UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**1:24-cr-438**
	:	
ABOUZAR RAHMATI,	:	**Judge Loren AliKhan**
	:	
Defendant.	:	

GOVERNMENT'S SENTENCING MEMORANDUM

The United States of America, by and through undersigned counsel, respectfully submits this memorandum in aid of sentencing. Rahmati has pleaded guilty to acting as an agent of the Iranian government without prior notification to the Attorney General, in violation of 18 U.S.C. § 951, and to conspiracy to do so, in violation of 18 U.S.C. § 371. There is no applicable Guidelines provision, so the Court must impose a sentence guided solely by the statutory factors under 18 U.S.C. § 3553(a). In this case, Rahmati abused the trust that his adopted country placed in him to engage in a years-long sophisticated effort to infiltrate the U.S. government and obtain sensitive information about U.S. critical aviation infrastructure on behalf of the intelligence services of Iran. He was far from a reluctant participant in this scheme. Rather, as a former officer in Iran's Islamic Revolutionary Guard Corps ("IRGC") with a longstanding personal relationship to a senior Iranian intelligence official, Rahmati acted on his own initiative and contacted an Iranian intelligence official in 2017 and stood to obtain significant financial benefits from the Iranian government in exchange for his subterfuge on its behalf. While Rahmati ultimately accepted responsibility for his crimes, the severity and duration of his criminal conduct merits a significant sentence with a substantial period of incarceration. Accordingly, for the reasons set forth below in further detail, a

sentence of 60 months' incarceration and 36 months of supervised release is sufficient but not greater than necessary to serve the goals of sentencing.

I. FACTUAL BACKGROUND

A. Iran and Its Intelligence Services

In 1984, the U.S. Department of State designated Iran as a State Sponsor of Terrorism. Since then, Iran has actively engaged in and directed an array of violent and deadly acts against the United States and its citizens globally. As the President recently stated in describing U.S. policy toward Iran, "[s]ince its inception in 1979 as a revolutionary theocracy, the Government of the Islamic Republic of Iran has declared its hostility to the United States and its allies and partners" and "remains the world's leading state sponsor of terror [that] has aided Hezbollah, Hamas, the Houthis, the Taliban, al-Qa'ida, and other terrorist networks." National Security Presidential Memorandum/NSPM-2, Imposing Maximum Pressure on the Government of the Islamic Republic of Iran, Denying Iran All Paths to a Nuclear Weapon, and Countering Iran's Malign Influence (Feb. 4, 2025). Indeed, in 1995, the President declared a national emergency under the International Emergency Economic Powers Act, 50 U.S.C. § 1705, because "the actions and policies of the Government of Iran constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States." Exec. Order 12957 (Mar. 15, 1995), 60 Fed. Reg. 14615. That emergency declaration has been continued every year since 1995, with the President recently stating that:

> The actions and policies of the Government of Iran—including its proliferation and development of missiles and other asymmetric and conventional weapons capabilities, its network and campaign of regional aggression, its support for terrorist groups, and the malign activities of the Islamic Revolutionary Guard Corps and its surrogates—continue to pose an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.

Continuation of the National Emergency With Respect to Iran, 90 Fed. Reg. 11887 (Mar. 7, 2025).

Iran's intelligence services—principally the IRGC and the Ministry of Intelligence and Security ("MOIS")—have a long history of engaging in acts of terrorism and violence inside and outside of Iran. The IRGC is an Iranian military and counterintelligence organization under the authority of the Supreme Leader of Iran. The IRGC plays a key role in Iran's development of ballistic missiles and in Iran's support for international terrorism generally as well as its support for specific foreign terrorist organizations such as Hizbollah and other militant groups. On October 25, 2007, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") designated the IRGC as a Specially Designated National ("SDN") pursuant to Executive Order No. 13382 for its support of Iran's ballistic missile and nuclear programs. Also in 2007, OFAC designated the IRGC-QF (also known as the "Quds Force") as a Specially Designated Global Terrorist ("SDGT") under Executive Order No. 13224 for providing material support to the Taliban and other terrorist organizations. On October 13, 2017, OFAC further designated the IRGC as a SDGT pursuant to Executive Order No. 13224 for providing material support to the IRGC-QF. On or about April 15, 2019, the U.S. Department of State designated the IRGC as a Foreign Terrorist Organization under Section 219 of the Immigration and Nationality Act for the IRGC's direct involvement in terrorist plotting, support for terrorism, and hostage-taking.

MOIS is one of the most dangerous and aggressive intelligence services operating against the United States and its allies. It has been linked to cyberattacks,[1] assassination plots,[2] hostage-

[1] *See* U.S. Department of the Treasury, "Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities," September 9, 2022, https://home.treasury.gov/news/press-releases/jy0941.

taking,[3] and surveillance of dissidents worldwide.[4] By way of examples, in 2021, the U.S. Department of Justice indicted four Iranian intelligence operatives for plotting to kidnap a Brooklyn-based journalist and human rights activist critical of the Iranian regime.[5] In July 2022, MOIS-linked cyber actors conducted wiper-style attacks that disrupted Albanian government systems, forcing a suspension of public services and damaging critical infrastructure.[6] In 2007, senior MOIS officers orchestrated the abduction and long-term detention of former DEA and FBI agent Robert Levinson in Iran, then engaged in a years-long disinformation campaign to deflect blame from the Iranian regime.[7]

---

[2] *See* Combating Terrorism Center at West Point, "Trends in Iranian External Assassination, Surveillance, and Abduction Plots," February 2022, Volume 15, Issue 2, https://ctc.westpoint.edu/trends-in-iranian-external-assassination-surveillance-and-abduction-plots/.

[3] *See* U.S. Department of State, "Sanctioning Iranian Intelligence Officers Involved in the Probable Death of Robert Levinson," March 25, 2025, https://www.state.gov/sanctioning-iranian-intelligence-officers-involved-in-the-probable-death-of-robert-levinson/.

[4] *See* Combating Terrorism Center at West Point, "Trends in Iranian External Assassination, Surveillance, and Abduction Plots," February 2022, Volume 15, Issue 2, https://ctc.westpoint.edu/trends-in-iranian-external-assassination-surveillance-and-abduction-plots/.

[5] *See* U.S. Department of Justice, "Iranian Intelligence Officials Indicted for Kidnapping Plot," July 13, 2021, https://www.justice.gov/opa/pr/four-iranian-intelligence-officers-charged-conspiracy-kidnap-us-journalist; see also U.S. Department of State, Country Reports on Terrorism 2021 – Iran, https://www.state.gov/reports/country-reports-on-terrorism-2021/iran/.

[6] *See* U.S. Department of the Treasury, "Treasury Sanctions Iranian Ministry of Intelligence and Minister for Malign Cyber Activities," https://home.treasury.gov/news/press-releases/jy0941.

[7] *See* Rewards for Justice, "Hostage Taking of Robert Levinson," https://rewardsforjustice.net/rewards/disappearance-of-robert-a-levinson/.

OFAC designated MOIS as an SDN on February 16, 2012, under Executive Orders Nos. 13224, 13553, and 13572 for being responsible for or complicit in the commission of serious human rights abuses against the Iranian people and Syrian people and for its support to terrorist groups, including al Qaeda, al Qaeda in Iraq, Hizballah, and Hamas. According to OFAC, MOIS has played a key role in the Iranian regime's brutal human rights abuses against the Iranian people and MOIS agents have been responsible for beatings, sexual abuse, prolonged interrogations and coerced confessions of prisoners, particularly political prisoners. MOIS has employed mock executions and forms of sexual violence in its interrogations of prisoners, and its agents have arrested and detained members of the Baha'i religion without charges. MOIS's global reach and history of malign, violent activity underscore the seriousness of Rahmati's decision to communicate with and provide information to MOIS.

B. Rahmati's Outreach to Iranian Intelligence in 2017

Rahmati is a 42-year-old dual citizen of the United States and Iran. He immigrated to the United States in 2011, where he completed a Ph.D. in electrical engineering and began working in the energy sector. In August 2017, Rahmati initiated contact with Iranian officials by emailing a former university classmate, Javad Jahromi, to congratulate him on his new position within the Iranian government and to offer his services. Jahromi was known to have ties to Iranian intelligence[8]. Specifically, Jahromi occupied a managerial position in MOIS in or around 2002.

[8] Jahromi previously served in Iran's Ministry of Intelligence and later became Minister of Information and Communications Technology. In 2019, OFAC sanctioned Jahromi for his role in surveillance and internet censorship activities conducted by the Iranian regime. In the press release, the U.S. Treasury Department described Jahromi as "a former employee of Iran's notorious Ministry of Intelligence [who] has advanced the Iranian regime's policy of repressive internet censorship since he took office in mid-2017 and has also been involved in surveillance against opposition activists." Press Release, U.S. Department of the Treasury, "Treasury Sanctions Iran's

Of note, Rahmati was well-aware of Jahromi's connections with MOIS. Rahmati and Jahromi were university roommates, and Rahmati was aware Jahromi was working for Iranian Intelligence during the time they lived together. In his August 2017 email to Jahromi, Rahmati wrote that "I would love to serve for our country in any way," and "I will be very happy if I hear from you and get a chance for any collaboration in future." This was not a response to pressure, coercion, or intimidation. It was a voluntary offer of assistance.

C. Rahmati's Efforts on Behalf of Iranian Intelligence

For at least five years between 2017 and 2022, Rahmati acted in the United States on behalf of the Iranian government and its intelligence services. He met three times in person with Iranian officials in Iran: twice in December 2017 (approximately 4 months after his email to Jahromi) and again during a trip to Iran in 2022. In between 2017 and 2022, Rahmati exchanged numerous emails with individuals affiliated with MOIS using an agreed-upon cover story to avoid detection from law enforcement.

In his initial meetings and communications with MOIS officials, Rahmati was asked to provide information related to the U.S. solar energy industry. He agreed to do so and began communicating under a false cover story. He sent publicly available research and reports to MOIS officials, including one document he purchased online from an industry database. Rahmati also specifically sought out additional employment opportunities that would advance his work on behalf of MOIS. Notably, on January 24, 2019, shortly before he began working at U.S. Company

---

Minister of Information and Communications Technology," Nov. 22, 2019, https://home.treasury.gov/news/press-releases/sm836; see also Associated Press, "Iran Names New Minister With Intelligence Background," https://apnews.com/article/c7e7ac1e30684e5babfc65a0d5848fb9.

1 on a contract for the Federal Aviation Administration (FAA), Rahmati emailed an individual he knew to be an Iranian intelligence officer (Iranian Intelligence Officer 1) that he "was in the process of moving to and joining a new company" and that together they could "work more effectively if it is finalized."

Rahmati's email correspondence with the Iranian Intelligence Officer 1 directly correlates with him taking FAA information into his personal possession. Specifically, on December 24, 2019, Rahmati emailed Iranian Intelligence Officer 1 and stated he was hoping to visit Iran during the upcoming Nowruz holiday and "God willing [he'd] visit" him on that trip. Two days after he sent the email, on December 26, 2019, Rahmati created a folder on his personal external hard drive entitled "[U.S. Company 1]-12242019." In the folder Rahmati saved numerous files, to include hundreds of proprietary, technical FAA documents. On February 2, 2020, Rahmati received another email from Iranian Intelligence Officer 1 instructing Rahmati "not to forget our souvenir [or gift]," which Rahmati knew to be a coded reference to information. Two days after he received the email, on February 4, 2020, Rahmati created a folder on his personal external hard drive entitled "[U.S. Company 1]-02042020." In the folder Rahmati again saved numerous files, to include hundreds of proprietary, technical FAA documents. Rahmati later deleted his email correspondence with Iranian Intelligence Officer 1 to avoid detection.

On March 17, 2022, the day before he departed for Iran, Rahmati saved several hundred files to a thumb drive, including access-controlled data from the FAA's internal network, such as policy documents on electrical standards at National Airspace System (NAS) air traffic control facilities and a list of U.S. airports with GPS coordinates and FAA-internal site numbers. Rahmati then took the thumb drive with him to Iran. While there, he and his brother met with MOIS

officials, who stated that they were looking for smart and loyal people because Iran had lots of "enemies" and needed to fight against them by gaining knowledge. The MOIS officials specifically emphasized new ideas and technology. Rahmati later described that, in this meeting, he realized the MOIS officials "need a spy" and that they "need us to do [a] bad thing." As compensation for his services, the MOIS officials offered Rahmati and his brother financial incentives in exchange for information, including free or low-interest loans or grants to finance future commercial projects in Iran. At the end of the meeting, consistent with prior discussions, the MOIS officials warned Rahmati and his brother that they should not share the conversation with anyone.

On April 11, 2022, the day after his meeting with MOIS officials, Rahmati copied the contents of a file titled "Airport Lists" into a new file and provided some or all of the contents of the thumb drive to MOIS. Upon returning to the United States, Rahmati emailed his brother a file intended for MOIS that included the sensitive airport data. He later deleted the email and directed his brother to do the same.

D. Indictment and Procedural History

On September 26, 2024, Rahmati was indicted on one count of acting as an agent of the Iranian government without prior notification to the Attorney General, in violation of 18 U.S.C. § 951, and one count of conspiring to do so, in violation of 18 U.S.C. § 371. He was arrested the next day, on September 27, 2024, and had his initial appearance that day before Magistrate Judge Zia Faruqui. On April 16, 2025, Rahmati pled guilty to the charges in the Indictment without a plea agreement. The Court set sentencing for August 26, 2025.

II. SENTENCING FACTORS UNDER 18 U.S.C. § 3553(a)

A. Nature and Circumstances of the Offense

Rahmati's offense is grave and implicates significant national security concerns. By providing detailed technical information to individuals he knew to be Iranian intelligence officers, Rahmati placed sensitive U.S. interests at risk. Although the documents he sent were not classified, their possession by the Iranian intelligence apparatus threatened U.S. national security interests. The first tranche of information he provided to Iranian intelligence included data about the U.S. solar energy industry, which Iranian intelligence officers and government officials expressly told Rahmati was difficult to obtain because of U.S. sanctions. In the second tranche of information, Rahmati provided sensitive FAA information about U.S. airports, geographic coordinates, and operational data. This type of information, in the hands of a hostile foreign intelligence service, could serve as a foundation for intelligence targeting, economic sabotage, or reconnaissance for future disruptive operations. Indeed, an FAA analysis conducted in or around August 2025 found that, taken as a whole, the FAA data Rahmati provided to Iranian intelligence would allow a person to gain a "reasonable understanding of how the [National Airspace System] power and electrical architecture is configured." Such information is especially dangerous in the hands of the government of a country that has consistently demonstrated that it is capable of violent and destructive conduct targeting U.S. interests.

As is the case here, other courts have recognized that national security offenses can warrant significant punishment where the defendant's conduct posed a real threat to U.S. interests, even in the absence of disclosures of classified information. For example, in *United States v. Chung,* the defendant was sentenced to 16 years' imprisonment for passing thousands of pages of *unclassified*

materials to the PRC, including technical engineering data belonging to Boeing, and information on military and civilian aerospace systems, in violation of 18 U.S.C. § 951, as well as conspiracy to violate and substantive violations of trade secret theft. *United States v. Chung*, 659 F.3d 815, 818 (9th Cir. 2011).

The damage caused by Rahmati's actions cannot be undone. Once sensitive U.S. infrastructure data is transferred to a hostile intelligence service, it is permanently compromised. The government cannot retrieve or erase the information he delivered, nor can it be certain how or when it may be exploited. Because the data relates to fundamental elements of FAA infrastructure, including system architecture and air traffic control protocols, mitigation would require substantial reengineering efforts across multiple agencies, making such an undertaking all but impossible. The uncertainty caused by Rahmati's choice to assist Iranian intelligence creates enduring risks to U.S. aviation systems and national security. His cooperation came only after he was caught and by then, the harm was already done.

Rahmati's conviction under 18 U.S.C. § 371 further underscores the gravity of his conduct. Conspiracy liability reflects not only his own actions, but his agreement with others to violate § 951. Conspiracies pose increased dangers because they increase the likelihood that the criminal objective will be successfully carried out, and often enable participants to reinforce each other's criminal intentions. And Rahmati's actions, which were neither incidental nor unintentional, support this conclusion. Rahmati's coconspirators specifically advised him to engage in covert communications, and after receiving direct instructions from known intelligence operatives, Rahmati agreed to supply follow-up material.

Rahmati knew full well that Iranian intelligence would not use his information for benign purposes but rather to support their fight against Iran's enemies. Rahmati had extensive experience with and knowledge of Iran's intelligence services. He grew up in Iran, lived with a university roommate who worked in Iranian intelligence, completed military training with the IRGC, and served in the IRGC as an officer. Indeed, Rahmati acknowledged later that, in his meetings with Iranian intelligence officers, he realized they needed "a spy" to do a "bad thing."

Overall, Rahmati's conduct showed a brazen willingness to cooperate with a foreign adversary at the expense of U.S. national security. In his own words, he later told FBI agents that he knew these individuals were not "good guys" and that they "wanted [him] to do bad things." He admitted that the reference to a "souvenir" or "gift" in follow-up emails from Iranian officials was understood to mean information, confirming that he recognized his role in carrying out their bidding, as well as the illicit nature of the relationship. The seriousness of this breach is not undone merely because the information Rahmati passed was not classified. There are other criminal statutes, and associated penalties, that prohibit passing classified information and national defense information. What matters here is the identity of Rahmati's co-conspirators, the agents on whose behalf he was acting, and the recipients and the context of his disclosures; all of which are facts that weigh heavily in favor of a substantial term of imprisonment for Rahmati.

B. History and Characteristics of the Offender

Rahmati's history and characteristics do not warrant a lenient sentence, when considering the factors under 18 U.S.C. § 3553(a)(1). He is a naturalized U.S. citizen who speaks fluent Farsi and English. He is a sophisticated individual with two master's degrees and a Ph.D. he acquired in his second language. As described in great detail in the Presentence Investigation Report ("PSR"),

Rahmati has a skillset that is in great demand in the current economy and he has been able to earn substantial legitimate income in the past. It is thus clear that Rahmati was capable of making a good living through non-criminal means. Despite that, it appears that one of his motives in offering himself to Iran's intelligence services was the offer of easy access to capital in Iran in the form of zero and/or low-interest loans or grants to support his commercial endeavors. But Rahmati could have easily financed those efforts within the law and he deliberately chose not to.

In addition, while the Government acknowledges the PSR writer's recommendation that "in light of his possible incarceration and money judgment obligation, it does not appear he has the ability to pay a fine," PSR (Dkt 21), at ¶ 86, the Government notes that Rahmati has held numerous six-figure jobs, including some such positions simultaneously, and has a net worth of $135,709, not including the $200,000+ increase in the estimated market value of his home. *See id.* ¶¶ 78-86.

This is also not Rahmati's first encounter with law enforcement. While there is no applicable Guideline range in this case, Rahmati's prior criminal history warrants one criminal history point, which would render him ineligible for the two-point offense level reduction for zero-point offenders under U.S.S.G. § 4C1.1(a)(1). As described in the PSR, in September 2017, a Virginia court (1) found facts sufficient to find Rahmati guilty on misdemeanor drug possession and distribution charges but deferred disposition until September 24, 2018, and (2) placed Rahmati on probation pursuant to Virginia Code § 18.2-251. PSR, at ¶ 48. Accordingly, Rahmati receives one criminal history point under U.S.S.G. §§ 4A1.2(f) and 4A1.1(c). *Id.* at ¶ 49.

C. The Need for the Sentence Imposed to Reflect the Seriousness of the Offense and Promote Respect for the Law

i. *Specific Deterrence*

Although Rahmati does not have a felony record, as noted above he has a prior Virginia state conviction from 2017 involving controlled substances and has repeatedly misrepresented material facts on government and employment forms, including his criminal history and his affiliation with the IRGC. This pattern of deception reflects a sustained willingness to subvert legal and security protocols to gain personal and professional advantages. Persistent deception, especially in national security-related contexts, justifies significant incarceration. His offense in this case continued that pattern, culminating in deliberate actions to aid a hostile foreign intelligence service. A sentence of 60 months is warranted to specifically deter him from reoffending and to reflect the severity of his calculated conduct.

ii. *General Deterrence*

A sentence of 60 months is necessary to send a clear and unequivocal message that acting on behalf of a hostile foreign intelligence service inside the United States, even without transferring classified material, will result in serious consequences. In today's complex threat environment, adversarial regimes like Iran continue to rely on diaspora-based operatives and sympathetic insiders to acquire sensitive information to help them gain strategic advantages over the United States. The deterrent effect of the sentence imposed in this case is not limited to those already working for foreign governments, but extends to others who may be approached or tempted to assist them, including those who, like Rahmati, do so on their own initiative.

This case also implicates a serious breach of public trust. Rahmati was not acting in a purely private capacity. While the U.S. Sentencing Guidelines do not apply to this particular offense,

the reasoning underlying U.S.S.G. § 3B1.3 (Abuse of Position of Trust or Use of Special Skill) is nonetheless instructive. That guideline reflects the Sentencing Commission's policy judgment that defendants who exploit positions of trust to facilitate or conceal criminal activity are more culpable than those who commit similar offenses without such access or discretion. According to the application notes, a position of trust "is characterized by professional or managerial discretion (i.e., substantial discretionary judgment that is ordinarily given considerable deference)" and the enhancement applies when the defendant "abused a position of public or private trust in a manner that significantly facilitated the commission or concealment of the offense." U.S.S.G. § 3B1.3, cmt. n.1. The rationale behind this policy is that such conduct not only enables wrongdoing that might otherwise be more difficult to accomplish or detect, but also undermines the integrity of institutions and relationships that rely on trust. *See, e.g.*, *United States v. Robinson*, 198 F.3d 973, 977 (D.C. Cir. 2000) (citation omitted) (noting factors indicating a defendant held a position of trust include "[t]he extent to which the position provides the freedom to commit a difficult-to-detect wrong, and whether an abuse could be simply or readily noticed"). A defendant who leverages a trusted position to serve a hostile foreign intelligence service, for example, has committed a particularly serious breach that heightens the need for punishment, deterrence, and protection of the public.

Rahmati was employed as a Senior Electrical Engineer on a government contract related to the National Airspace System with the FAA, giving him access to internal documents, non-public data and protected infrastructure details. He completed a background check to be eligible for his position. To have access to information about the National Airspace System, Rahmati was required to sign a "Confidential Information Non-Disclosure Agreement," in which he agreed to

not "disclos[e] to others or use for my own benefit or the future benefit of any individual, any trade secrets, confidential information, or proprietary/restricted data received" in connection with his work supporting the FAA's National Airspace System. His position placed him in a role of public responsibility and trust, which he knowingly abused. Government contractors are expected to safeguard sensitive information, not use it as currency in covert exchanges with hostile intelligence services. A meaningful custodial sentence is necessary to reaffirm the sanctity of the government's trust in its workforce and to deter others who might similarly exploit public roles for personal or ideological gain, and to the detriment of U.S. national security interests.

Rahmati was not a passive bystander; he proactively initiated contact, engaged in coded communications, exfiltrated sensitive FAA data, and took deliberate steps to conceal his activities. A significant custodial sentence is needed to dissuade others who might rationalize similar conduct on the basis that they are only sharing "unclassified" or "public" information. When that information is knowingly funneled to a foreign intelligence service, it becomes a national security threat. Moreover, the global reach and technological capacity of hostile regimes make insider contributions exponentially more dangerous. Even modest contributions can be used as targeting intelligence, reconnaissance data, or building blocks for broader strategic objectives.

In Rahmati's case, information about U.S. airports with GPS coordinates and FAA site numbers could help an adversary identify vulnerable or strategically important airfields for surveillance or disruption. Combined with internal FAA policy documents, that information could be used to exploit gaps in airport infrastructure security or assist in planning cyber or physical attacks. Similarly, information about the U.S. solar energy sector, which is a component of critical infrastructure, could aid in targeting energy production or distribution systems. These risks are

amplified when the recipient is a foreign intelligence agency like MOIS, which has demonstrated both the intent and capability to act on such information.

D. The Need to Avoid Unwarranted Sentencing Disparities

The proposed 60-month sentence aligns with the punishment imposed in numerous analogous cases, particularly when considering the breadth and seriousness of Rahmati's conduct. Unlike many other defendants charged under 18 U.S.C. § 951, Rahmati independently initiated contact with Iranian operatives, used covert communications techniques, and exfiltrated sensitive government data while working under a government contract through a position he obtained after completing a background check in which he lied about his connections to the Iranian government. His conduct spanned multiple years, involved coordination with family members, and culminated in the delivery of FAA infrastructure data to one of the world's most dangerous intelligence services.

In *United States v. Ji Chaoqun*, 107 F.4th 715 (7th Cir. 2024), Ji, a Chinese national, was sentenced to 96 months after conviction at trial for providing a Chinese intelligence officer with biographical information on individuals for potential recruitment and attempting to facilitate the acquisition of advanced aerospace and satellite technologies. Ji also joined the U.S. Army under false pretenses and offered to deliver photographs of Roosevelt-class aircraft carriers to the Chinese Ministry of State Security. Like Ji, Rahmati engaged in covert conduct on behalf of a hostile foreign intelligence service, seeking to provide that service with access to sensitive U.S. technology and infrastructure information. While Ji's efforts targeted military assets, Rahmati's exfiltration of internal FAA data relating to critical infrastructure represents a similarly grave

threat. Both cases involved strategic deception and national security risks, and the 60-month recommendation here is consistent with the magnitude of harm recognized in Ji's case.

In *United States v. Carlos Alvarez*, No. 05-cr-20943 (S.D. Fla.), Alvarez used his position as a professor at Florida International University to gather information and develop contacts of interest to the Cuban government, as well as to recruit Cuban-Americans as agents of Cuba. He pleaded guilty to conspiracy in violation of 18 U.S.C. § 371 and received the statutory maximum of 60 months. Although his conduct spanned decades and involved a concerted effort to serve a hostile foreign government, it primarily focused on community intelligence and influence operations. In contrast, Rahmati's actions directly targeted the technical backbone of U.S. civil aviation infrastructure. By exfiltrating non-public FAA documents, including GPS data and internal standards applicable to air traffic control systems, Rahmati provided Iran with sensitive information that could assist in identifying potential weaknesses or access points in U.S. aviation systems, thereby enabling future exploitation or disruption by hostile actors.

United States v. Ping Li, 24-cr-334 (M.D. Fla.), also involved the defendant's provision of unclassified technical data about U.S. critical infrastructure to a foreign adversary. In *Ping Li*, the defendant worked on behalf of a Chinese intelligence service for over a decade while employed at a major U.S. telecommunications company and an international information technology company. Among other information, Li provided sensitive cybersecurity information from his employer, which he knew he was not authorized to share. Li also provided information to the Chinese intelligence service about U.S. based Falun Gong and pro-democracy advocates. The defendant received a sentence of 48 months' imprisonment and a $250,000 fine.

In *United States v. Abouammo*, 2024 WL 4972564 (9th Cir. 2024), the defendant, a former Twitter employee and unregistered agent of the Saudi government, was initially sentenced to 42 months for accessing non-public user data and facilitating the targeting of dissidents at the direction of the Saudi government. On appeal, the Ninth Circuit vacated and remanded the sentence solely on a technical loss-calculation issue, but did not disturb the district court's findings as to the seriousness of the misconduct, which included covertly collecting and transmitting private communications. *Id.* at *2. Like Abouammo, Rahmati abused a position of trust (to protect the privacy of customers' personal information) within a U.S. company to deliver non-public information to a foreign government. But unlike Abouammo, Rahmati's work was actually on behalf of the U.S. government and he obtained his position after a formal background check. While Abouammo's conduct targeted individual privacy and speech, Rahmati's actions threatened (and continue to threaten) critical national infrastructure. A 60-month sentence for Rahmati remains consistent with the gravity recognized in Abouammo's case, especially given the potentially broader harm to public safety and national security.

While some § 951 cases have resulted in lower sentences, those often involved shorter durations of conduct, fewer overt acts, defendants who were passive recruits rather than self-initiating actors, and defendants who had not proactively sought a position with access to sensitive U.S. government data about critical infrastructure. For example, in *United States v. Doostdar*, 18-cr-255-PLF (D.D.C.), in January 2020, the defendant was sentenced to 38 months in prison for a 951 conspiracy and a substantive 951 violation (in addition to violations of IEEPA) because he worked for the Iranian government to surveil and collect identifying information about American citizens and U.S. nationals who were affiliated with an organization to which the Iranian

government is hostile (Mujahadeen-e-Khalq, or MEK). But Doostdar acted for only approximately one year and was not employed in a position of public trust, distinguishing the severity of his conduct from Rahmati's five years working for Iranian intelligence during which he sought out and obtained a position as a U.S. government contractor. The nature of the information Rahmati accessed, including non-public aviation and infrastructure data, also distinguishes this case from those where only general or open-source information was transmitted.

The Probation Office recommends a 20-month sentence anchored primarily in two ostensibly "similar cases" in this District where defendants were convicted under § 951, but overlooks significant factual differences and, more importantly, that each of the defendants in those two cases provided substantial assistance to the government and were sentenced after the government's requests for downward departures were granted under U.S.S.G. § 5K1.1. *See* Sentencing Recommendation, Dkt. 25 (Aug. 11, 2025). Also, neither occupied and abused a position of trust with direct access to sensitive government information.

First, in *United States v. Butina*, 18-cr-218-TSC (D.D.C.), the defendant was sentenced to 18 months in prison for conspiring to violate § 951 on behalf of Russian government officials to whom she provided information about U.S. persons working in politics and took steps to establish an unofficial line of communication connecting the two groups. Butina, a Russian national studying in the United States, was a private citizen who attended political events and organized "seemingly innocuous events" called "friendship dinners" to further the conspiracy. Gov't Memorandum in Aid of Sentencing, at 4-10, Dkt. 101 (Apr. 19, 2019). In that case, the government argued that an appropriate sentence for Butina would have been 24 months' imprisonment, but that an 18-month sentence was appropriate given the defendant's cooperation. *Id.* at 1.

Second, in *United States v. Yeo*, 20-cr-87 (D.D.C.), defendant Yeo was sentenced to 14 months in prison for violating § 951 by working for agents of the People's Republic of China to assist in the recruitment of U.S. persons with security clearances. Yeo, a Singaporean national, was a Ph.D. candidate who "used the internet and social media to find U.S. citizens who were likely to have access to valuable information, such as U.S. military and government employees with high-level security clearances." Gov't Memorandum in Aid of Sentencing, at 1-2, Dkt 14 (Oct. 1, 2020). At sentencing, the government requested a 16-month sentence and argued that, had Yeo not received cooperation credit, he should have received a 30-month sentence. *Id.* at 1. In contrast to defendants Butina and Yeo, who were foreign nationals acting as facilitators, Rahmati was a naturalized U.S. citizen and U.S. Government contractor who had passed a U.S. government background check and signed an explicit confidentiality agreement before proactively seeking out contact with Iranian intelligence. Accordingly, Rahmati is significantly more culpable than defendants Butina and Yeo and therefore merits a significantly more serious sentence.

Given these factors, a sentence of 60 months' imprisonment is not only appropriate but necessary to preserve proportionality with both more and less severe § 951 and espionage-related offenses. It reflects a serious breach of national security protocols and avoids sending a message that this form of covert cooperation with a foreign intelligence agency will be treated as routine or low-level misconduct.

III. CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court impose a sentence of 60 months' imprisonment, a fine, and 36 months of supervised release. Such a sentence will appropriately reflect the seriousness of the offense, the defendant's acceptance of responsibility, and the need to deter others while avoiding unwarranted disparities.

JEANINE FERRIS PIRRO
UNITED STATES ATTORNEY

*/s/ Christopher Tortorice*_____
Christopher Tortorice
TX Bar Number 24048912
Assistant United States Attorney
National Security Section
601 D Street, N.W.
Washington, D.C. 20530
Office: (202) 252-7155
Christopher.tortorice@usdoj.gov

JOHN A. EISENBERG
ASSISTANT ATTORNEY GENERAL

*/s/ Beau Barnes*_____
Beau D. Barnes
D.C. Bar Number 1024150
Alexander H. Wharton
D.C. Bar Number 156120
Trial Attorneys
Counterintelligence & Export Control Section
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue NW
Office: (202) 305-4679 (Barnes)
Office: (202) 514-4523 (Wharton)
Beaudre.Barnes@usdoj.gov
Alexander.Wharton@usdoj.gov