television network. I have relied on open sources in this instance because it is likely the same information Schmidt would have had available when using the internet to research options for transmitting information to the Chinese intelligence services.

On or about February 29, 2020, while still in Turkey, SCHMIDT used Google Maps to conduct research on driving directions from the airport in Beijing to the MSS headquarters. The following screenshots from Google Maps were recovered from SCHMIDT's iCloud account:





On March 2, 2020, SCHMIDT departed Turkey and returned to the United States.

H. SCHMIDT Travels to the PRC in March 2020.

A few days later, on March 6, 2020, SCHMIDT departed the United States and traveled to Hong Kong. SCHMIDT has not since returned to the United States.

On March 9, 2020, a few days after arriving in Hong Kong, SCHMIDT traveled to Beijing, returning to Hong Kong on March 12, 2020. While in Beijing, SCHMIDT

engaged in a variety of activities relevant to the offenses charged in the Indictment filed in this case, as detailed below.

On March 9-10, 2020, SCHMIDT conducted several Google searches and visited websites related to espionage and intelligence topics, including:

- Searched "interrogation field manual"
- Searched "fm human intelligence"
- Visited webpage: "If it's Spy, it's here – Reddit"
- Visited: "Espionage – Reddit"
- Visited: "What Do Real Spies Do and How are they Recruited – Reddit"
- Visited: "I am [specified U.S. Person 2] a Former Covert CIA – Reddit"

That same day, SCHMIDT created and modified a Word document entitled, "Humint AIT." The document was recovered from SCHMIDT's Apple iCloud account. The "Humint AIT" document is four pages long and discusses in detail various aspects of U.S. Army intelligence collection, dissemination, and training, including: the types of intelligence reports that are prepared and disseminated; methods of conducting interrogations; methods of conducting human source operations; and the types of training courses offered for HUMINT officers. An official with the U.S. Army who is qualified and authorized to make classification determinations has reviewed this information and determined that, although unclassified, it constitutes information related to the national defense because it pertains to intelligence activities, including covert actions, and intelligence sources and methods.

The following day, on March 10, 2020, SCHMIDT's phone was in close proximity to the MSS headquarters in Beijing. The below screenshot taken from Apple Maps was recovered from SCHMIDT's iCloud account. The map depicts SCHMIDT's phone's location (the blue dot in the lower left-hand corner) relative to the Ministry of Public Security, which is located at the same site as the MSS headquarters that SCHMIDT had researched on Google Maps on February 29, 2020.

On March 11, 2020, SCHMIDT used Google to search for and view several maps of U.S. Military installations. Many of the installations were locations SCHMIDT had visited while with the Army, including Fort Huachuca, the U.S. Army Intelligence Center of Excellence, the Military Intelligence Museum, Schofield Barracks, and Joint Base Lewis McChord, McChord Air Force Base, Building 9116 (the home of the 109th Expeditionary Military Intelligence Battalion).

I. SCHMIDT Continues his Espionage Activities from Hong Kong.

SCHMIDT departed Beijing on March 12, 2020, and returned to Hong Kong where he has resided since that time. As detailed below, SCHMIDT continued his espionage activities from Hong Kong during the next several months.

//

//

//

1. SCHMIDT Drafts Documents Containing National Defense Information.

On or about March 16, 2020, SCHMIDT created a Word document entitled "High Level Secrets" (written in Chinese characters). SCHMIDT made modifications to the "High Level Secrets" document on March 19, 2020. That same day, SCHMIDT also modified the document he previously created while in Turkey, entitled, "Important Information to Share with Chinese Government." Both documents were recovered from SCHMIDT's Apple iCloud account. As detailed below, the Army has determined that both documents contain a variety of classified information that relates to the national defense.

The "High Level Secrets" document contains 23 pages. Nearly all of it is written in English except for the title and the following introductory passage (translated from Chinese characters):

> If you read this document, please make sure that the State Security Bureau of People's Republic of China [MSS] receives it. The content is a high-level secret of U.S. intelligence and can help the Chinese people. The content is in English, please use an advanced translator to translate it into Chinese to avoid language barriers.

At the beginning of the document, SCHMIDT explained his purpose in creating the document and his desire to transmit national defense information to PRC Intelligence Services:

> My name is Joseph Schmidt. I'm a human intelligence collector that just got out of the military. I'm trying to send some information to the Chinese government about the United States Intelligence Services. I'll provide some documents to verify my identity, and I hope that it reaches the proper authorities.
>
> *****
>
> My last year in the military [] left me with experience working with an advanced intelligence team on a project with technology that is very compartmentalized, to the extent that the majority of people in the intelligence field are unaware of its existence. I will only discuss this

> technology in person if I can meet with a qualified member of the Chinese Security Bureau.
>
> *****
>
> Over the course of the next several weeks, I'll be releasing information in a series of short documents about my experience with United States Intelligence. I also have experience with highly classified technology that I would be happy to share with you if you would like my expertise. I can help to create training programs that either mimic American Intelligence Source Handling courses, or training for surveillance teams to more effectively identify American Spy Handlers by training your intelligence teams in the highest techniques that American Intelligence forces use.
>
> *****
>
> For documented proof of my service and position, please see my attached Enlisted Record Brief (ERB) which contains proof of my Top Secret-Secured Compartmentalized Information Clearance, as well as all the afore-mentioned schools and duty locations. I also am including a picture of my CAC card, which is my military Identification, my DD 214 which serves as proof of my honorable discharge from service, a picture of my SIPR token, which provides access to the United States Secret intelligence network, and a photocopy of my passport.

The remainder of the "High Level Secrets" document discussed SCHMIDT's training and experience in HUMINT collection; the functions and capabilities of U.S. HUMINT collectors; the curriculum and substance of various Army HUMINT training courses; and tradecraft used by U.S. HUMINT collectors, including information regarding surveillance detection routes, casing for meeting locations, source assessment, and operational testing. The document also identifies the geographic locations of numerous U.S. Military installations.

//

//

//

//

//

The "High Level Secrets" document has been reviewed by a Defense Intelligence Senior Executive Service ("DISES") member in the U.S. Army,[4] who is an Original Classification Authority ("OCA"). The OCA determined that information contained therein is properly classified at the SECRET level. Specifically, the OCA identified numerous portions of the document that constitute national defense information.

The document entitled "Important Information to Share with Chinese Government" contains 22 pages. It contains extensive details regarding the use of human sources in U.S. military intelligence, including source types, source assessment and categorization, assessing sites for source meetings, source communication planning, and the application of tradecraft to source handling. The OCA reviewed the document and determined that information contained therein is properly classified at the SECRET level and identified numerous portions of the document that constitute national defense information.

2. SCHMIDT Attempts to Transmit Information to PRC SOE 1.

On March 19, 2020, SCHMIDT took photographs of the front and back of his Army PKI card and his Army CAC card. The photographs were recovered from Schmidt's Apple iCloud account. According to Army personnel, the PKI card serves as an encryption key for accessing the Army's classified Secret network and related databases, referred to as the Secret Internet Protocol Router Network ("SIPRnet"). The CAC card serves as a badge/ID that allows access into certain Army premises.

//

//

//

[4] The DISES member has 26 years of active service and two years of civilian service with the U.S. Army. He currently serves as the Director, Directorate of Counterintelligence, Human Intelligence, Security, and Foreign Disclosure, Office of the Deputy Chief of Staff, G-2, Headquarters, Department of the Army at the Pentagon. His responsibilities include the review of Army Human Intelligence information for classification purposes pursuant to Executive Order 13526 ("Classified National Security Information"). As the Director, Army G-2X, he has been delegated by the U.S. Army Deputy Chief of Staff, G-2, Original Classification Authority pursuant to Executive Order 13526.

On March 22, 2020, SCHMIDT used Gmail account 1 to send an email to a PRC state-owned enterprise ("SOE 1").[5] Prior to sending the email, SCHMIDT used Google to conduct the following research relating to SOE 1, which identified SOE 1 as being under the direct control of the PRC State Council:

- Searched "Chinese security companies"
- Searched "Chinese cybersecurity companies"
- Searched "Chinese smart card security"
- Visited: "China Security Company Directory|Security Companies in China"
- Visited a webpage containing an article about SOE 1 which stated: "Chinese e-government and smart card firm [SOE 1], whose parent company is under the direct control of China's cabinet, the State Council, has been awarded contracts to process Hong Kong people's ID card and other data as they cross the border into mainland China."
- Searched for the name of SOE 1
- Visited the home webpage for SOE 1.
- Searched for "sipr acronym"

Shortly thereafter, SCHMIDT sent the following email[6] to a public email account associated with SOE 1:

> Hello, I am a retired United States Army Intelligence Agent. I have a Secret Internet Protocol Routing PKI token that I would like to reverse engineer to give to the Chinese government. This type of card is what US intelligence agencies use to gain access to SIPR, the intelligence network with TOP SECRET documents and information. It is a very rare card to find outside

---

[5] Based on open source research, I know that SOE 1 is a subsidiary of the China Aerospace Science and Industry Corporation Limited, a PRC state-owned enterprise. SOE 1 has produced intelligence-gathering software tools that the Chinese government requires businesses to use to pay taxes. This software has been found to have numerous backdoors built into it that can be used in support of cyber-hacking activities by the Chinese government. To develop the software, SOE 1 collaborated with universities that are linked with the MSS. I have relied on open sources here for the same reasons described in footnote 3.

[6] Schmidt wrote this email in both Chinese characters and in English. The English portion is quoted here. The Chinese language portion of the email contains a very similar message.

> of the intelligence community, and if used properly, it can improve China's ability to access the SIPR network.
>
> If I give you card, can you look into the security algorithms that it uses for me? By the way, I'm sorry my Chinese is so bad. I don't know how to translate most of this terminology, and I appreciate your patience. Where can I turn in the card at? Thank you!!
>
> Best regards, Joey

3. SCHMIDT Prepares Additional Information to Transmit to PRC.

On March 29, 2020, Schmidt took photographs of several hand-drawn sketches. The photographs were recovered from SCHMIDT's Apple iCloud account. The sketches depict information known to SCHMIDT through his service in the Army, including: (a) a flow chart entitled, "Intelligence Report Flow"; (b) an organizational chart of the chain of command involving SCHMIDT's battalion at JBLM; and (c) an organizational chart for a "Drone PED Team Hierarchy." According to the Army, none of the information contained in these sketches is classified.

The next day, on March 30, 2020, SCHMIDT created a Word document entitled, "Open Source Intelligence Analysis." The document was recovered from SCHMIDT's Apple iCloud account. The document discussed and purported to demonstrate how open-source maps, such as Google Earth, can be used to identify the locations of U.S. Military facilities worldwide. In the document, SCHMIDT described this process as "an invaluable look in discovering adversary locations and activities." According to the Army, none of this information is classified.

On April 29, 2020, SCHMIDT created a Word document entitled, "An Analysis of U.S. Embassy Job Postings in China." The document was recovered from SCHMIDT's Apple iCloud account. The document purported to explain how one can "look at a job posting from the U.S. embassy [] to identify a potentially suspicious job, that could be related to espionage or spy handling." The document further explained how to confirm that a "suspicious posting [is] . . . affiliat[ed] with the intelligence community" and how

to "identify sources the person is working with." According to the Army, none of this information is classified.

On May 7, 2020, SCHMIDT used Gmail account 1 to send the following message to his sister:

> Hey Mary, there's something I need to tell you. The real reason I left America is because of a disagreement with American policy. I don't talk about it often, but I learned some really terrible things about the American government while I was working in the Army, and I no longer feel safe living in America or like I want to support the American government. I don't plan on going back any time, except maybe once to sell my house, and I plan on limiting my contact with people who live in America. So basically, I'll be going off the map for a long time. If you don't hear from me, it's because I don't trust the U.S. government, and I want to minimize my communication to U.S. numbers. I'll still communicate occasionally by email, but I just wanted to give you a heads up so you don't worry about me.

4. SCHMIDT Creates Two More Documents With Classified NDI.

On May 12, 2020, SCHMIDT created a 28-slide PowerPoint presentation entitled, "Use of Technology in Military Source Operations and Interrogations." SCHMIDT modified the presentation on May 13, 2020. The file was recovered from SCHMIDT's Apple iCloud account. The first slide of the presentation was entitled, "About Me." This slide lists SCHMIDT's military experience, intelligence experience, and training in Mandarin Chinese. The rest of the presentation discussed various intelligence topics.

The OCA has reviewed the document and determined that information contained therein is properly classified at the SECRET level. Additionally, the OCA identified numerous portions of the document that constitute national defense information.

On May 20, 2020, SCHMIDT took a photograph of a hand-drawn sketch entitled, "Mat V Computers." The photograph was recovered from SCHMIDT's Apple iCloud account. The sketch contained a diagram of connected computer hardware and servers. It also had handwritten notations including "Top Secret Network," "SIPR," and references

to a particular Army computer network. Another OCA[7] has reviewed the sketch and determined that information contained therein constitutes CONTROLLED UNCLASSIFIED information, meaning that its disclosure could cause damage to the national security of the United States. Specifically, this OCA has certified that "an unauthorized release of this document would have a serious adverse effect on organization operations, organization assets, and/or individuals."

5. SCHMIDT Attempts to Transmit Information to PRC SOE 2.

On July 8, 2020, SCHMIDT took a photograph of a hand-drawn map depicting an unknown area with a parking lot, buildings, trees, paths, and a "brick courtyard." In the courtyard, there is a drawing of a bench with the notation: "Bench for meeting site." The photograph was recovered from SCHMIDT's Apple iCloud account.

On July 21, 2020, SCHMIDT used Gmail account 2 to send an email to a PRC state-owned enterprise ("SOE 2").[8] Prior to sending the email, SCHMIDT used Google to conduct the following research relating to SOE 2, which indicates that SCHMIDT identified SOE 2 as being affiliated with the PRC Ministry of Science and Technology:

- Searched "Ministry of Science and Technology"
- Searched "Institutions Subordinate to Ministry of Science and Technology"
- Visited webpage "The Ministry of Human Resources and Social Security of the People's Republic of China shall be publicly announced by some of the institutions affiliated with the Ministry of Science and Technology"

---

[7] In December 2017, an OCA reviewed the sketch and determined the appropriate classification for this information was "UNCLASSIFIED//FOR OFFICIAL USE ONLY," and that its unauthorized release would have an adverse effect on operations, organization assets, and/or individuals. Subsequently, another OCA determined the correct classification marking for the sketch is "CONTROLLED UNCLASSIFIED" information for the same reasons. The later OCA was delegated OCA authority pursuant to Executive Order 13526 and the May 5, 2011, memorandum of the Deputy Secretary of Defense.

[8] Based on open source research, I know that SOE 2 was established with the approval of the Chinese government. SOE 2 is affiliated with the Ministry of Science and Technology and also operates under the State Development Planning Commission. The missions of SOE 2 include managing the day-to-day affairs and implementation of China's Agenda 21 and its Priority Program and conducting research in the area of sustainable development. I have relied on open sources here for the same reasons described in footnotes 3 and 5.

Shortly thereafter, SCHMIDT sent the following email to a public email account associated with SOE 2:

> Subject: Background of intelligence warrior in providing technological information to your company
>
> Hello,
>
> I am a veteran with the US military with assignments in intelligence. Hence, I'm quite familiar with many of the most advanced US intelligence technologies. I want to apply the knowledge to enhance the capability of your company and accelerate the development of your technologies. I am currently living in Hong Kong and looking for employment in China. I am in possession of Top Secret Clearance/Secret Compartmentalized Information from the US, as well as a PKI card of the Secret Internet Protocol Routing Network (a US Intelligence Community's Global Top-secret Network), which I need to pass on to your company. Please contact me if you would like to look back [sic] this information. My WeChat number is [].
>
> Joseph Schmidt
> Intelligence Officer

J. SCHMIDT's Continuing Efforts to Obtain Immigration Status in Hong Kong and the PRC.

Since his arrival in Hong Kong in early March 2020, SCHMIDT had been trying to obtain employment in China and a PRC work permit/visa so he could permanently relocate to China. However, due to a variety of factors, including China's policies in response to the COVID-19 pandemic, SCHMIDT was having trouble obtaining a PRC visa.

In July 2020, just two weeks prior to SCHMIDT's email to SOE 2, he was notified by Hong Kong immigration authorities that he had been "overstaying in Hong Kong" since June 12, 2020, and his application for an extension of a visitor status was "refused." Hong Kong immigration authorities ultimately issued a recognizance bond for SCHMIDT, allowing him to remain in Hong Kong while he worked out the details of his immigration status.

SCHMIDT finally received a work permit from the PRC on August 7, 2020.

On September 28, 2020, SCHMIDT used Gmail account 2 to send an email to Hong Kong immigration authorities. SCHMIDT requested the return of his passport and explained that he was in the process of working "with the Chinese visa office to begin preparations to leave" Hong Kong.

Since then, SCHMIDT has continued to pursue legal immigration status in Hong Kong while he waited to relocate to China.

Brandon Tower
Special Agent, Federal Bureau of Investigation

Signed and sworn to before me on the 4th day of October, 2023.

Sandra Holder
(Signature of Notary)

Sandra Holder
(Name of Notary)

My Commission Expires: December 28, 2025

Notary Public
State of Washington
SANDRA S HOLDER
LICENSE # 22006574
MY COMMISSION EXPIRES
DECEMBER 28, 2025