A SECURITY SPRINT: ASSESSING THE U.S. HOMELAND'S VULNERABILITIES TO CHINESE COMMUNIST PARTY AGGRESSION

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM, LAW ENFORCEMENT, AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MAY 23, 2023

Serial No. 118–14

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

54–073 PDF WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
NICK LALOTA, New York
MIKE EZELL, Mississippi
ANTHONY D'ESPOSITO, New York
LAUREL M. LEE, Florida
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
SHEILA JACKSON LEE, Texas
DONALD M. PAYNE, JR., New Jersey
ERIC SWALWELL, California
J. LUIS CORREA, California
TROY A. CARTER, Louisiana
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
GLENN IVEY, Maryland
DANIEL S. GOLDMAN, New York
ROBERT GARCIA, California
DELIA C. RAMIREZ, Illinois
ROBERT MENENDEZ, New Jersey
YVETTE D. CLARKE, New York
DINA TITUS, Nevada

STEPHEN SIAO, *Staff Director*
HOPE GOINS, *Minority Staff Director*
NATALIE NIXON, *Chief Clerk*
SEAN JONES, *Legislative Clerk*

SUBCOMMITTEE ON COUNTERTERRORISM, LAW ENFORCEMENT, AND INTELLIGENCE

AUGUST PFLUGER, Texas, *Chairman*

DAN BISHOP, North Carolina
TONY GONZALES, Texas
ANTHONY D'ESPOSITO, New York
ELIJAH CRANE, Arizona
MARK E. GREEN, MD, Tennessee *(ex officio)*

SETH MAGAZINER, Rhode Island, *Ranking Member*
J. LUIS CORREA, California
DANIEL S. GOLDMAN, New York
DINA TITUS, Nevada
BENNIE G. THOMPSON, Mississippi *(ex officio)*

MICHAEL KOREN, *Subcommittee Staff Director*
BRITTANY CARR, *Minority Subcommittee Staff Director*
ALICE HAYES, *Subcommittee Clerk*

CONTENTS

A SECURITY SPRINT: ASSESSING THE U.S. HOMELAND'S VULNERABILITIES TO CHINESE COMMUNIST PARTY AGGRESSION

Tuesday, May 23, 2023

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM,
LAW ENFORCEMENT, AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:23 p.m., in room 310, Cannon House Office Building, Hon. August Pfluger [Chairman of the subcommittee] presiding.

Present: Representatives Pfluger, Bishop, Crane, Magaziner, Correa, and Goldman.

Also present: Representatives Greene, and Jackson Lee.

Chairman PFLUGER. The Committee on Homeland Security, Subcommittee on Counterterrorism, Law Enforcement, and Intelligence will come to order.

This hearing is this subcommittee's second hearing focusing on the threats that the Chinese Communist Party poses to the U.S. homeland. The purpose of this hearing is to better understand how the Federal Government is responding to the numerous threats posed by the CCP that impact the U.S. homeland and to identify vulnerabilities that must be resolved in the Federal Government's approach to mitigating these threats.

I now recognize myself for an opening statement.

Well, good afternoon and welcome to the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence second hearing exploring the threats the Chinese Communist Party poses to the U.S. homeland. I would like to thank all of our witnesses for testifying today.

In March of this year, this subcommittee convened a hearing entitled "Confronting Threats Posed by the Chinese Communist Party to the U.S. Homeland". During that hearing, with the support of testimony from national security experts, Members learned about the many ways in which the CCP is deceiving and manipulating the United States to commit espionage in the homeland and to overturn a global rules-based order. We also discussed the CCP's aggressive strategy of military civil fusion and how it manifests as threats to our homeland. The subcommittee heard how the CCP is leveraging Confucius Institutes, programs the CCP claims are meant for language learning and cultural exchange, at U.S. universities and colleges to recruit American scientists and researchers to promote military civil fusion and suppress Chinese dissidents who are studying on American campuses. There is even evidence that the CCP is utilizing nontraditional intelligence collectors, such as Chinese academic researchers, to commit espionage in the U.S. homeland. We learned that the CCP has orchestrated the theft of anywhere between $225- and $600 billion in intellectual property annually, according to the Commission on the Theft of American Intellectual Property.

One of the witnesses, Bill Evanina, the former director of National Counterintelligence and Security Center, put this into perspective for us, explaining that that equates to nearly $4,000 to $6,000 per American family of four after taxes.

The subcommittee discussed the imminent threats the CCP poses to U.S cybersecurity and critical infrastructure, as well as its efforts to undermine American economic security. Furthermore, we heard how the CCP is refusing to cooperate in international counter-narcotics efforts, tacitly approving of the traffic of illicit fentanyl and related precursor chemicals needed to produce fentanyl from China to Mexico, fueling the American opioid crisis.

Today, we will revisit all of these pressing issues and more. The committee will hear from the Federal Bureau of Investigation, the FBI, the Department of Homeland Security regarding the role that each of those agencies play in mitigating CCP threats to the U.S. homeland.

During this committee's Worldwide Threats hearing in November 2022, FBI Director Wray stated that the greatest long-term threat to our Nation's ideas, innovation, and economic security is the foreign intelligence and economic espionage threat from China. The FBI has investigated many cases of CCP intrusions, including making critical arrests surrounding the illegal Chinese police station operating in Manhattan, New York, arrests the committee asked DHS and FBI about in an April 24 letter that remains unanswered at this point in time, and bringing those involved in the CCP's brazen cyber intrusions to justice.

At the same time, DHS has begun to prioritize the threats posed by the CCP by crafting an unrealistic 90-day sprint that focuses on defending critical infrastructure, disrupting the global fentanyl supply chain, bolstering screening and vetting for illicit travelers from the People's Republic of China, mitigating PRC malign economic influence, securing the Arctic Region, and mitigating counterintelligence threats posed by the PRC. While these efforts from both the FBI and DHS are necessary steps in the right direction, we must ensure countering the CCP as the highest priority for all entities involved in the homeland security enterprise.

Unlike the Biden administration, previous administrations, including the Trump administration, acknowledged the threat posed by the CCP at a time when it was not popular to do so. For example, in November 2018, the Department of Justice under the Trump administration launched the China Initiative to raise awareness and to identify and prosecute CCP trade secret theft and economic espionage and to protect American critical infrastructure and supply chains from CCP's malign influence.

In February 2022, the DOJ ended the China Initiative, in which they said was in favor of a broader approach to countering nation-state threats. However, it appears the decision was motivated by nothing more than identity politics, fueled by unfounded accusations that investigations under the initiative were excessive or racially biased. In fact, Assistant Attorney General Matthew Olsen admitted that he had not seen any indication of bias or prejudice in decision making by the Department of Justice in the related cases, and that actions "were driven by genuine national security concerns". Following the scuttling of the China Initiative, security experts warned that the motion emboldened China to increase its spying on the United States.

In a similar fashion, on January 12, 2021, in the final days of the Trump administration, DHS published the *DHS Strategic Action Plan to Counter the Threat Posed by the People's Republic of China*—again January 12, 2021. This comprehensive plan laid out four critical areas of focus for DHS to counter CCP malign efforts. They included border security and immigration, trade and economic security, cybersecurity and critical infrastructure, and maritime security. Following the transition to the Biden administration, DHS continued to work consistently on mitigating CCP threats from the component level. However, there was not a clear message regarding DHS headquarters priorities in the issue space until recently.

On April 20, 2023, Secretary Mayorkas issued the 90-day People's Republic of China Threats Sprint, displaying an encouraging shift in the Department's focus to threats emanating from the CCP. However, 90 days is not sufficient to undo the CCP's 73-year-long campaign to undermine the United States and our national security interest. China has been racing ahead for decades while we sprint to catch up, we must do more. Both DHS and the FBI need to form long-term strategic plans like the ones established under the Trump administration that can counter evolving threats from the CCP now and into the future.

I want to reiterate what I said when the subcommittee met for its first hearing this Congress. This conflict is not with the individual citizens of the PRC, this conflict is with the CCP, an authoritarian regime that commits genocide against its own people, censors free speech across the globe, and aims to end democracy as we know it. We must ensure we are enacting common-sense policy and strategy that can mitigate CCP aggression in the homeland. We need to rise above personal politics and confront the grave security threat posed by the CCP together.

I hope that during this discussion we can have a bipartisan hearing that talks about the threats, that gets rid of the distractions that I think have captured the politics over the last 2 years, and really focus on what is happening from the CCP as it affects our own homeland.

[The statement of Chairman Pfluger follows:]

STATEMENT OF CHAIRMAN AUGUST PFLUGER

MAY 23, 2023

Good morning, and welcome to the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence's second hearing exploring the threats the Chinese Communist Party (CCP) poses to the U.S. homeland. I would like to thank all our witnesses for testifying today.

In March of this year, this subcommittee convened a hearing entitled, "Confronting Threats Posed by the Chinese Communist Party to the U.S. Homeland."

During that hearing, with the support of testimony from national security experts, Members learned about the many ways in which the CCP is deceiving and manipulating the United States to commit espionage in the homeland and overturn global rules-based order. We also discussed the CCP's aggressive strategy of Military-Civil Fusion and how it manifests as threats to our homeland.

The subcommittee heard how the CCP is leveraging Confucius Institutes, programs the CCP claims are meant for language learning and cultural exchange, at U.S. universities and colleges to recruit American scientists and researchers to promote Military-Civil Fusion and suppress Chinese dissidents who are studying on American campuses.

There is even evidence that the CCP is utilizing "non-traditional" intelligence collectors, such as Chinese academic researchers, to commit espionage in the U.S. homeland.

We learned that the CCP has orchestrated the theft of anywhere from $225 to $600 billion in Intellectual Property annually according to the Commission on the Theft of American Intellectual Property.

One of the witnesses, Bill Evanina, the former director of the National Counterintelligence and Security Center, put this into perspective for us, explaining that equates to nearly $4,000 to $6,000 per American family of four after taxes.

The subcommittee discussed the imminent threats the CCP poses to U.S. cybersecurity and critical infrastructure as well as its efforts to undermine American economic security.

Furthermore, we heard how the CCP is refusing to cooperate in international counter-narcotics efforts, tacitly approving of the traffic of illicit fentanyl and related precursor chemicals needed to produce fentanyl from China to Mexico, fueling the American opioid crisis. Today, we will revisit all these pressing issues and more.

The committee will hear from the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) regarding the role they each play in mitigating CCP threats to the U.S. homeland.

During this committee's Worldwide Threats hearing in November 2022, FBI Director Wray stated that, "the greatest long-term threat to our Nation's ideas, innovation, and economic security is the foreign intelligence and economic espionage threat from China."

The FBI has investigated many cases of CCP intrusions, including making critical arrests surrounding the illegal Chinese police station operating in Manhattan, New York—arrests the committee asked DHS and FBI about in an April 24th letter that remains unanswered to this day—and bringing those involved in the CCP's brazen cyber intrusions to justice.

At the same time, DHS has begun to prioritize the threats posed by the CCP by crafting an unrealistic 90-day sprint that focuses on defending critical infrastructure, disrupting the global fentanyl supply chain, bolstering screening and vetting for illicit travelers from the People's Republic of China (PRC), mitigating PRC malign economic influence, securing the Arctic region, and mitigating counterintelligence threats posed by the PRC.

While these efforts from both the FBI and DHS are necessary steps in the right direction, we must ensure countering the CCP is the highest priority for all entities involved in homeland security.

Unlike the Biden administration, the Trump administration acknowledged the threat posed by the CCP at a time when it was not popular to do so.

For example, in November 2018, the Department of Justice (DOJ), under the Trump administration, launched the China Initiative to raise awareness, and to identify and prosecute CCP trade secret theft and economic espionage, and to protect American critical infrastructure and supply chains from CCP's malign influence.

In February 2022, the DOJ ended the China Initiative, in which they said was "in favor of a broader approach to countering nation-state threats."

However, it appears the decision was motivated by nothing more than identity politics fueled by unfounded accusations that the investigations under the initiative were excessive or racially biased. In fact, Assistant Attorney General Matthew Olsen admitted that he had not seen any indication of bias or prejudice in decision making by the Department of Justice in the related cases and that actions were "driven by genuine national security concerns."

Following the scuttling of the China Initiative, security experts warned that the action emboldened China to increase its spying on the United States.

In a similar fashion, on January 12, 2021, in the final days of the Trump administration, DHS published the "DHS Strategic Action Plan to Counter the Threat Posed by the People's Republic of China."

This comprehensive plan laid out four critical areas of focus for DHS to counter CCP malign efforts: border security and immigration; trade and economic security; cybersecurity and critical infrastructure; and maritime security.

Following the transition to the Biden administration, DHS continued to work consistently on mitigating CCP threats from the component level; however, there was not a clear message regarding DHS Headquarters' priorities in the issue space until recently.

On April 20, 2023, Secretary Mayorkas issued the "90-Day People's Republic of China Threats Sprint," displaying an encouraging shift in the Department's focus to threats emanating from the CCP. However, 90 days is not sufficient to undo the CCP's 73-year-long campaign to undermine the United States. China has been racing ahead for decades, while we "sprint" to catch up. We must do more.

Both DHS and the FBI need to form long-term strategic plans, like the ones established under the Trump administration, that can counter evolving threats from the CCP now and into the future.

I want to reiterate what I said when the subcommittee met for its first hearing this Congress: This conflict is not with individual citizens of the PRC—this conflict is with the CCP, an authoritarian regime that commits genocide against its own people, censors free speech across the globe, and aims to end democracy as we know it.

We must ensure we are enacting common-sense policy and strategy that can mitigate CCP aggression in the homeland.

We need to rise above personal politics and confront the grave security threat posed by the CCP together. I continue to look forward to bipartisan cooperation on this important topic, and I am eager to hear the testimony we will receive today.

Chairman PFLUGER. Now, I would like to recognize the Ranking Member, the gentleman from Rhode Island, Mr. Magaziner, for his opening statement.

Mr. MAGAZINER. Thank you, Chairman, for calling today's hearing. Thank you to our witnesses for appearing today.

It is indisputable that the Chinese Communist Party is the United States' greatest competitor on the world stage. It is also indisputable that the CCP is actively trying to undermine the economy and security of the United States.

As I noted in our hearing on the topic in March, it is important to be clear here that our adversary is the CCP as they have become more aggressive in trying to undermine U.S. interests, not the Chinese people or people of Chinese descent living and working in the United States. Anyone who targets individuals based on their race or national origin must be condemned and must be prosecuted appropriately.

Now, it is important to highlight that this competition we find ourselves in with the CCP touches on many areas, from defense to foreign policy to political ideology. But it is first and foremost an economic competition. That is why the CCP has aggressively pursued unfair economic practices, like currency devaluation, the use of weak and inhumane labor standards, and in particular, intellectual property theft, targeting both the U.S. Government agencies and United States companies in their effort to usurp our global economic leadership. The CCP routinely engages in espionage and cyber exploitation to steal American intellectual property, trade secrets, and defense information.

Each year, the CCP's economic espionage against American businesses costs between $225- and $600 billion, according to the FBI. In 2020, just one Chinese national stole intellectual property worth $1 billion dollars from his employer, a United States petroleum company. One billion dollars stolen by just one individual. Last year, a Boston-based cybersecurity firm found that a Chinese state actor had exfiltrated hundreds of gigabytes of IP in sensitive data from about 30 companies around the world. The estimated cost of that IP loss runs into the trillions. But even more alarming is that the intellectual property stolen by the CCP did not just include commercial product designs and trademarks for cheap, knockoff, counterfeit products, it included blueprints for fighter jets, helicopters, missiles, pharmaceuticals, and large-scale technologies.

These thefts of intellectual property and trade secrets threaten our national defense and also our economic advantage, hurting our companies and costing American jobs. The CCP does not plan to stop. In fact, they have become more assertive. The CCP's Made in China 2025, or MIC 2025 Initiative, lays out a broad set of industrial plans to boost China's economic fortunes by advancing its position in manufacturing and supply chains. Over the past decade, the CCP has also used foreign investments through its Belt and Road Initiative to develop China-centered and -controlled global infrastructure, transportation, trade, and production networks. But importantly, this initiative is more than just an economic challenge. It is expanding China's reach into hundreds of companies around the world and troublingly building digital networks that are giving the Chinese Communist Party access to troves of sensitive data from around the world which can be used against United States interests.

Now, I am pleased that under the leadership of President Biden and Secretary Mayorkas, DHS issued the Quadrennial Homeland Security Review, the first in 9 years, including a focus on threats related to the CCP. The 2023 review directly tackles the threat posed by the Chinese Communist Party to our competitiveness, democratic institutions, and homeland security. I am also pleased that the Biden administration has taken the threat of the CCP seriously with the passage of the CHIPS and Science Act, the establishment of the China House at the State Department, and the launch of the 90-day Sprint at DHS.

I look forward to hearing from today's witnesses about the broad threats to the United States from the Chinese Communist Party and in hearing how the DHS and FBI work with Federal partners across our country to protect American businesses and Government from CCP espionage.

Finally, I look forward to hearing how DHS is implementing the Biden administration's Quadrennial Homeland Security Review and receiving an update on the status of the DHS 90-day Sprint on China.

Thank you again to our witnesses for being here today, and I yield back.

[The statement of Ranking Member Magaziner follows:]

STATEMENT OF RANKING MEMBER SETH MAGAZINER

MAY 23, 2023

It is indisputable that the Chinese Communist Party is the United States' greatest competitor on the world stage. And it is indisputable that the CCP is actively trying to undermine the economy and security of the United States at home and abroad. As I reiterated in our last hearing on this topic in March, the threat emanating from China is from the CCP as they have become more aggressive in trying to undermine U.S. interests, not the Chinese people.

At the outset, I think it is important to highlight that this competition we find ourselves in touches upon many areas, from defense to foreign policy to political ideology, but is first and foremost an economic competition. That is why the CCP has aggressively pursued unfair economic practices like currency devaluation, the use of weak and inhumane labor standards, and in particular intellectual property theft, targeting both United States Government agencies and U.S. companies in its effort to usurp our global economic leadership.

The CCP routinely uses espionage and cyber exploitation to steal American intellectual property, trade secrets, and even defense information. Each year, China's economic espionage against American businesses costs between $225 and $600 billion, according to the FBI. In 2020, just one Chinese national stole intellectual property worth a billion dollars from his employer, a U.S. petroleum company.

Just. One. Person.

And last year, a Boston-based cybersecurity firm, Cyberreason, found that a Chinese state actor had exfiltrated hundreds of gigabytes of IP and sensitive data from about 30 companies around the world. The estimated cost of that IP loss runs into the trillions.

But even more alarming is that the intellectual property stolen by China did not just include commercial product designs and trademarks for cheap, knock-off counterfeit trinkets—it included blueprints for fighter jets, helicopters, missiles, pharmaceuticals, and large-scale technologies. These thefts of intellectual property and trade secrets threaten our national defense, and also reduces the economic advantage of the United States, hurting our companies and costing American jobs—and the CCP does not plan to stop.

The CCP has plans to become more assertive. Its "Made in China 2025," or MIC2025, initiative lays out a broad set of industrial plans that aim to boost China's competitiveness by advancing its position in manufacturing and supply chains. Over the past decade, the CCP has also used foreign investments through its Belt and Road Initiative to develop China-centered and—controlled global infrastructure, transportation, trade, and production networks. This unprecedented initiative is more than just an economic challenge to the United States—it is expanding China's reach into hundreds of countries around the world and reducing the costs of doing business with China.

Perhaps most troublingly, Belt and Road investments in building next-generation digital networks world-wide are giving the Chinese Communist Party access to troves of sensitive data from around the world, which it can use against the United States. How does the CCP plan to advance its position? By using every tool at its disposal—including spycraft—to leapfrog into emerging technologies. U.S. officials and cybersecurity analysts have described MIC2025 as a blueprint for the types of companies and industries China will target through espionage and hacking. FBI Director Christopher Wray put the CCP threat into perspective when he said, "[t]he greatest long-term threat to our Nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China."

I am pleased that under the leadership of President Biden and Secretary Mayorkas, DHS finally issued the Quadrennial Homeland Security Review—the first in 9 years. The 2023 review directly tackles the threat posed by the Chinese Communist Party to our competitiveness, democratic institutions, and homeland security. I am pleased that the Biden administration has taken the threat of the CCP seriously with the passage of the Chips and Science Act, the establishment of the China House at the State Department, and the 90-Day Sprint at DHS.

I look forward to hearing from today's witnesses about the broad threats the United States faces because of the Chinese Communist Party. I am particularly interested in hearing how DHS and the FBI work with Federal partners to protect American businesses and the Government from CCP espionage. Furthermore, I look forward to hearing how DHS is implementing the Biden administration's Quadrennial Homeland Security Review and receiving an update on the status of the DHS 90-Day Sprint on China.

Chairman PFLUGER. Thank you, Ranking Member Magaziner.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MAY 23, 2023

The U.S. Government must communicate to the American people the CCP's ambitions to expand and modernize its military, develop strategic technologies and digital infrastructure globally, and to exert its influence with the aim of undermining our democratic institutions. We should not demonize the Chinese people, but make no mistake—the CCP seeks to exploit American openness in order to steal economic secrets and undermine our security.

This is a strategic competition between U.S. democratic values and Chinese authoritarianism. It is a contest between U.S. economic opportunity and the CCP's dependence on market manipulation. It is a struggle between the First Amendment right of free speech and the state-controlled Chinese media. And it is a competition between the values of inclusiveness and civil liberties in America against the state-sponsored CCP surveillance that violates the human rights of the Chinese people. Democrats have worked hard to deter the Chinese Communist Party's security and economic aggression by out-competing China, investing in innovation and resilience, and promoting democratic values.

Under the Biden administration and Democratic leadership in Congress, the United States has made heavy investments in technology, industry, and supply chains to prevent the CCP from achieving its goal of undermining the U.S. economy and displacing America as the world's global leader.

Last year, Democrats passed—and President Biden signed into law—the CHIPS and Science Act, which invests $280 billion to increase domestic semiconductor production, strengthen U.S. industry, create jobs here at home, reduce inflation, and ensure the United States remains competitive vis-á-vis China on all fronts. Due to the seriousness of the CCP threat, this effort should have been bipartisan, but nearly 90 percent of House Republicans voted against the bill and therefore against standing up to China.

However, given today's hearing I am hopeful that we can work together to bridge the partisan gap and build on the CHIPS Act investments. We must unite against the CCP as it pursues its goal of global dominance. Together, Democrats and Republicans must invest in American competitiveness to counter expansive Chinese military ambitions, persistent cyber attacks, and threats to our global supply chain. I am certain we can come together on this issue, as just last week this committee united to pass bipartisan legislation to address cyber intelligence vulnerabilities hidden within Chinese drone technology. Today, we hope to continue to show bipartisan support for enhanced cyber security, economic stability, and counterintelligence efforts.

As I have stated before, as we deliberate on how best to strengthen the homeland against the Chinese Communist Party's actions, we must reject anti-Asian rhetoric and condemn violence against Chinese Americans. It is essential that we celebrate and support our Nation's diversity and not fall into any CCP-polarization traps as it advances China's economic and national security agendas. I thank today's witnesses for lending their expertise.

Chairman PFLUGER. Without objection, the gentlewoman from Georgia, Ms. Marjorie Taylor Greene, is permitted to sit on the dais and ask questions of the witnesses.

Without objection, the Chair may declare the committee in recess at any point in time.

I am pleased to have a distinguished panel of witnesses before us today on this very important topic, and I ask that the witnesses please rise and raise their right hands.

[Witnesses sworn.]

Chairman PFLUGER. Let the record reflect that the witnesses have answered in the affirmative.

I would like, now like to formally introduce our witnesses.

Ms. Jill Murphy is the deputy assistant director of the Federal Bureau of Investigations Counterintelligence Division. Ms. Murphy began her career with the FBI in 2002. Her initial work with the FBI included investigations of Asian organized crime in America and worked with the Joint Terrorism Task Force to focus on the fight against al-Qaeda and its affiliates. In 2010, Ms. Murphy transitioned to the China Counterintelligence Division at FBI headquarters. From 2014 to 2016, she served on the National Security Council as director of counterintelligence, coordinating counterintelligence policy and operations. Most recently, Ms. Murphy worked as the CIA's chief of counterespionage. Welcome.

Next. Mr. Iranga Kahangama is the assistant secretary for Cyber Infrastructure Risk and Resilience at the Department of Homeland Security. Previously, he served at the White House and the National Security Council as director for Cyber Incident Response. In that role, he oversaw the Federal Government's response to a wide range of malicious cyber activity, including the Russia-attributed Solar Winds incident, China's exploitation of Microsoft Exchange servers, and ransomware attacks on the Colonial pipeline. Prior to the NSC, he served as senior policy advisor at the FBI, working on an array of cyber, internet, and technology policy issues. Welcome.

Finally, Mr. Tyrone Durham currently serves as the acting director of the Nation State Threat Center in the Department of Homeland Security's Office of Intelligence and Analysis. In this role, Mr. Durham oversees the Center's efforts to identify and assess foreign adversarial threats to the U.S. homeland, primarily in the areas of counterintelligence, trade, and supply chain, as well as intellectual property. Before this role, Mr. Durham was the senior advisor for cyber and senior subject-matter expert at DHS Cyber Mission Center. Prior to joining DHS, Mr. Durham served more than 2 decades in intelligence with the FBI at its New York Field Office and Headquarters' criminal, counterterrorism, counterintelligence, and cyber programs. Welcome and thank you. Mr. Durham concluded his career at the FBI as unit chief in the FBI's Counterintelligence Division, identifying and assessing threats from the People's Republic of China.

Welcome.

Mr. MAGAZINER. Mr. Chairman, before we proceed, I ask unanimous consent that Ms. Jackson Lee be permitted to sit on the subcommittee and question the witnesses.

Chairman PFLUGER. So ordered.

I would like to thank all the witnesses for being here today.

I now recognize Ms. Jill Murphy, if you will, Ms. Murphy. For all the witnesses, I know you have written statements. Thank you for those. Please do summarize the statements and stick to 5 minutes. Thank you.

STATEMENT OF JILL M. MURPHY, DEPUTY ASSISTANT DIRECTOR OF COUNTERINTELLIGENCE, FEDERAL BUREAU OF INVESTIGATION

Ms. MURPHY. Good afternoon. Chairman Pfluger, Ranking Member Magaziner, and Members of the committee. Thank you for the opportunity to discuss the FBI's counterintelligence work against the People's Republic of China and the ways the FBI works with members of the U.S. intelligence community, public and private entities, the American people, to protect the U.S. homeland from the Communist Government of China.

Our Nation faces a wider-than-ever array of challenging threats. We see nations such as China, Russia, and Iran becoming more aggressive and more capable in their nefarious activity than ever before. These nations seek to undermine our core democratic values, our economic and scientific institutions. They employ a growing range of tactics to advance their interests and to harm the United

States. Defending American institutions and values against these threats is a national security imperative and a priority for the FBI.

With that, the greatest long-term threat to our Nation's ideas, innovation, and economic security is the foreign intelligence and economic espionage threat from China. It's a threat to our economic security and by extension, our national security. The China government aspires to equal or surpass the United States as a global superpower and influence the world with a value system shaped by undemocratic authoritarian ideas. The pursuit of these goals is often with little regard for international norms or laws. When it comes to economic espionage, the Chinese government uses every means at its disposal against us blending cyber, human diplomacy, corporate transactions, pressure on U.S. companies operating in China to achieve its strategic goals to steal our companies' innovations.

These efforts are consistent with China's express goal to become a national power, modernizing its military, and creating innovative, driven economic growth. To pursue this goal, China not only uses human intelligence officers, co-optees, nontraditional collectors, as you mentioned, sir, corporate, corrupt corporate insiders, but also sophisticated cyber intrusions, pressure on U.S. companies, shell game corporate transactions, joint venture partnerships that are anything but a true partnership. There's nothing traditional about the scale of their theft. It's unprecedented in the history of the FBI. American workers and companies are facing greater, more complex danger than they've ever dealt with before. Stolen innovation means stolen jobs, stolen opportunities for work, and stolen national power and stolen leadership in these industries.

The Chinese government targets cutting-edge research and innovation at our universities as well as in private industry. This is no secret. The Chinese government publicizes the key technologies they tend to target and acquire. The Made in China 25 Plan, for example, lists ten broad areas spanning industries like robotics, green energy production, agricultural equipment, aerospace, and biopharma. The governor of China's 14th 5-year plan targets things like AI, quantum, semiconductors, brain science, smart manufacturing, robotics. The government of China is willing to lie, cheat, and steal their way into unfairly dominating entire tech sectors, putting competing U.S. companies out of business.

They aren't just interested in technology. The Chinese government is interested in cost and pricing information, internal strategy documents, bulk, PII, anything that can give them a competitive advantage. The Chinese government is fighting a generational fight to surpass our country in economic and technological leadership, but not through legitimate innovation, not through fair and lawful competition, and not by giving their citizens the freedom of thought and speech and creativity that we treasure here in the United States.

The Chinese government makes American ventures operating in China establish Chinese community party cells within their companies. The companies operating in China are susceptible to the laws and regulations of the Chinese government, which enables the stealing of U.S. information and technology. The American people and businesses should know if you are an owner, a security official, an employee of a U.S. business, no matter the size, and you create cutting-edge technology and the semiconductor, quantum computing, AI, machine learning, new energy, biotech, aerospace, robotics, the list goes on, or you create a widget or a software component that contributes to the manufacturing process of one of these technologies, your company's intellectual property and employees are targets of sophisticated nation-state actors like China, both here in the United States and abroad.

To be clear, this is not about the Chinese people as a whole or Chinese Americans, this is about a threat emanating from the Chinese Communist Party, which controls the Chinese government.

Finally, the strength of any organization is its people. The threats we face as a Nation have never been greater or more diverse, and the expectations on the FBI have never been higher. Our fellow citizens look to the FBI to protect the United States from all threats, and the people of the FBI continue to meet and exceed those expectations every day. I want to thank them for their dedicated service.

Thank you for the opportunity to testify today, and I look forward to the questions.

[The prepared statement of Ms. Murphy follows:]

PREPARED STATEMENT OF JILL M. MURPHY

MAY 23, 2023

Good morning, Chairman Pfluger, Ranking Member Magaziner, and Members of the committee. Today, I am honored to be here, representing the people of the Federal Bureau of Investigation ("FBI"), who tackle some of the most complex and most grave threats we face every day with perseverance, professionalism, and integrity. Sometimes at the greatest of costs. I am extremely proud of their service and commitment to the FBI's mission and to ensuring the safety and security of communities throughout our Nation. On their behalf, I would like to express my appreciation for the support you have given them in the past and ask for your continued support in the future.

FOREIGN INTELLIGENCE THREATS

Top Threats

We see nations such as China, Russia, and Iran becoming more aggressive and more capable in their nefarious activity than ever before. These nations seek to undermine our core democratic, economic, and scientific institutions. They employ a growing range of tactics to advance their interests and to harm the United States. Defending American institutions and values against these threats is a national security imperative and a priority for the FBI.

With that, the greatest long-term threat to our Nation's ideas, innovation, and economic security is the foreign intelligence and economic espionage threat from China. It's a threat to our economic security—and by extension—to our national security. The Chinese government aspires to equal or surpass the United States as a global superpower and influence the world with a value system shaped by undemocratic authoritarian ideals. The pursuit of these goals is often with little regard for international norms and laws.

When it comes to economic espionage, the PRC uses every means at its disposal against us, blending cyber, human intelligence, diplomacy, corporate transactions, and pressure on U.S. companies operating in China, to achieve its strategic goals to steal our companies' innovations. These efforts are consistent with China's expressed goal to become a national power, modernizing its military and creating innovative-driven economic growth.

To pursue this goal, China uses not only human intelligence officers, co-optees, and corrupt corporate insiders, but also sophisticated cyber intrusions, pressure on U.S. companies in China, shell-game corporate transactions, and joint-venture "partnerships" that are anything but a true partnership. There's also nothing traditional about the scale of their theft—it's unprecedented in the history of the FBI. American workers and companies are facing a greater, more complex danger than they've ever dealt with before. Stolen innovation means stolen jobs, stolen opportunities for American workers, stolen national power, and stolen leadership in the industries."

National Counterintelligence Task Force ("NCITF")

As the lead U.S. counterintelligence agency, the FBI is responsible for detecting and lawfully countering the actions of foreign intelligence services and organizations as they seek to adversely affect U.S. national interests. The FBI recognized the need to coordinate similar efforts across all agencies, and therefore established the National Counterintelligence Task Force ("NCITF") to create a whole-of-Government approach to counterintelligence. The FBI established the national-level task force, or NCITF, in the National Capital Region to coordinate, facilitate, and focus these multi-agency counterintelligence operations, and to programmatically support local Counterintelligence Task Force ("CITF") operations. Combining the authorities and operational capabilities of the U.S. intelligence community; Federal, State, and local law enforcement; and local CITFs in each FBI field office, the NCITF coordinates and leads whole-of-Government efforts to defeat hostile intelligence activities targeting the United States.

Transnational Repression

In recent years, we have seen a rise in efforts by authoritarian regimes to interfere with freedom of expression and punish dissidents abroad. These acts of repression cross national borders, often reaching into the United States. It's important to note countries like China, Russia, and Iran, stalk, intimidate, and harass certain people in the United States. This is called transnational repression.

Transnational repression can occur in different forms, from threats against family members, to assaults and attempted kidnapping. Governments use transnational repression tactics to silence the voices of their citizens, U.S. residents, or non-citizens connected to the home country. This sort of repressive behavior is antithetical to our values as Americans. People from all over the world are drawn to the United States by the promise of living in a free and open society—one that adheres to the rule of law. To ensure that this promise remains a reality, we must continue to use all of our tools to block authoritarian regimes that seek to extend their tactics of repression beyond their shores.

Foreign Malign Influence

Our Nation is confronting multifaceted foreign threats seeking to both influence our national policies and public opinion, and cause harm to our national dialog and debate. The FBI and our interagency partners remain concerned about, and focused on, foreign malign influence operations—which include subversive, undeclared, coercive, or criminal actions used by foreign governments in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic institutions and processes.

Foreign malign influence is not a new problem, but the interconnectedness of the modern world, combined with the anonymity of the internet, have changed the nature of the threat and how the FBI and its partners must address it. Foreign malign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries—hoping to reach a wide swath of Americans covertly from outside the United States—to amplify existing stories on social media in an attempt to discredit U.S. individuals and institutions.

The FBI is the lead Federal agency responsible for investigating foreign malign influence threats. Several years ago, we established the Foreign Influence Task Force ("FITF") to identify and counteract foreign malign influence operations targeting the United States. The FITF is led by the Counterintelligence Division and comprises agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions. It is specifically charged with identifying and combating foreign malign influence operations targeting democratic institutions and values inside the United States. In all instances, the FITF strives to protect democratic institutions, develop a common operating picture, raise adversaries' costs, and reduce their overall asymmetric advantage.

The FITF brings the FBI's national security and traditional criminal investigative expertise under one umbrella to prevent foreign influence in our elections. This better enables us to frame the threat, to identify connections across programs, to aggressively investigate as appropriate, and—importantly—to be more agile. Coordinating closely with our partners and leveraging relationships we have developed in the technology sector, we had several instances where we were able to quickly relay threat indicators that those companies used to take swift action, blocking budding abuse of their platforms.

Following the 2018 midterm elections, we reviewed the threat and the effectiveness of our coordination and outreach. As a result of this review, we further expanded the scope of the FITF. Previously, our efforts to combat malign foreign influence focused solely on the threat posed by Russia. Utilizing lessons learned since 2018, the FITF widened its aperture to confront malign foreign operations of the PRC, Iran, and other global adversaries. To address this expanding focus and wider set of adversaries and influence efforts, we have also added resources to maintain permanent "surge" capability on election and foreign influence threats.

In addition, the domestic counterintelligence environment is more complex than ever. This Nation faces a persistent and pervasive national security threat from foreign adversaries, particularly Russia and China, conducting sophisticated intelligence operations using coercion, subversion, malign influence, disinformation, cyber and economic espionage, traditional spying and non-traditional human intelligence collection. Together, they pose a continuous threat to U.S. national security and its economy by targeting strategic technologies, industries, sectors, and critical infrastructures. Historically, these asymmetric national security threats involved foreign intelligence service officers seeking U.S. Government and U.S. intelligence community information. The FBI has observed foreign adversaries employing a wide range of nontraditional collection techniques, including the use of human collectors not affiliated with intelligence services, foreign investment in critical U.S. sectors, and infiltration of U.S. supply chains. The FBI continues to adjust its CI priorities and posture to address the evolving and multifaceted threat.

CONCLUSION

Finally, the strength of any organization is its people. The threats we face as a Nation have never been greater or more diverse and the expectations placed on the FBI have never been higher. Our fellow citizens look to the FBI to protect the United States from all threats, and the people of the FBI continue to meet and exceed those expectations, every day. I want to thank them for their dedicated service.

Chairman Pfluger, Ranking Member Magaziner, and Members of the subcommittee, thank you for the opportunity to testify today. I am happy to answer any questions you might have.

Chairman PFLUGER. Thank you, Ms. Murphy.

The Chair now recognizes for his opening statement, Mr. Kahangama.

STATEMENT OF IRANGA KAHANGAMA, ASSISTANT SECRETARY FOR CYBER, INFRASTRUCTURE, RISK AND RESILIENCE, OFFICE OF STRATEGY, POLICY, AND PLANS, DEPARTMENT OF HOMELAND SECURITY

Mr. KAHANGAMA. Thank you, Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the subcommittee. Thank you for inviting me here today to testify about threats and vulnerabilities to the homeland posed by the People's Republic of China. The Department of Homeland Security shares your concerns and looks forward to working with you to address these pressing challenges. The Department is on the front lines of countering these threats and takes this mission seriously and with the highest attention.

Today, I will talk to you about the multi-pronged approach this Department is taking to address our vulnerabilities in the homeland and perhaps even more importantly, how we are making our country more resilient.

As the administration's National Security Strategy states and the National Cybersecurity Strategy reiterates, the PRC is our only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do so. In cyber space our interconnectedness and the technology that enables it exposes us to a dynamic and evolving threat that Beijing actively exploits, one that is not contained by borders or centralized actors. The PRC also routinely engages in transnational repression, using illegal tactics to surveil, threaten, and harass targets both in person and digitally around the globe. Such attempts circumvent established means of law enforcement cooperation and directly violate our sovereignty. It highlights that the PRC often lacks a legal basis for pursuing such targets.

On economic security, the PRC abuses legal avenues such as foreign investment and international trade, to exploit our open rules-based system in pursuit of a zero-sum approach to global competition. This approach seeks to undermine American leadership, security, prosperity, and competitiveness.

DHS is unwavering in its commitment to countering the PRC's whole-of-government threat by providing a whole-of—whole-of-homeland response, whether in cyber space, in defense of our critical infrastructure, our economic security, or preventing the assault on democratic values and freedoms.

As Secretary Mayorkas made clear when recently directing DHS to engage in a 90-day sprint on the PRC threat, Beijing poses an especially grave threat to the homeland, one that touches all of our Department's missions. We must ensure that we are poised to guard against this threat not only today, but well into the future. We defend against threats to cyber space and our critical infrastructure through the Cybersecurity and Infrastructure Security Agency. CISA works to shine a light on the tactics, techniques, and procedures the PRC uses against our vulnerable systems, frequently in concert with inter-agency and international partners.

The private sector, who own and operate most of the critical infrastructure in this country, are also essential partners in our collective efforts against PRC threats. CISA established the Joint Cyber Defense Collaborative to bring together State, local, Tribal, and territorial partners with private-sector partners to conduct real-time information sharing.

Our law enforcement components—Secret Service, Homeland Security Investigations, and Customs and Border Protection—work with partners to counter PRC intellectual property theft, goods made by forced labor, and instances of transnational repression. The Coast Guard is actively ensuring the security of our ports and maritime sector, including from equipment made by PRC state-owned enterprises. The Transportation Security Administration is also on the front lines of securing our various transportation nodes, be they surface or air.

In addition to addressing these very real homeland security concerns, the Department also recognizes that these are threats posed by the PRC government and not the people of China or of Chinese origin. The Department condemns all forms of anti-Asian hate and discrimination, and actively works with these communities to ensure their protection. This is particularly relevant as I sit here before you today during Asian American, Native Hawaiian, and Pacific Islander Heritage Month.

Chairman Pfluger, by holding this hearing today, it is clear to this subcommittee that the subcommittee takes seriously the threat to the homeland posed by the PRC. DHS knows that we are not alone in this challenge, and we thank you for your commitment.

I thank you again for the opportunity to testify today and look forward to taking your questions.

Thank you.

[The joint prepared statement of Mr. Kahangama and Mr. Durham follows:]

JOINT PREPARED STATEMENT OF IRANGA KAHANGAMA AND TYRONE DURHAM

MAY 23, 2023

Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the subcommittee, thank you for the opportunity to discuss critical work the Department of Homeland Security (DHS) is doing to combat the wide and multifaceted threat posed by the People's Republic of China (PRC). As the administration's National Security Strategy states, and the National Cybersecurity Strategy reiterates, the PRC is our only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it. Consistent with this strategy and its pillar to invest in our strengths at home, DHS is leading efforts domestically to counter PRC threats to the homeland. We do this day in and day out with international, interagency, and private-sector partners.

We must match our adversaries' determination through a whole-of-Government response, with DHS playing a leading role on the front lines of that defense every day. Whether it is our work securing systems in cyber space, investigating acts of transnational repression and transnational cyber crime, ensuring goods made from forced labor are not entering the country, or scrutinizing investments made in our companies and critical infrastructure, we take this mission seriously and with the highest attention.

INTELLIGENCE ASSESSMENT AND RESPONSIBILITIES

The PRC operates globally, using all instruments of national power to target the United States, and has a broad range of sophisticated intelligence capabilities. It continues to employ both overt and clandestine methods to undercut U.S. national security and economic security interests, such as stealing advanced and sensitive technologies using traditional and non-traditional collectors, amplifying narratives that sow doubt in U.S. institutions, and messaging against U.S. politicians it deems hostile. It also uses sister-city agreements, and other seemingly benign economic and cultural outreach to foster exploitable relationships, exert influence, and strengthen its foothold in the homeland. Recently, the PRC set up so-called "police stations" on U.S. soil to intimidate dissidents and other perceived adversaries.

Our homeland faces an array of complex threats from the PRC. In cyber space, our interconnectedness and the technology that enables it exposes us to a dynamic and evolving threat environment that Beijing actively exploits, one that is not contained by borders or limited to centralized actors. The PRC also routinely bypasses law enforcement cooperation and extradition procedures and instead engages in transnational repression by using illegal tactics to surveil, threaten, and harass targets, both in person and digitally, around the globe. These activities directly violate the sovereignty of the host country and highlight that the PRC often lacks a legal basis for pursuing such targets. On economic security, the PRC abuses foreign investment and international trade by using illicit means to exploit this rules-based multilateral trading system in pursuit of a zero-sum approach to global competition that seeks to undermine American global leadership, national security, prosperity, and competitiveness.

DHS's Office of Intelligence and Analysis (I&A) is increasing intelligence collection and reporting on a wide range of potential threats and issues that the PRC poses to the United States, including threats within cybersecurity, counterintelligence, and transnational repression in the United States. This intelligence assists our partners in recognizing this activity, contributing to increased awareness of these threats by stakeholders who may be best positioned to identify and mitigate the activities first-hand. I&A also produces strategic intelligence on threats to U.S. economic competitiveness, including intellectual property theft, supply chain threats, potentially harmful foreign investments, and illicit trade.

CYBERSECURITY

The PRC poses a highly advanced cyber threat to the homeland. It continues to leverage increasingly sophisticated, large-scale cyber espionage operations against the U.S. Government and a range of industries, organizations, and dissidents in the United States. The PRC uses cyber means to illicitly obtain U.S. intellectual property, personally identifiable information, and export-controlled information. PRC-backed malicious hackers, including those within the People's Liberation Army and the Ministry of State Security, are among the most active groups targeting governments and critical infrastructure, and the most active group targeting businesses around the globe. One PRC malicious hacking group, known as Advanced Persistent Threat 41, or APT41, has stolen intellectual property from at least 30 multinational companies in the pharmaceutical, energy, and manufacturing sectors, resulting in hundreds of billions of dollars of lost revenue. In addition to numerous state-affiliated APT groups, the PRC leverages a wide-ranging framework of laws to require all organizations operating in China—including joint ventures with foreign companies—to aid the regime in national intelligence efforts, with the obstruction of such efforts punishable under criminal law. This includes mandatory disclosure laws to compel organizations to report zero-day vulnerabilities, potentially leading to their exploitation before patching, and may punish companies when they do not comply.

To meet this challenge, the DHS Cybersecurity and Infrastructure Security Agency (CISA) publishes a variety of products to support organizations. Advisories, Alerts, and Malware Analysis Reports—frequently released in conjunction with other agencies and increasingly other countries—provide technical details on tactics, techniques, and procedures used by PRC state-sponsored cyber actors. For example, in October 2022, CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) released a joint-seal advisory outlining the top Common Vulnerabilities and Exposures used by the PRC since 2020. To mitigate against these types of threats, in October 2022, the Department released the Cybersecurity Performance Goals (CPGs), voluntary practices that outline the highest-priority baseline measures businesses and critical infrastructure owners of all sizes can take to protect themselves from malicious state actors and improve their overall defensive posture.

In the wake of PRC-affiliated APT Hafnium conducting broad exploitation of Microsoft Exchange Servers in 2021, CISA led asset response and mitigation efforts as part of the Cyber Unified Coordination Group that was stood up to combat this activity. Not only did CISA publish guidance to mitigate the group, but it also worked hand-in-hand with interagency partners and industry to ensure broad-based awareness and mitigation.

Public-private partnerships are another critical tool DHS uses to counter cyber threats and improve collective cybersecurity resilience. The DHS-led Cyber Safety Review Board (CSRB), a group made up of leading cyber experts in the public and private sectors, raised concerns about the PRC's mandatory vulnerability disclosure laws in the context of its review of the log4j vulnerability. Not only did the Board raise concerns about this law potentially affording the PRC an exclusive window to take advantage of these vulnerabilities, it also noted possible sanctions placed on a company in the PRC for responsibly reporting a vulnerability to the wider cybersecurity community.

Likewise, CISA established the Joint Cyber Defense Collaborative (JCDC) in August 2021, which represents an evolution of the Federal Government's approach to operational collaboration and public-private partnerships. The JCDC is comprised of members of the interagency, private industry, and State, local, Tribal, and territorial (SLTT) representatives to engage as co-equal partners in real-time and persistent collaboration for operational outcomes. For example, in February 2022, a JCDC private-sector member leveraged the Collaborative's operational relationships to alert two foreign governments that they were targets of novel PRC malware called Daxin. CISA was able to connect the Government and the private-sector company to assist in remediation in less than 48 hours, thanks to the strong public-private relationships of the JCDC.

DHS is also working closely with SLTT and interagency partners to improve our cybersecurity posture and protect our critical infrastructure. In July 2021, DHS launched StopRansomware.gov with the Department of Justice and other Federal partners—the first whole-of-Government website that pools Federal resources to combat ransomware and helps private and public organizations of all sizes. In September 2022, CISA and the FBI built on this effort to launch the Joint Ransomware Task Force (JRTF) to coordinate a whole-of-Government effort to combat the threat of ransomware. In September 2022, the Department announced the State and Local Cybersecurity Grant Program (SLCGP) to help SLTT partners address cybersecurity risks and cybersecurity threats to information systems. In fiscal year 2022, $185 million was made available under the SLCGP, with varying funding amounts allocated over 4 years from the Infrastructure Investment and Jobs Act.

Internationally, DHS is creating enduring partnerships with partners on cybersecurity, law enforcement, research and development, emergency management, and resilience. This includes the Secretary's participation in Singapore Cyber Week in October 2022, where he highlighted the risks of PRC-affiliated technology, and the signing a memorandum of cooperation on cybersecurity with Japan in January 2023. This agreement will allow Japanese agencies to strengthen operational collaboration with DHS, enhance the security of critical infrastructure, foster more opportunities for partnership, and continue sharing best practices with our Indo-Pacific partners. These alliances not only aid in countering malicious cyber activity from foreign adversaries, but also criminals who operate globally. For example, in January 2023, the FBI and the U.S. Secret Service, along with critical cooperation from international partners in Germany, the Netherlands, and Europol, were collectively able to dismantle the Hive ransomware group—a criminal operation that targeted more than 1,500 victims, including hospitals, schools, and critical infrastructure, across the globe.

INTELLECTUAL PROPERTY RIGHTS (IPR) THEFT

America's global leadership is underpinned by a fair, open, and competitive economy that cultivates opportunities and innovation at home and abroad. For too long, the PRC has exploited the rules-based multilateral trading system in pursuit of a zero-sum approach to global competition while seeking to undermine American global leadership, national security, prosperity, and competitiveness. DHS plays an active role in securing the U.S. economy and its supply chains from PRC-related threats, through its various investigative authorities. DHS will continue to lead these efforts across our component missions to identify and mitigate foreign direct investment and surveillance risk while preserving the American-led order and ensuring fair and open global trade.

DHS works closely with interagency partners across several venues dedicated to protecting our national security and economic security, both operationally and in the on-going development of national policy. We participate in robust, risk-based screening of inbound foreign direct investment via the Committee on Foreign Investment in the United States (CFIUS); advise the Federal Communications Commission (FCC) on the national security implications of foreign entities seeking U.S. licenses to operate communications critical infrastructure via the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (known as Team Telecom); support the Commerce Department in exercising its authorities to assess broad risks to the information and communications technology supply chain from foreign adversaries; and lead the U.S. Government's response to stop global IP theft and enforce trade laws via U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI)-led National Intellectual Property Rights Coordination Center (IPR Center). These efforts derive their strength from the interagency approach, which brings together all relevant U.S. Government expertise on various technologies, industry sectors, and mission equities. DHS ensures these collaborative efforts benefit from our unique cybersecurity, critical infrastructure, and border security expertise.

For example, the United States has implemented carefully tailored restrictions on the most advanced semiconductor technology exports to China that are premised on national security concerns. HSI is expanding its efforts to counter the illicit acquisition of American microelectronics and other strategically important technology. These efforts include supporting the newly-established Disruptive Technology Strike Force.

The Department has leveraged its authority within these interagency bodies to take significant steps to protect U.S. national and economic security from malign PRC activity. On October 26, 2021, the FCC revoked and terminated China Telecom America's (CTA) domestic and international Section 214 licenses in response to a joint recommendation from DHS and the Departments of Justice and Defense in their capacity as members of Team Telecom. This terminated CTA's ability to provide domestic and international telecommunications services within the United States. In addition to actions taken against PRC entities' ability to offer telecommunications services in the United States, the Department continues to leverage Team Telecom to address national security threats posed by the deployment of equipment from PRC vendors on critical telecommunications infrastructure, such as subsea fiber optic cables that carry most international communications traffic.

FORCED LABOR

The PRC's use of government-sponsored forced labor constitutes an economic threat against the United States and our international partners and undermines legitimate trade. In recent years, the PRC carried out what the United States has rightly characterized as a campaign of genocide against the predominantly Muslim Uyghurs and other members of ethnic and religious minority groups in the Xinjiang Uyghur Autonomous Region (Xinjiang) of western China.

The United States has long recognized the PRC's campaign constitutes a state-sponsored system of repression of these ethnic groups, and goods mined, produced, or manufactured, wholly or in part, with forced labor are unfairly traded goods that undermine the rule of law and threaten the economic security of legitimate businesses and their workers.

DHS has powerful tools in Section 307 of the Tariff Act of 1930 and the Uyghur Forced Labor Prevention Act of 2021 to prohibit the importation of goods made in whole or in part with forced labor. U.S. Customs and Border Protection is responsible for enforcing these laws, including by identifying and reviewing high-risk shipments, and detaining, excluding, or seizing and destroying merchandise determined to violate any forced labor prohibitions.

In its role as the Chair of the Forced Labor Enforcement Task Force, DHS leads the implementation and enforcement of these laws, while collectively leveraging the authorities and expertise of our sister agencies, including the Departments of State, Labor, Commerce, Justice, and Treasury, and the Office of the U.S. Trade Representative to develop initiatives that can support and enhance compliance.

TRANSNATIONAL REPRESSION

The PRC threat is not limited to the economic or cyber domain. Operation Fox Hunt, a PRC government effort through which Beijing targets and seeks to repatriate and prosecute PRC individuals living in foreign countries whom the PRC alleges are guilty of corruption and should be returned to the PRC, has been used to target critics and dissidents living around the globe. Another recent example of the PRC's efforts to engage in acts of transnational repression is the PRC's unlawful operation of "overseas police service stations" in more than 50 countries, including the United States.[1] These acts no doubt represent only the tip of the iceberg of the PRC's transnational repression efforts in this country.

The PRC's repressive activities span far beyond U.S. borders and involve efforts to manipulate the rules and mechanisms of international law enforcement cooperation. Uyghur and other PRC diaspora communities in the United States have highlighted the detrimental impacts of politically-motivated INTERPOL red notices issued at the request of the PRC government, which have resulted in the detention of community members overseas. DHS and its interagency partners have worked together over the last 2 years to strengthen the actions the U.S. Government is able to take in support of the internal INTERPOL reforms to prevent abuse of its critical tools for politically-motivated purposes.

Another important aspect of DHS's strategy to counter transnational repression is its continuous engagement with targeted communities, which helps us to better understand the scope of the threat and respond appropriately. The PRC diaspora—including Uyghurs, Tibetans, and Hong Kongers—living in the United States often faces virtual harassment, threats, and attacks, including on social media platforms. Significantly, their family members in the PRC may face retaliation such as exit bans, loss of employment, and detention. DHS is working with members of affected communities to share information on Federal resources available to support nationals in the United States and to support those seeking refuge in the United States.

At the Summit for Democracy in March, Secretary Mayorkas outlined new initiatives to counter the misuse of technology against communities who are at heightened risk of cyber threat targeting and transnational repression. CISA's High-Risk Community Protection Initiative, which is resourced by the JCDC, will focus initially on engaging civil society organizations to listen and learn about the cybersecurity threats they are facing, find out what support is most needed, identify positive work to amplify, and then work through the JCDC and with partners to fill cybersecurity gaps. Additionally, CISA, in coordination with the State Department, will cohost a Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression with the United Kingdom. At this dialog, DHS will work with international partners from Australia, Canada, Denmark, Estonia, France, Japan, New Zealand, Norway, and the United Kingdom to improve the cybersecurity

[1] See Safeguard Defenders September Report "Patrol and Persuade."

of civil society organizations, engage in information sharing on the threats facing high-risk communities, and identify opportunities for greater collaboration around the world.

CONCLUSION

In summary, the PRC poses a range of threats across different vectors to the United States and our homeland. However, DHS remains clear-eyed in our understanding of these multifaceted challenges and continues to proactively undertake efforts to mitigate risks to our Nation's security and our democratic way of life. We remain unwavering in our commitment to counter the PRC's whole-of-Government threat by providing a whole-of-homeland response, whether in cyber space, in the defense of critical infrastructure, our economic security, or in preventing the assault on democratic values and freedoms.

Thank you for the opportunity to appear before you today and we look forward to taking your questions.

Chairman PFLUGER. Thank you.

The Chair now recognizes for his opening statement Mr. Durham.

STATEMENT OF TYRONE DURHAM, ACTING DIRECTOR, NATION STATE THREATS CENTER, OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY

Mr. DURHAM. Thank you. Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you today where my testimony will provide an overview of the complex threat to the homeland from the government of the People's Republic of China.

Let me be clear about the intent of my opening statement and testimony. At no time should anything I communicate be taken as aspersions against the people of China or against any Chinese or other Asian Americans in the United States. My comments and testimony pertains solely to the actions, policies, practices, and procedures of the Chinese government.

The increasingly aggressive activities of the PRC represent significant threats to the homeland as the PRC continues to challenge the United States by using a whole-of-government approach to undercut our competitiveness and democracy. The PRC uses an innovative combination of traditional and nontraditional intelligence tradecraft, cyber espionage, and predatory economic methods to gain illicit access to U.S. critical infrastructure and steal American innovation, along with research, technology, and other intellectual property. The PRC exploits our academic and scientific communities by compelling some foreign students, scholars, and researchers to identify and collect sensitive information and research. It also uses talent recruitment programs to acquire the technical know-how to exploit the information at it stole.

The PRC's top-tier cyber espionage and attack capabilities represent significant on-going threats to the U.S. public and private-sector interests. The PRC uses cyber means to illicitly obtain U.S. intellectual property, personally-identifiable information, and export controlled information. Their push to develop their own industrial base and to secure access to critical supply chains for manufacturing, research, and social stability likely includes investments in the United States using subversion to gain access to new technologies, businesses, and research institutions. PRC firms also engage in various licit and illicit investment strategies to acquire real estate and other assets and gain proximate access to targets in the homeland for malign purposes. Moreover, through its National Security Law, the PRC could compel organizations and citizens to comply with state intelligence efforts, thereby expanding its whole-of-government effort to a whole-of-society effort targeting the homeland.

To meet these challenges, DHS remains committed to sharing information with our partners to mitigate threats to the homeland. The Office of Intelligence and Analysis placed intelligence officers locally in every fusion center across the Nation to share information related to intelligence threats from the PRC and other foreign adversaries. The Department works closely with Homeland Security advisors and the private sector in every State and territory to increase the resiliency and preparedness of our communities.

Thank you again for the opportunity to appear before you, and I look forward to your questions.

Chairman PFLUGER. Thank you, Mr. Durham.

Members will now be recognized in order of seniority for their 5 minutes of questioning. An additional round of questioning may be called after all Members have been recognized.

I now recognize myself for 5 minutes of questioning.

I appreciate all of your testimonies, the seriousness with which you take this threat. I do want to highlight that last month, the FBI made two arrests related to the secret Chinese police station operating in New York City and charged dozens more as part of a larger PRC effort to locate in America pro-democracy Chinese activists and others who are openly critical of Beijing's policies and to suppress their speech. On the 24th of April, Chairman Green and myself sent a letter to both DHS and to the FBI requesting additional information about this police station. It has now been over 2 weeks past that deadline that we asked for, so I would ask you, please, to respond to that letter in writing and to highlight that. It is very important that we understand what has happened, but this Manhattan-based police station was operating as a provincial branch for the Ministry of Public Security, which belongs to the Commerce Indie list for its implication in human rights violations.

My question, and we will start with Ms. Murphy, is how was the station associated with such a nefarious organization? How did it pop up in New York City?

Ms. MURPHY. Thank you for the question, sir, and I'm happy to work with the team so we can get you a more fulsome response, probably in a Classified setting.

As you know and as you remarked in your opening statement, the threat from China is complex and vast. The way that they work in the United States, and I imagine in other countries who are seeing similar threats from the Communist government of China, is very diversified and layered. So when we talk about universities or researchers or academics or innovation, China proliferates all those spaces to include in our communities where Chinese Americans live, as a way to influence those communities. We work actively to identify those and investigate them.

Chairman PFLUGER. Would you say that they are using every available tactic, technique, and procedure to infiltrate American national security interest and interest writ large?

Ms. MURPHY. I would say that their attack surface is large.

Chairman PFLUGER. OK.

Ms. MURPHY. They are using all the tools in their toolbox to gather information, whether it's Classified, intellectual property, sensitive, un-Classified, anything that they consider of value.

Chairman PFLUGER. OK. We will follow up on that a little bit later.

I would like to go to the well-documented approach that they have used to acquiring either critical minerals, critical industries, farmland, ranch land, some of them near military sites, especially sensitive military sites.

Mr. Kahangama, can you comment on the acquisition of this farmland? Has DHS or FBI overlaid the flight path of that Chinese spy balloon that came over the United States several months ago with acquisition, acquired land, and anything else that would be of note?

Mr. KAHANGAMA. Thank for the question, Chairman. I would defer some of those questions to our intelligence colleagues about specifics about what happened. But what I can mention is that we do feel that we have tools to address these types of concerns.

First, to your point about land acquisitions, I think thanks to Congress as well, real estate purchases are now included as within the purview of what we call CFIUS, the Committee on Foreign Investment in the United States. So we do have an ability to look at land purchases when they have a nexus specifically to military sites or what would be airports or seaports, and conduct a risk assessment if a foreign purchase of that is subject to foreign control. So we do feel that we have some tools against that.

With the balloon specifically, DHS's CISA did track the flight path of the balloon and critical infrastructure nodes that were associated with it. I believe CISA conducted about 27 notifications and outreach to State and local and critical infrastructure entities to help them understand and mitigate against the risk.

Chairman PFLUGER. Did it appear that the overflight path was actually over acquisitions by CCP-related entities?

Mr. KAHANGAMA. I don't have the information, but I deferred to my intelligence colleagues.

Chairman PFLUGER. OK. I will do a follow-up here for Mr. Durham.

We have heard about the variety of threats and what Mr. Kahangama just talked about with the land acquisitions. Could you speak to the threats of CCP-owned agricultural operations and the effect that has on our supply chains and our Nation's food security?

Mr. DURHAM. Thank you, Chairman, for that question.

I think one of the things we know about the CCP is that their actions and activities are strategic and long-term. We've taken a specific set of individuals in the organization and built a team around PRC activities to better understand exactly what they're doing in terms of their agricultural purchases and such. We believe we have information that we could provide to you in a Classified setting to better elucidate their activities.

Chairman PFLUGER. Thank you. My time has expired. We have multiple requests out to both of your agencies for those Classified briefings, and we expect those to be filled.

I now recognize the Ranking Member, Mr. Magaziner, for his line of questioning.

Mr. MAGAZINER. Thank you, Chairman.

There is a lot we could touch on here, but I want to focus my initial questions on the issue of IP theft.

There is obviously a national security imperative that we protect the intellectual property and trade secrets of our defense industry and related industries. But there is also an economic imperative that we protect American companies and American jobs from intellectual property theft. When an American manufacturer or an American agricultural firm has their intellectual property stolen, that ultimately costs American jobs.

So I will start with Mr. Kahangama. The 2023 Quadrennial Homeland Security Review warns that the CCP is seeking to acquire our intellectual property and sponsoring a relentless barrage of cyber attacks that threaten our competitiveness. Can you describe for us how DHS is working with industry partners and other Federal agencies to shore up our vulnerabilities and guard against the theft of intellectual property?

Mr. KAHANGAMA. Absolutely. Thank you for that question, Ranking Member.

This is an utmost priority for the Department. A lot of our efforts are led through the Homeland Security Investigations Intellectual Property Rights Center, the IPR Center, and that is an inter-agency collaboration center where we are able to have industry come in, provide them threat briefings, conduct information sharing, and otherwise provide specific threat information to some of these targeted entities.

I think the cybersecurity angle is very important as well. Our Cybersecurity and Infrastructure Security Agency is actively working on addressing specific PRC cyber threats because the best indicator of what is going to be stolen is what's already been exploited. So we've done things like publish lists of known vulnerabilities that the PRC has already exploited and pushed that information out so that industries, sensitive technology holders, and others can patch those holes and otherwise protect themselves. We've also conducted a wide array of briefings, both Classified and un-Classified, to share this threat with them and continue to engage in real-time information sharing.

Mr. MAGAZINER. Thank you.

I will ask a similar question to Ms. Murphy. Can you talk about what the FBI is doing, again with other Federal agencies and with private-sector partners to help protect American intellectual property and in so doing, protect American jobs?

Ms. MURPHY. Absolutely. This is a top priority for me and for the FBI. There's a lot of obviously nuance to this threat and different layers. So let's start with the innovation in emerging tech society. We've learned through interactions that venture capitalists are the best at identifying the tech that is going to actually succeed because their money depends upon it. So we've done extensive outreach, especially in the San Francisco area, with venture capitalists to try and identify what that tech is, to help protect that. But we also know through our outreach that smaller entrepreneurs don't have the money to invest in protecting their intellectual property or in cybersecurity. So we've done a lot of outreach in that space to try and educate people about intellectual property, and those efforts are on-going.

When we talk about delivering uncompromised technology to our war fighters, when there's a place like AFWERX or AFC that's doing outreach to the emerging tech space, we work closely with them to try and protect the technologies that they're bringing in from principal research all the way through into Classified space and their labs.

So it's a space that we're very focused on and we're doing a lot of outreach on. I think that will continue and grow.

Mr. MAGAZINER. Thank you.

Just one more question on this topic for any of you. If there are people watching this hearing from home who may own a business or run a business or run a local utility or other piece of critical infrastructure, what can you do for them? Like, what are the resources for the people who are watching at home, who want to know what their vulnerabilities are, who want to know how to protect themselves? Can they reach out to DHS, can they reach out to the FBI? What services can you offer to help them protect themselves?

Ms. MURPHY. I think both agencies—I'll pass it over to Iranga, but I think both agencies offer different tools to help depending on the range of what they're looking at, whether it's from cybersecurity, educational, protecting intellectual property, insider threat. I think both agencies have tools, and I would encourage them to reach out.

Mr. KAHANGAMA. Thank you. If I could just follow up CISA, specifically at CISA.gov, their website has actual free services that cost nothing that small and medium businesses can download and utilize to effectively scan their systems and understand the threat picture. They can also reach out to CISA for a little bit more specific and in-depth vulnerability assessments, but there are a number of free tools on our website.

Mr. MAGAZINER. Thank you.

For those watching at home, CISA is the Cybersecurity and Infrastructure Security Agency, C–I–S–A. So we encourage everybody to take advantage of those services.

I yield back.

Chairman PFLUGER. The gentleman's time has expired.

The Chair now recognizes the gentleman from North Carolina and the Chairman of the Subcommittee on Oversight, Mr. Bishop.

Mr. BISHOP. Thank you, Mr. Chairman.

Ms. Murphy, a good bit of your testimony focuses on—I know this hearing subject matter is the threats from China, and some of those are covered, but a lot of your written testimony focuses on the FBI's Foreign Influence Task Force that comes under the Counterintelligence Division that you are the deputy director of, correct?

Ms. MURPHY. There's three deputy assistant directors in the counterintelligence division. The Foreign Influence Task Force actually falls under a different deputy assistant director, but it is in the Counterintelligence Division.

Mr. BISHOP. But in the division. OK. Has the Foreign Influence Task Force changed its practices any as a result of the revelations from the Twitter files or from the litigation undertaken by the Attorneys General for Louisiana and Missouri?

Ms. MURPHY. So, sir, I would have to take that question back to the team and get you an answer. I'm not aware of their processes or any changes that they've made.

Mr. BISHOP. Are you familiar with the work of that—and you have read the Twitter files, I assume?

Ms. MURPHY. I have not.

Mr. BISHOP. You have not read any of it?

Ms. MURPHY. No.

Mr. BISHOP. Interesting. Are you aware that the FBI regularly meets or met before the 2020 election with the social media platforms?

Ms. MURPHY. I saw the media reporting on that.

Mr. BISHOP. OK. Are they still meeting in the same way with the social media platforms?

Ms. MURPHY. Sir, I would have to take that question back. I personally am not meeting with the social media companies in my role.

Mr. BISHOP. OK, and you receive no reporting and you are otherwise unfamiliar internally with the activities of the Foreign Influence Task Force insofar as their interactions and engagement with social media platforms is concerned?

Ms. MURPHY. No, sir. That's not part of my role or my purview and my job.

Mr. BISHOP. I see.

Let me ask this question. One of the, perhaps the most effective operation by the counter foreign malign influence operation by the FBI in the 2020 election was convincing social media not to—or to suppress the Hunter Biden laptop story by preparing them to be on the lookout for hack-and-dump operations. Did the FBI know at that time the content of the Hunter Biden laptop, which it had in its possession by means of a subpoena?

Ms. MURPHY. Sir, I don't know the answer to that. I'd have to respectfully refer you to the attorney that's prosecuting that case.

Mr. BISHOP. Who are the other deputy directors in addition to yourself in the Counterintelligence Division?

Ms. MURPHY. Scott Grady is the deputy director of Intelligence. Right now, we have an acting director, Roman Roznosky, over Russia and other countries.

Mr. BISHOP. Which one supervises the Foreign Influence Task Force?

Ms. MURPHY. Scott Grady.

Mr. BISHOP. You have written about foreign malign influence in your testimony. In fact, of the testimony, which is only about 3½ pages, a full page of it is about foreign malign influence. Actually, page-and-a-half. What do you know personally about the FBI's actions against foreign malign influence?

Ms. MURPHY. In those instances, sir, it would be things like the police station and the Chinese influence in the United States against Chinese Americans living here or Chinese persons being in the United States that they're trying to repress or take back.

Mr. BISHOP. What about the portion that—see if I can find something here. What about this part, you said, coordinating closely with our partners and leveraging relationships we have developed in the technology sector, we had several instances where we were able to quickly relay threat indicators that those companies, speaking of social media companies, used to take swift action blocking budding abuse of their platforms. What do you know about that?

Ms. MURPHY. Sir, that might be a reference to our work with forum partners.

Mr. BISHOP. Well, this is in your written testimony before the committee.

Let me give you a fuller context. It says the FITF brings the FBI's national security and traditional criminal investigative expertise under one umbrella to prevent foreign influence in our elections. This better enables us to frame the threat, to identify connections across programs, to aggressively investigate as appropriate, and importantly, to be more agile. Then you talked—and then that last sentence where I read. So do you personally not have knowledge of that since you don't actually deal with the FITF?

Ms. MURPHY. As I stated, the Foreign Intelligence Task Force falls under DAD Scott Grady. I've seen, as I mentioned, the media reports. I know that there's engagements, but those aren't part of my role and that's not something that I take part of them.

Mr. BISHOP. It is curious that it is included in your testimony in that case.

I would ask you more, but I guess my time has expired, so I will yield back.

Chairman PFLUGER. The gentleman's time has expired.

The Chair now recognizes the gentleman from New York, Mr. Goldman.

Mr. GOLDMAN. Thank you very much, Mr. Chairman. Thank you to our witnesses for being here today.

Mr. Durham, I appreciated very much you saying in your opening statement that your comments are not directed at Chinese Americans or AAPI individuals who are in this country, but at the Chinese government. I have a district that is more than 20 percent API, much of which is of Chinese descent and the hateful rhetoric that has come from our former President and others over the last several years has led to a record increase in hate crime, especially against those of Chinese descent.

I want to talk a little bit about the distinction that you are drawing, which I think is an important one, particularly as it relates to the so-called police stations that the Chinese government has set up at various places around the world, including in our country.

Ms. Murphy, I am sure you are aware, and the Chairman referenced this case, the two arrests in my district of two Chinese nationals for operating one of these police stations, which, so everybody is clear, is really designed to track Chinese dissidents or Chinese citizens in the United States essentially as an unsanctioned police station, so to speak. Now, I am assuming, Ms. Murphy, you are not going to be able to speak much about that specific prosecution, but can you tell us more broadly, taking a step out of that prosecution, what the FBI understands about these police stations and the effort of the Chinese government to intimidate and threaten Chinese, either citizens or dissidents, who are living in this country?

Ms. MURPHY. Thank you for the question.

As I think the committee is aware, China goes through great lengths to control the narrative about the country of China. This is a way that they use influence and intimidation tactics against people that are in the United States that may have ties to China or views about China that the Chinese government doesn't agree with. So it doesn't just happen herein the United States, it happens in other countries too. We work proactively to identify and then investigate these instances, whether they're identified as police stations or liaison bureaus. We also work with foreign partners when we find information to share with them and they share back with us.

Mr. GOLDMAN. Can you describe some of the tactics that the Chinese government uses?

Ms. MURPHY. Sure. I think on the same day that the arrest in New York happened, we also announced an indictment against MPS for using a——

Mr. GOLDMAN. I am sorry, what is MPS?

Ms. MURPHY. The Ministry of Public Security. I think it's probably better for a Classified session, but they use tactics such as harassment, threatening relatives overseas, they can act like they are the arm of the government here, they use, you know, wide-ranging intimidation tactics.

Mr. GOLDMAN. Mr. Kahangama, I am not sure, or Mr. Durham, I am not sure if either one of you is the specific DHS witness to address this, but I wanted to ask a little bit about Chinese governmental efforts to interfere in elections, both in this country as well as others, including Canada. To the extent that you can talk about this in an un-Classified setting, where do things stand with those efforts as we are moving forward toward 2024?

Mr. KAHANGAMA. Thank you for the question, Congressman.

Unfortunately, I will not be able to talk about that in this session, but I'm more than willing to arrange a Classified session for you with regard to that question.

Mr. GOLDMAN. I am not surprised, but it is something I think we are particularly concerned about. I know the Foreign Influence Task Force, FITF, was created in part to address the efforts of foreign entities to interfere in our elections and to try to infiltrate our national security.

So I do hope that we are all of—you three and your agencies are very much focused on this and making sure that our election infrastructure is as strong as it can be.

My time is now up. So thank you for the time, and I yield back.

Chairman PFLUGER. The gentleman's time has expired.

The Chair now recognizes the gentleman from Arizona, Mr. Crane.

Mr. CRANE. Thank you, Mr. Chairman. Thank you to the panelists who have come here today to share your time.

Ms. Murphy, you work for the FBI, is that correct?

Ms. MURPHY. Yes, sir.

Mr. CRANE. Ms. Murphy, do you know what elite capture is?

Ms. MURPHY. Elite capture?

Mr. CRANE. Yes, do you know what elite capture is?

Ms. MURPHY. No, sir.

Mr. CRANE. So, basically, elite capture is used by the CCP as a form of political warfare that seeks to control the actions of political, academic, business, and cultural leaders outside of China to benefit the CCP. The means of control take a variety of forms, including financial incentives, financial dependence or compromised business entanglements, offers of access to opportunities within China, ideological appeal, and even blackmail. Are you familiar with these techniques, ma'am?

Ms. MURPHY. I am familiar with those techniques.

Mr. CRANE. Do you have experience with those techniques? Seeing those techniques in your job?

Ms. MURPHY. Experience in seeing the Chinese government use those techniques?

Mr. CRANE. Yes. Or any other nation-state that wants to compromise U.S. officials?

Ms. MURPHY. I don't know that I've seen them personally, but I'm familiar with those techniques, yes, sir.

Mr. CRANE. OK.

Ms. Murphy, are you aware that a Chinese spy balloon just recently flew over the United States for about a week?

Ms. MURPHY. I am.

Mr. CRANE. Ms. Murphy, are you aware that the CCP is buying up U.S. farmland near military bases?

Ms. MURPHY. I've heard reports of that. I don't know what evidence I've seen of it.

Mr. CRANE. OK. Ms. Murphy, does it concern you some of the revelations that have been coming out of the Oversight Committee about the millions of dollars that have been paid to the Biden family recently?

Ms. MURPHY. I'm not aware of money being paid to the Biden family.

Mr. CRANE. Oh, you are not aware of that at all?

Ms. MURPHY. No, sir.

Mr. CRANE. That is interesting. You work for the FBI, right?

Ms. MURPHY. Yes, sir, I do. But I would respectfully refer you to the investigators over that case. I'm sure we can get you a brief on that. That is not a case that I handle.

Mr. CRANE. Yes, well, I don't need a brief on that, ma'am, to know that there are nation-states that have paid millions of dollars to the Biden family. That is one of the reasons that we are having this hearing, that is one of the reasons that Americans are so concerned that they see Chinese spy balloons flying over the United States for an entire week, that is why they are so concerned that they see these Chinese police stations being set up here, and they are wondering, how could this go on, this doesn't make any sense. Yet the son of the President of the United States is involved and entangled for many years now in multiple business deals that the President claims he knows nothing about. You, ma'am, you sit here before the Homeland Security Committee—our job is to protect the homeland, and you act as if you don't know anything about it.

Do you understand why the American people are concerned, ma'am? Yes or no?

Ms. MURPHY. I understand why American people should be concerned about the threat from the Chinese Communist Party.

Mr. CRANE. Yes. Do you see any connections with what I talked about, when I was talking about elite capture? Are you connecting the dots at all?

Ms. MURPHY. No, sir.

Mr. CRANE. You don't connect the dots? So your job is to protect the American people. I just read you what elite capture is, the summary, the definition of elite capture. Everybody knows in this town what is going on, everybody knows what is coming out of these committee hearings right now. It is pretty sad coming from somebody who, as a young man, wanted to be a part of your organization because of the reputation that men and women from the FBI had built up over decades, and now the American people hardly trust the FBI, they struggle with the Department of Justice. Quite frankly, generally, they feel as if you don't have the right politics, you can basically do whatever you want. The American people, quite honestly, are wondering why Hunter Biden is still walking the streets.

Thank you. I yield back.

Chairman PFLUGER. The gentleman yields.

The Chair now recognizes the gentle lady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Let me thank the Chair and Ranking Member, as always, for their courtesies.

Let me be as delicate as I can possibly be, and certainly express my friendship to all of the Members on the other side of the aisle, but I would offer to say that I have the highest respect for the FBI as I have worked with the Bureau for over 28 years. I was here in the U.S. Congress after 9/11, during 9/11, ran for my life from the United States Capitol, went to Ground Zero during the recovery, watched the pain of firefighters removing remains, and watched the intensive investigation that was augmented by the work of the FBI.

We created the U.S. Department of Homeland Security, and I could not be more proud of the work that the Department have done. In particular, was key in stopping the potential attack at the beginning—as a number of terrorist potential came in after 9/11. We were still concerned about international terrorism. We now know that, according to the FBI, the No. 1 terrorist act against all of us is domestic terrorism, as evidenced by January 6.

I am very glad, Mr. Durham, that you made it very clear that this hearing should not be about Chinese Americans. Patriots, families, students, teachers, doctors, people in my community of Houston, Texas, I want them to know that this hearing—I could not sit in this hearing if this was an attack on Asian Americans, Chinese Americans. We have seen the rise in hatred. So, as I noticed that your position deals with nation-state threats, let us be framed, particularly about what we are doing herein. I have to respect my friend, but I haven't gotten one question about Hunter Biden. I haven't seen any association with Mr. Biden with the President of the United States of America, short of the fact that as parents, we all have our children and we love them.

So let me just ask, Ms. Murphy, you indicated you were getting information, but right now you have not come here to discuss Hunter Biden, is that correct?

Ms. MURPHY. That is correct, ma'am.

Ms. JACKSON LEE. Nor you are here to discuss the President of the United States' connectedness to Hunter Biden other than your recognition that it is his father?

Ms. MURPHY. That's correct.

Ms. JACKSON LEE. Thank you so very much.

Mr. Durham, and I have some questions I need to get to quickly, but I just want to make sure, am I correct, as you made your opening remarks, that this hearing—or you did not come here to attack Chinese Americans who are patriots serving in respective responsibilities across America in the Asian American community?

Mr. DURHAM. That's correct, Congresswoman.

Ms. JACKSON LEE. You are not here to promote hate based upon our responsibilities in national security?

Mr. DURHAM. That's correct, I am not.

Ms. JACKSON LEE. Thank you so very much.

I just wanted to make sure that we were clear on the responsibilities that we have here today.

Let me just say that as a Member, I have had the Chinese from the government approach my staff. I have had them approach me. I am the Congresswoman in the area where the Chinese council had to be closed down, rightly so by the former administration. We welcomed that. I am not a stranger, but I recognize that we must discern in order to be intelligent.

Let me quickly say, in today's testimony, we have heard extensively about the Chinese Communist Party's illicit use of transnational repression against its own diaspora. Concerned about that and the foreign malign influence campaigns directed the people of the United States, tactics that are repressive, coercive, and even criminal. What have we learned about these operations and how do we intend to counter these disinformation campaigns, protect our homeland, and prevent these attacks from undermining our free market activities in our democratic institutions?

Go at it, whichever one is going to answer first.

The last, how can we best prevent these activities from disrupting our free market activities in our democratic institutions?

Somebody should comment on the dangers of AI with respect to the Chinese.

If you could start—you want the FBI to start, Ms. Murphy?

I will yield to Homeland Security. Thank you.

Mr. Kahangama.

Mr. KAHANGAMA. Thank you for the question.

So I think in the remaining time, one program I would like to highlight is a recently-announced High-Risk Community Protection Initiative from our Cybersecurity Infrastructure Security Agency. So it's engaging diaspora, civil society groups, and communities in the United States, understanding the threats and then offering them cybersecurity services, including from things like spyware that may be leveraged to otherwise undermine them in this country.

Ms. JACKSON LEE. Mr. Durham——

Chairman PFLUGER. The gentlelady's time has expired.

Ms. JACKSON LEE. Should he answer the question if my mouth was moving? Mr. Durham, would you just give a word? The Chairman is being very kind. He is a fellow Texan and I will step back and thank him. I will step back.

Mr. DURHAM. Thank you, Congresswoman.

I say this about the PRC, they are very aggressive in their activities and they will use every technique, tool, or procedure within their toolbox to ensure that they accomplish their goals. They will turn those tools against diaspora communities as well. It is not uncommon for them to do it. We, as my colleagues have just said, are working with those communities to help them understand the threats.

Ms. JACKSON LEE. Thank you for your courtesy and Ranking Member for your courtesy.

Chairman PFLUGER. I thank the gentlelady. Her time has expired.

The Chair will now move into a second round of questioning. We have other Members who I know will be rejoining at a variety of points.

The Chair now recognizes myself for an additional 5 minutes of questioning.

I would like to enter into the record the letter that I sent on the 17th April about the police station in New York and the request for that.

So ordered.

[The information follows:]

MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Eighteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

April 24, 2023

The Honorable Christopher Wray
Director
Federal Bureau of Investigation
Washington, D.C. 20535

The Honorable Alejandro Mayorkas
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Director Wray and Secretary Mayorkas:

We write to request additional information about an illegal Chinese government police station in Manhattan, New York. On April 17, 2023, the Federal Bureau of Investigation (FBI) arrested two individuals for operating a Chinese police station in Lower Manhattan and obstructing justice by destroying evidence.[1] In a related case, the FBI charged 40 officers of China's national police for their involvement in transnational repression schemes targeting U.S. residents, which is when foreign governments illegally stalk, intimidate, or assault people in the United States.[2] These two plots where designed by the Chinese Communist Party (CCP) to harass Chinese nationals residing in the United States and suppress dissidents from speaking out against the CCP's oppressive regime.

The Chinese police station located in Manhattan drew national outrage when the non-governmental organization Safeguard Defenders released a report in September 2022 revealing the presence of 110 Chinese police stations located around the world, including in New York.[3] The FBI then indicated it was investigating the Manhattan-based Chinese police station, culminating in the April 17th arrests. Two men, "Harry" Lu Jianwang, 61, of the Bronx, and Chen Jinping, 59, of Manhattan, were charged with conspiring to act as agents of the CCP.[4] The defendants worked together to establish the first overseas policed station in the U.S. on behalf of

---

[1] Press Release, U.S. Dep't of Justice, *Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government*, https://www.justice.gov/opa/pr/two-arrested-operating-illegal-overseas-police-station-chinese-government (last visited April 17, 2023).

[2] Press Release, U.S. Dep't of Justice, *40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents*, https://www.justice.gov/opa/pr/40-officers-china-s-national-police-charged-transnational-repression-schemes-targeting-us (last visited April 17, 2023); Fed. Bureau of Investigation, Transnational Repression, https://www.fbi.gov/investigate/counterintelligence/transnational-repression (last visited April 17, 2023).

[3] *110 Overseas Chinese Transnational Policing Gone Wild*, SAFEGUARD DEFENDERS https://safeguarddefenders.com/sites/default/files/pdf/110%20Overseas%20%28v5%29.pdf (last visited April 17, 2023).

[4] Press Release, U.S. Dep't of Justice, *Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government*, https://www.justice.gov/opa/pr/two-arrested-operating-illegal-overseas-police-station-chinese-government (last visited April 17, 2023).

Director Wray
Secretary Mayorkas
April 24, 2023
Page 2

the CCP's Ministry of Public Security (MPS). In the related case, the defendants, including 40 MPS officers and two officials in the Cyberspace Administration of China (CAC), allegedly targeted and repressed U.S. residents whose political views and actions are disfavored by the CCP, such as advocating for democracy in the People's Republic of China.[5] The presence of this police station not only violated U.S. sovereignty, but circumvented both judicial and law enforcement cooperating procedures.[6]

The Committee is examining the persistent threats posed by the CCP to U.S. homeland security, in which the CCP continues to brazenly violate U.S. autonomy.[7] In February 2023, the CCP flew a surveillance balloon across the majority of the continental United States, collecting intelligence on sensitive military and homeland security sites.[8] The Committee continues to monitor and take action against Chinese Confucius Institutes and other Chinese entities of concern, which are operated on U.S. college campuses at the behest of the CCP to commit academic espionage. While the New York Chinese police station has been shut down, our work to mitigate CCP threats to the homeland is far from over. Therefore, we request responses to the following questions as soon as possible, but no later than May 8, 2023.

1. When was the FBI and the Department of Homeland Security (DHS) notified of the Chinese police station operating in Manhattan, New York as well as the Chinese national police officers working to repress U.S. residents?

2. When did the FBI begin its investigation of the Chinese police station operating in Manhattan, New York as well as the Chinese national police officers working to repress U.S. residents?

3. What actions has DHS taken to mitigate the malign impact of the Chinese police station operating in Manhattan, New York as well as the Chinese national police officers working to repress U.S. residents?

4. In addition to the Chinese police station operating in Manhattan, New York, there are allegations of these illegal organizations operating in a separate location in New York, NY, Los Angeles, California, San Francisco, California, Houston, Texas, as well as

[5] Press Release, U.S. Dep't of Justice, *40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents*, https://www.justice.gov/opa/pr/40-officers-china-s-national-police-charged-transnational-repression-schemes-targeting-us (last visited April 17, 2023)
[6] Press Release, U.S. Dep't of Justice, *Two Arrested for Operating Illegal Overseas Police Station of the Chinese Government*, https://www.justice.gov/opa/pr/two-arrested-operating-illegal-overseas-police-station-chinese-government (last visited April 17, 2023).
[7] *Confronting Threats Posed by the Chinese Community Party to the U.S. Homeland: Hearing Before the Subcomm. on Counterterrorism, Law Enforcement, and Intelligence of the H. Comm. on Homeland Sec.*, 118th Cong. (Mar. 9, 2023).
[8] Natasha Betrand, *Chinese spy balloon was able to transmit information back to Beijing*, CNN https://www.cnn.com/2023/04/03/politics/chinese-spy-balloon/index.html (last visited April 17, 2023).

Director Wray
Secretary Mayorkas
April 24, 2023
Page 3

cities in Nebraska and Minnesota.[9] What is DHS and the FBI doing to combat the malign influence occurring in these additional locations and across the homeland?

After you have provided this information in writing, we request the FBI and DHS provide Committee staff a briefing about the CCP's malign influence operations within the U.S. homeland, to include but not limited to the activities of a Chinese police station in New York no later than May 22, 2023. Please contact the Committee on Homeland Security Majority staff at (202) 226-8417 with any questions about this request.

Per House Rule X, the Committee on Homeland Security is the principal committee of jurisdiction for overall homeland security policy and has special oversight functions of "all Government activities relating to homeland security, including the interaction of all departments and agencies with the Department of Homeland Security."

Thank you for your prompt attention to this matter.

Sincerely,

MARK E. GREEN, MD
Chairman

AUGUST PFLUGER
Chairman of the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence

[9] Isabel Vincent, *After FBI busts Chinese 'police station' in NYC, six more exposed in US*, New York Post https://nypost.com/2023/04/18/chinese-police-stations-allegedly-spying-on-nyc-la-more/ (last visited April 17, 2023).

Chairman PFLUGER. Additionally, I would like to reiterate from the Chair's perspective to reflect my opening statement today and also in our previous hearing, the very first hearing that we had on this topic, what many of my colleagues have asserted, which is this has absolutely everything to do with the malign influence of the Chinese Communist Party and not of its people, and especially of those of any sort of Chinese descent that may live here or in any other diaspora around the world.

But I think it is fascinating to hear all three of you say that every tactic, technique, and procedure, as Mr. Durham just said, that they are very aggressive and every tool will be used, which I think is why we are here.

I will get into some questions for Ms. Murphy.

Are you aware that in November 2018, DOJ's China Initiative was established to address some of the most critical threats to national security posed by the Chinese Communist Party and that this initiative sought to raise awareness and to identify and prosecute Chinese trade secret theft and economic espionage, as well as to protect American critical infrastructure and supply chains from covert influence?

Ms. MURPHY. Yes, sir, I'm aware of that initiative.

Chairman PFLUGER. Do you agree with the former Attorney General that about 80 percent of all Federal economic espionage prosecutions have alleged conduct that would benefit the Chinese state and about 60 percent of all U.S. trade secret theft cases have had a nexus to China?

Ms. MURPHY. I can't confirm nor deny that, but that——

Chairman PFLUGER. In general——

Ms. MURPHY [continuing]. Wouldn't surprise me.

Chairman PFLUGER. You were working in the department at that time?

Ms. MURPHY. At the FBI? Yes, sir.

Chairman PFLUGER. Yes. OK. Do you agree in general that the connections are vast?

Ms. MURPHY. Yes, absolutely.

Chairman PFLUGER. Do you agree with your boss, FBI Director Wray, that the greatest long-term threat to our Nation's information and intellectual property and to our economic vitality is the counterintelligence and economic espionage threat from China?

Ms. MURPHY. Yes, sir, absolutely.

Chairman PFLUGER. Is it true that the FBI launches a counterintelligence case into China as often as once every 12 hours?

Ms. MURPHY. I don't know the exact numbers, but we have a lot of Chinese counterintelligence investigations. It's probably about half of the work that we do in the counterintelligence to Asia.

Chairman PFLUGER. Well, half. About how many on-going investigations would you say?

Ms. MURPHY. I don't know that I can give you in a specific number, but I'd say over 2,000.

Chairman PFLUGER. Over 2,000?

Ms. MURPHY. Yes sir.

Chairman PFLUGER. Incredible.

Is it true that the director of National Security Agency under President Obama, Keith Alexander, has called the Chinese state theft of U.S. intellectual property the greatest transfer of wealth in history?

Ms. MURPHY. I think so, yes. I believe that's true.

Chairman PFLUGER. Ms. Murphy, my question is this, as I mentioned previously, you have mentioned that the CCP will use any tactic, technique, procedure. Are they trying to influence industry leaders, key government leaders, people that have influence inside the United States?

Ms. MURPHY. I can't think of a specific example off the top of my head, but they definitely wield influence. I don't know if there is——

Chairman PFLUGER. Are they trying to influence certain people that they can bring into harmonization with what the CCP is trying to do to undermine our own national security? Is it in their interest to gather people inside the United States, whether they be government officials or industry leaders? As my colleague from Texas just mentioned, you are the Counterintelligence deputy director, so.

Ms. MURPHY. No, I understand, but what I'm trying to think through is they certainly try to influence innovation and get into a space to take intellectual property.

Chairman PFLUGER. So do they not try to influence people?

Ms. MURPHY. No, they certainly try to influence. I'm just trying to think through—so I would say Confucius Institute would be one way that they try to influence people. They've certainly used tactics to repress their own people.

Chairman PFLUGER. Have they tried to garner favor so that they can influence government leaders for their own benefits to undermine U.S. national security? Would this be a tactic they would do?

Ms. MURPHY. I think that's probably a question for a closed session, sir.

Chairman PFLUGER. Ms. Murphy, I think that the American people are having a hard time with the Department of Justice right now because of answers to questions like this. This is very simple. Ask a thousand people in our country this same question and they are going to say of course they are trying to do that. Do you have knowledge of this?

Ms. MURPHY. Sir, I think that's better for a closed session.

Chairman PFLUGER. I would like to remind the witnesses that you are testifying under oath.

Ms. MURPHY. I understand that.

Chairman PFLUGER. Do you have awareness of the CCP trying to use malign influence by gaining favor with government or industry leaders in the United States?

Ms. MURPHY. Sir, I think we'd have to take that to a closed session.

Chairman PFLUGER. Well, I look forward to that. We have multiple letters that we have sent to you that have gone unresponded to, including something that was previously discussed. I look forward to the Confucius Institute discussion as well.

My time has expired.

I now recognize the Ranking Member, Mr. Magaziner.

Mr. MAGAZINER. Thank you, Chairman.

I think we are touching on some important issues here. I mean, foreign malign influence is a real threat, and it takes many forms. It can take the form of trying to influence individuals in key positions, it can also take the form of trying to influence public opinion in a variety of ways. That is why I believe it is entirely appropriate that in Ms. Murphy's written testimony she highlighted the issue of foreign aligned influence from the CCP. Let's be clear, here in this country, we value the First Amendment, we value our individual freedoms, but the First Amendment does not apply to foreign governments trying to stoke division in our country, it does not apply to foreign governments trying to influence individual Americans, it doesn't apply to foreign governments at all, as a matter of fact. Nor does it apply to anyone, foreign or domestic, who is engaging in criminal activity, like plotting acts of violence.

So it is absolutely appropriate and important that we support the work of rooting out foreign malign influence that is seeking to do things like influence public opinion in the favor of the CCP or individuals.

My hope, again, is that this conversation can continue to be a bipartisan one. I could certainly spend my whole 5 minutes talking about the former President and his family's business dealings in China, which are well-documented, but I think we can all at least agree that whatever the political affiliation is of our elected officials, hopefully in the future, people will exercise better judgment in discretion in who they decide to do business with and avoiding doing business with individuals who may be aligned with governments that are adversaries of the United States.

So, listen, at at a high level, that is why this work is so important. We have to make sure that across agencies, we are doing everything in our power to limit the ability of the CCP to undermine our democratic values, to undermine our economy, and to undermine our national security.

So with all of that being said, either Mr. Durham or Mr. Kahangama, can you just give us a summary of what the 90-day DHS sprint entails? What is the work that is being done at DHS right now to escalate our ability to defend against the CCP threat?

Mr. KAHANGAMA. Thank you for the question. I'm happy to answer it.

So, as was mentioned, the 90-day sprint involves a concerted Department-wide focus on six key areas to counter the threat from the PRC in the homeland. This includes countering their pursuit of critical infrastructure, their economic coercion, countering their role in fentanyl coming across our border, securing our screening and vetting systems to make sure they're able to identify those risks, countering the PRC's movement and activities in the Arctic, and then making sure we're maximizing our counterintelligence information sharing against PRC-based counterintelligence threats.

I think what I'd like to emphasize is that these activities are what the Secretary is using to focus the Department and to elevate things that we've already been doing, make maximum and efficient use, just like our State Department and CIA, and others are centralizing their China and PRC-based activities. It's to set a stronger foundation for longer-term activities to counter these, it's part of an endeavor to work with inter-agency partners and the private sector and really to infuse the PRC into every aspect of our mission set, because we've come—it's been made quite clear that the PRC threatens all aspects of our mission, so reorienting and pivoting the Department to that threat for long-term awareness is part of that campaign.

Mr. MAGAZINER. Thank you.

I only have limited time left. I spent most of my first round of questions focused on the issue of IP theft against U.S. companies. Another persistent cyber threat from the CCP is their attempts to infiltrate critical infrastructure, particularly utilities. Can you just speak briefly about that threat and about DHS's actions to mitigate it?

Mr. KAHANGAMA. Thank you.

I would say that the threat of PRC intrusions into our critical infrastructure is the most pressing concern we would have with regard to the PRC. Their potential ability to gain access and hold our decision making at risk in light of a conflict is of utmost concern. We are actively working to ensure that we are engaged with critical infrastructure owners to patch systems, to share information, to turn off systems that are actively being exploited, and making sure that we take a whole-of-Government approach, whether that involves working with partners from DoD, the DOJ, Department of Commerce, and others.

Chairman PFLUGER. The gentleman's time has expired.

The Chair now recognize the gentleman from North Carolina, Mr. Bishop.

Mr. BISHOP. Thank you.

Ms. Murphy, does the FBI have any recommendations or opinion about Members of Congress making use of TikTok?

Ms. MURPHY. Sir, I don't know that the FBI has an opinion on Members of Congress using TikTok as an application. I think you're probably aware that the FBI employees are not allowed to put TikTok on their FBI-issued Government devices. And that we only——

Mr. BISHOP. Mm-hmm. Why is that?

Ms. MURPHY. Because we are only allowed approved apps on our Government device. I think that the committee is probably aware of the threat that the FBI perceives from TikTok or a nation-state like China having access to data to millions of Americans.

Mr. BISHOP. Would there be any reason to believe that that threat would not also apply if Members of Congress are using TikTok?

Ms. MURPHY. No, there would be no reason not to think that that wouldn't be a threat to Congress.

Mr. BISHOP. Ms. Murphy, do you have any responsibility for the FBI's FISA 702 database use?

Ms. MURPHY. I don't have any responsibility for the database, no.

Mr. BISHOP. Well, all right. Maybe my question was not very clear. Let me ask it this way. A *Reuters* article a couple of days ago points out that the FISA Court, in an opinion issued in April 2021, just declassified and released by the ODNI, found that the FBI improperly searched for information in a U.S. database of foreign intelligence 278,000 times over several years, including on Americans suspected of crimes, according to a ruling released Friday. Are you conversant with that subject matter?

Ms. MURPHY. No, sir. We have a person that's assigned specifically to deal with the 702 matter.

Mr. BISHOP. Who is that?

Ms. MURPHY. His name is Mike Herrington.

Mr. BISHOP. OK. You do not have that within your purview then?

Ms. MURPHY. Not the specific thing that you're talking, no.

Mr. BISHOP. Would you be aware of the—well, you would not be able to speak to, for example, changes that have been made by the FBI to prevent the abuses that the FISA Court described in its order, correct?

Ms. MURPHY. So I know that we've implemented significant changes. For instance, I know that the numbers that the FBI has queried on U.S. person information acquired under FISA 702 in 2022 was approximately 204,000, and that represented a 93, almost 94 percent drop year over year from 2021.

Mr. BISHOP. There has been sort-of a pattern. It was 3 million, and then this order talked about it being 278,000. But there have been a series of events where the 702 database use has been critiqued by the FISA Court. Americans only learn about it subsequently. Why should Americans be confident now that the use of the database is appropriate if these things—previous steps have been taken to correct the abuses, but it continues to happen, according to the FISA Court?

Ms. MURPHY. So I think the FISA Court, sir, is different than FISA 702. Applications that go in front of the FISA Court are full FISAs.

Mr. BISHOP. No, no, no, the FISA Court was the Court that issued the opinion that said the 702 database has been being abused by the FBI. You are aware of that, aren't you?

Ms. MURPHY. Yes, sir.

Mr. BISHOP. OK. That is what I am talking about. The FISA Court has repeatedly said the FBI is abusing its access to the 702 database. Why should Americans be convinced that now the FBI has rectified that, whereas it didn't before?

Ms. MURPHY. Sir, I don't know the details of that report, but what I would tell you is that the FBI strives to protect the American people. When there's policies or procedures in place, that that are identified to have——

Mr. BISHOP. I am really looking for specifics. OK.

Let me ask this question, does anyone on the panel know the holding of the Supreme Court case *Lamont* v. *Postmaster General,* 1965? Just to clue you in, it is the case that deals with whether Americans have a First Amendment right of access to foreign propaganda. Is none of you aware of that case?

Mr. Kahangama, do you have any responsibility for the MDM team at the Department of Homeland Security, the one that deals with misinformation, disinformation, and malinformation?

Mr. KAHANGAMA. I do not.

Mr. BISHOP. OK. Mr. Durham, do you have any responsibility for that?

Mr. DURHAM. Thank you for the question, Congressman.

I have a team at DHS that looks at foreign malign activities, yes.

Mr. BISHOP. Explain what that is, please, or what your team does.

Mr. DURHAM. My team looks at various efforts of the CCP, Russia, and other foreign nations, and how they attempt to influence opinions, win the hearts and minds of individuals in the United States, and engage in activities that would ultimately be in their benefit entirely.

Mr. BISHOP. Does DHS continue to switchboard, in the testimony of one of your officials on the MDM team?

Mr. DURHAM. Sir, I'm not aware of any switchboarding. I'm not in position to address that question.

Mr. BISHOP. My time has expired.

Chairman PFLUGER. The gentleman's time has expired.

The Chair now recognizes the gentleman from Arizona, Mr. Crane.

Mr. CRANE. Thank you, Mr. Chairman.

I want to make a comment about something that one of my colleagues who just left the room said. He made a reference to the former President of the United States and his family and their known business dealings in China and other places. I found it interesting because one of the biggest differences between the Trump family and their foreign business dealings and the Biden family and their foreign foreign business dealings is that the Trump family actually owns businesses. They actually own hotels and resorts. OK. Pretty stark difference from what we are learning—what many of us knew, and now we are actually hearing, as the Oversight and Judiciary Committee, actually get to bring in witnesses.

The sad thing is for everybody in this room, everybody in this room, everybody in this town, everybody in this country knows that if the FBI and our DOJ had the type of damning information, hard evidence, bank records, et cetera on the money laundering that this President, his family have been up to the last couple of years, and their names were Eric and Don Jr., we wouldn't even be having this hearing. You know why? They would be in jail. This is exactly the type of thing I was talking about, Ms. Murphy. This is exactly why so many of your colleagues have had enough, and they have become whistleblowers.

Ms. Murphy, what do you think about that? So many of your colleagues have had enough. What do you think about the whistleblowers that just said, I can't do it anymore. I can't cover for the organization, the institution that I work for, because I didn't swear an oath to them, I actually swore an oath to the United States and the Constitution. What do you think about that, ma'am? Do you feel like they betrayed the institution or are you glad that they are up here?

Ms. MURPHY. Sir, I appreciate the question.

I'm proud and I'm happy that we live in a country where there's whistleblower protection acts and that people can come forward when they think things have been done incorrectly.

You know, like I support the FBI. I think the FBI does amazing work.

Mr. CRANE. You know, ma'am, I think they do do some amazing work, too. But I think we both know that its reputation is massively tarnished. I think we are both glad that we have whistleblower provisions in this country. But I think if you weren't under oath and we weren't wearing these clothes and in this room right now and we were having a private conversation, I sure hope there is part of you that is embarrassed and disgusted with what the FBI has been up to. I know the American people are. I mean, look at the movies growing up. You guys are in, like every movie as the hero. When you were a little girl and you were watching movies growing up, did you notice that? Those cool blue jackets with the bright yellow lettering, the FBI on it, was that pretty cool watching those movies growing up and those TV shows and now getting to work for this organization?

Ms. MURPHY. It's amazing to work for this organization. Yes, sir.

Mr. CRANE. Is there a part of you, though, that feels torn, ma'am? Like the whistleblowers that are coming up here now in droves, that just say, I can't, I can't do it anymore. I didn't swear an oath to the FBI. Is there a part of you that feels torn or not at all? Ma'am, I am asking you a serious question.

Ms. MURPHY. Sir, I'm very proud to work for the FBI. I think I stated that.

Mr. CRANE. I know you are. That is not what I asked you, ma'am. I asked you if you feel torn.

Ms. MURPHY. Not at the least.

Mr. CRANE. Not the slightest?

Ms. MURPHY. Uh-uh.

Mr. CRANE. Well, that is pretty sad, ma'am. That really is. It really shows who your allegiances are to. It really does. As somebody who served this country myself, and I come from a very proud unit, the Seal teams, I know that my allegiances are not to NSW, Naval Special Warfare, they are not to a Seal team. I am glad, I am so proud that we have men and women who see their oath to this country, and they said, I can't do it anymore. I am going to go try and straighten this out so that the organization that I love can maybe, just maybe, be turned around, quit being a partisan tool, and actually protect the American people, which it clearly is not doing right now.

Thank you. I yield back my time.

Chairman PFLUGER. The gentleman yields.

The Chair will now enter to a third round of questioning and recognizes myself for 5 minutes of questioning.

I would like to enter into the record the annual Threat Assessment by the Office of the Director of National Intelligence*, and it basically goes to the previous question that I mentioned.

Let me just read Malign Influence Operations. What this ODNI report says, it says Beijing has adjusted by redoubling its efforts to build influence at the State and local level to shift U.S. policy in China's favor because of Beijing's belief that local officials are more pliable than their Federal counterparts. PRC actors have become more aggressive with their influence campaigns. It goes on to talk about—and I will enter this into the record—it goes on to talk about other tactics, techniques, and procedures.

Chairman PFLUGER. Ms. Murphy, you mentioned the work that the FBI has done on Confucius Institutes. I am proud to sponsor a bill and legislation that gets at the heart of Confucius Institutes. Do you believe that the CCP is using malign influence to affect outcomes of research and other academia outcomes at our universities?

Ms. MURPHY. Sir, so I don't know if I'd say it's to affect the outcomes, but probably more to steal the research.

Chairman PFLUGER. OK.

On May 12, 2023, Special Counsel John Durham submitted a 300-page report to Attorney General Garland examining the FBI's investigation into alleged links between the 2016 Trump campaign and Russian efforts to interfere in the Presidential election. Ms.

---

*The information has been retained in committee files and is also available at *https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf*.

Murphy, does your department deal with counterintelligence, specifically elections?

Ms. MURPHY. The Counterintelligence Division does, yes, sir. It works it along with another division that deals with election security.

Chairman PFLUGER. So your division deals with counterintelligence and has access to election security.

Ms. MURPHY. So election security isn't owned by the Counterintelligence Division. There's a specific part of the FBI that deals with election security, but we work with that piece of the FBI in regards to protecting elections and obviously with DHS.

Chairman PFLUGER. Special Counsel Durham assessed that neither U.S. law enforcement nor the Intelligence Committee appears to have possessed any actual evidence of collusion in their holdings at the commencement of the Crossfire Hurricane Investigation. The Bureau subsequently discounted or willfully ignored material that did not support the narrative of a collusive relationship between Trump and Russia.

As the deputy assistant director for the FBI's Counterintelligence Division, are you familiar with this report?

Ms. MURPHY. I have not read that report, sir.

Chairman PFLUGER. You have not read the Durham report?

Ms. MURPHY. I have not yet read the Durham report, no, sir.

Chairman PFLUGER. I am honestly speechless at this point in time. I am not sure what to think of this, as someone who has spent an entire career in counterintelligence. Special Counsel Durham found that the FBI moved too quickly with its investigation of the 2016 campaign and relied on uncorroborated evidence when launching its investigation. Does this concern you?

Ms. MURPHY. I'm sorry, can you repeat the question?

Chairman PFLUGER. That there was a very fast pace of the investigation and that uncorroborated evidence was used when launching the investigation. Does that concern you?

Ms. MURPHY. So, again, sir, I haven't read the Durham report, so I'm not sure—you know, I have no knowledge of——

Chairman PFLUGER. Does this fall under the counterintelligence umbrella?

Ms. MURPHY. The Durham Report? I'm sure portions of it do, yes, sir.

Chairman PFLUGER. Does a suggestion or an accusation of election collusion between a foreign government and the United States or a person or an entity in the United States fall under counterintelligence?

Ms. MURPHY. Yes, sir.

Chairman PFLUGER. So the alleged collusion between Mr. Trump in 2016 and Russia would have fallen under the Counterintelligence Division of the FBI?

Ms. MURPHY. Yes, sir.

Chairman PFLUGER. And you have not read the Durham report?

Ms. MURPHY. I have not read the Durham report.

Chairman PFLUGER. Is there a reason? Is it not required to——

Ms. MURPHY. No, I just haven't had time.

Chairman PFLUGER. Ms. Murphy, do you actively investigate counterintelligence with foreign entities around the world?

Ms. MURPHY. Yes, sir.

Chairman PFLUGER. This is a sincere question, does election collusion worry you?

Ms. MURPHY. Yes, obviously election collusion would worry me. Yes sir.

Chairman PFLUGER. Does any malign influence to the United States worry you?

Ms. MURPHY. Yes sir.

Chairman PFLUGER. OK. I would highly recommend reading that, because we spent 4 years discussing that there was uncorroborated evidence. The Durham Report specifically outlines the outcome of that. It is very disappointing to hear this and I think this is why we have these discussions and questions.

The Chair's time has expired and I now recognize the gentleman from New York, Mr. Goldman.

Mr. GOLDMAN. Thank you Mr. Chairman.

Perfect timing because I would like to address some of what the Chairman just addressed and some of what my colleague from Arizona addressed in attacking the FBI.

First, let's talk about the Durham report. I will make it real short for you Ms. Murphy. The Durham Report seemed to fail to consider the fact that the original tip that set off the Crossfire Hurricane Investigation was that Russia would be disseminating hacked emails about related—that would help Donald Trump. Lo and behold at the end of July that is exactly what happened. So the Durham Report focused solely on what was internally within the intelligence files of the FBI and did not mention the obvious corroboration that the tip turned out to be true.

Second, the Durham Report said that an investigation was justified to be opened. It should have just been a preliminary investigation as opposed to a full investigation.

Third, the Durham Report talks all about the Steele dossier, which had nothing to do with the origination of the Russia investigation and had nothing to do with the Mueller investigation. It was not relied on. That investigation of course led to, I believe, six individuals connected to the Trump campaign who were convicted, whereas the Durham Report, the Durham investigation, had one guilty plea by someone who was referred from the Office of Inspector General and two acquittals on pretty pathetic charges. So let's get our facts straight about the Durham Report.

Second, I want to address what my colleague from Arizona was saying about the FBI whistleblowers. I was actually in that hearing last week, he was not. What I can tell you about those individuals is separate and apart from whether they are whistleblowers or not, they were deemed by the FBI to be national security risks because one allowed his own personal views of January 6 to affect his official duties by not turning over to his superior open-source information that ultimately led a different agent to determine that a subject was actually at the Capitol committing violence on January 6.

Second, another one, another special agent decided that he was the legal expert on what a legitimate grand jury subpoena was and was not and refused to serve a grand jury subpoena on a witness that had been issued by the grand jury with the support of a Federal prosecutor and his supervisory agent. Yet he decided that he knew best and so he refused to do that.

My colleague wants to talk about being a partisan tool, I think is what he used. Sadly, and perhaps unwittingly, the partisan tool here is someone who is Donald Trump's henchmen funding these witnesses to try to diminish and undermine the FBI. Why are they trying to diminish and undermine the FBI at Donald Trump's direction and behest? Because the FBI is investigating Donald Trump. That is what we are doing here. That is why—and I see my colleague from Georgia, who I am sure is waved on to this committee——

Chairman PFLUGER. The committee will suspend.

I would advise Members that under Clause 1 of Rule 17 of the Rules of the House, they must observe the House standards of decorum and debate and conduct. They must act and speak respectfully and may not use disorderly words, unparliamentary language, such as words impugning the motives of their colleagues or words that are partially or personally offensive.

Yield back to the gentleman from New York.

Mr. GOLDMAN. Could I have my minute back, since you suspended?

Chairman PFLUGER. Yes.

The time was approximately 1 minute and 15 minute, 1 minute and 20.

Mr. GOLDMAN. Thank you. Appreciate it.

So why are my colleagues trying to undermine the FBI? Why are they asking to defund the FBI? It is not because the FBI is not doing its job, it is because the FBI is doing its job. The problem they have is that the FBI is doing its job in investigating their dear leader, Donald Trump. If you can undermine the investigator, if you can undermine independent journalists doing investigative reporting, then you can undermine our entire system of democracy. That is the authoritarian playbook 101, you attack the democratic institutions, you attack the independent, objective individuals who provide checks and balance in a democracy, and then, rather than follow the law and the rules, you can violate the law and the rules because there is no one with any credibility who can hold you in check.

So, do you want to know the reason why the FBI is going down in its credibility? It is because it is being attacked by people on the other side of the aisle. That has to stop.

I yield back.

Chairman PFLUGER. The Chair now recognizes the gentleman from North Carolina, Mr. Bishop.

Mr. BISHOP. Ms. Murphy, I also was surprised at your answer that you haven't read the Durham report. Do you consider the Durham report contents—or let me ask you this, have you been briefed on the report? That was a no. Your mic sounds like it is off. Was it working?

Ms. MURPHY. No, sir.

Mr. BISHOP. There we go. So you haven't been briefed on it. Have you read even the executive summary?

Ms. MURPHY. No, sir.

Mr. BISHOP. Here is a portion. Our investigation determined that the Crossfire Hurricane investigators did not and could not corroborate any of the substantive allegations contained in the Steele reporting, nor was Steele able to produce corroboration for any of the reported allegations even after being offered $1 million or more by the FBI for such corroboration. Further, when interviewed by the FBI in January 2017, Danchenko, he is the primary subsource, also was unable to corroborate any of the substantive allegations in the report. That is just a sample.

I know Mr. Goldman spent a good bit of time attempting to sort-of denigrate the Durham Report for understandable reasons. It is devastating to the FBI. That seems to me that that would be—and since it was a counterintelligence investigation that the Special Counsel appointed by the Department of Justice has summarized in terms like that, that that would be of grave concern to you as a deputy director of the FBI responsible for counterintelligence. Can you explain why—and you said you haven't had time to read it? It has been out since the 12th of this month, so almost, I guess—what is this, the 23rd—so 11 days. Mr. Goldman has obviously been briefed on and read it, many Members of Congress have. Why is that not a matter of such import that you would want urgently to understand what the Special Counsel concluded about the work of the Counterintelligence Division in such a grave case?

Ms. MURPHY. Sir, if you'd like a brief on the Durham Report from the Counterintelligence Division, I'm happy to take that back.

Mr. BISHOP. Wow. That sounds almost contemptuous.

Let me ask you this, then. Just go back to what you have written in your submitted testimony to this committee today. I was a little bit stuck on the first round of questioning, but let me just go back to it. It is your testimony—let me begin at the end of photograph or the third page of your testimony. This was talking about malign influence. Again, I think you said that you don't really have much responsibility for that, but surely you must know the details behind this. You said utilizing lessons learned since 2018, the FITF widened its aperture to confront malign foreign operations of the PRC, Iran, and other global adversaries. To address this expanding focus and wider set of adversaries and influence efforts, we have also added resources to maintain permanent surge capability on election and foreign influence threats.

Can you explain the details behind that, please.

Ms. MURPHY. Sir, I think when we're talking about surging resources, I think it's the permanent staffing of the Foreign Intelligence Task Force.

Mr. BISHOP. What is surge capability? That sounds like something that you can add people when you need it.

Ms. MURPHY. I think we did surge, and I think now we've made those positions permanent.

Mr. BISHOP. I see. So you have made—there is permanent surge capability. So if you ever need to surge, you got people permanently employed to do whatever you may need to interfere with the election.

How about—yes, that is just astonishing. I am just without words, that the FBI is unconcerned. Do you know whether anybody at the FBI has read the Durham Report?

Ms. MURPHY. I'm sure people have read the Durham Report, sir.

Mr. BISHOP. Can you name anybody that you know has read it?

Ms. MURPHY. No, sir.

Mr. BISHOP. Do you intend to read it?

Ms. MURPHY. I do intend to read it.

Mr. BISHOP. Does the FBI intend to undertake any changes in the way it conducts counterintelligence operations based on the Durham Report?

Ms. MURPHY. I can't answer that, sir. I can take that question back.

Mr. BISHOP. I yield.

Chairman PFLUGER. The gentleman yields.

The Chair now recognize the gentleman from Arizona, Mr. Crane.

Mr. CRANE. I am going to yield my time to the gentlewoman from Georgia.

Chairman PFLUGER. The gentleman yields to the gentlelady from Georgia, Ms. Taylor Greene.

Ms. GREENE. Thank you. I appreciate it. I appreciate you guys coming to speak to the committee today. Thank you very much for letting me wave on.

Just a few months ago, our Nation watched in absolute horror while a Chinese spy balloon traversed across the United States of America, spying on our military bases, our country's infrastructure, just surveilling everything that China could take in as it traveled across the United States. The Biden administration did absolutely nothing. Americans were so upset. The outrage was unbelievable.

Then finally, finally, the spy balloon gets shot down over the Atlantic after China completed its mission. Come to find out, after they picked up the pieces out of the ocean, that there—and they knew from pictures they were taking that this device was sending back images and information back to China. It is almost unspeakable. It is unspeakable that this actually happened.

In 2018, the Department of Justice announced the China Initiative to combat the CCP's relentless campaign to steal U.S. intelligence, technology, and cutting-edge research.

Ms. Murphy, I share my colleagues' shock that you haven't read the Durham Report, so I am not sure how much you know about the China Initiative. under President Trump's administration. But I think it was very important, as well do many Americans who feel threatened by China. China wants to replace us economically, and they are doing a pretty damn good job of it. China wants to beat us militarily, and they have the fastest-growing military in world history. So Americans that exist and live and pay all the taxes outside of this city truly feel threatened by China. We are greatly appreciative of the Trump administration that had the China Initiative.

In March 2022, even FBI Director Christopher Wray, who is loyal completely to the left and trying to go after their political enemies, admitted that the Bureau had more than 2,000 China-related cases and was opening a new China-related case every 12 hours. In spite of this, despite the clear need for a mission focusing on CCP threats, Assistant Attorney General Matthew Olsen ended the China Initiative based on accusations that the investigations under the initiative were excessive or racially biased.

Ms. Murphy, you have quite an extensive career, and I would think you would understand the threats that China poses to us. Do you agree with Attorney General Matthew Olsen ending the China initiative?

Ms. MURPHY. Thank you for the question.

I agree the threat from the Chinese Communist government is massive and something that we need to take very seriously in all levels of our Government and our private and public sectors. I think the China Initiative is something that was misperceived by our Chinese community to be against Chinese people. I think that concept behind the Chinese Initiative was to protect academic institutions and research from the Chinese Communist government. I think the things that we're doing to protect research in universities and innovation continues in that space. If people are doing criminal acts or grant fraud, then we're working with those institutions to take corrective action or criminal prosecution.

Ms. GREENE. Well, Ms. Murphy, protecting our national security and protecting our country from everything, protecting our intelligence, protecting our technology, protecting America's interests has nothing to do with anyone's race or any type of identity. The China Initiative wasn't any type of anything to go against Chinese Americans. This was all about fighting the CCP. So would you agree that this initiative needs to be put back in place?

Ms. MURPHY. I would say that the work that we're doing in that area continues.

Ms. GREENE. Well, I don't think it is good enough, because obviously, FBI Director for—Director Christopher Wray has admitted that more than 2,000 related cases have been opened. Now there is a China-related case every 12 hours. So I would say that you all are failing at your mission.

Chairman PFLUGER. The gentleman's time has expired.

Ms. GREENE. Yes. I yield back to Mr. Crane. Thank you.

Chairman PFLUGER. The gentleman's time has expired.

Mr. CRANE. I yield back.

Chairman PFLUGER. The Chair now recognizes Ms. Greene for her 5 minutes of questioning.

Ms. GREENE. Thank you, Mr. Chair.

I would like to continue talking about this Chinese spy balloon here for for just a minute. It is, it is truly shocking. Senior U.S. Government officials reported in February 2023 that the Chinese spy balloon was able to gather intelligence from several sensitive homeland defense sites resulting from the Biden administration's of course, willful refusal, shocking refusal, something that Americans just do not understand, can't comprehend, why it wasn't shot down. Given it is a proven fact that the Biden family has been receiving payments, from our oversight investigation, from CCP-linked foreign nationals in exchange for power and influence, this could very well be strategic sabotage by the CCP-basically-owned White House.

I would like to ask you, Mr. Kahangama, do you think that this is a national security threat against our homeland?

Mr. KAHANGAMA. Thank you for the question.

While I would defer some of the intelligence questions to my colleague in the intelligence community, I would say that the ability of the high-altitude balloon to conduct surveillance from the CCP perspective is a threat to our country.

Ms. GREENE. Right. But given the fact that we have seen money transferred from China into LLCs and then that money being paid out to multiple Biden family members, that is a clear—it actually puts our country at risk, our entire national security at risk when that is happening. That is proven in bank statements, it has been shown in financial reports that exist in the Treasury that we have reviewed. I think it is very serious.

What kinds of vulnerabilities to sensitive homeland security sites and critical infrastructure were likely created as a result of this intelligence breach.

Mr. KAHANGAMA. Thank you for the question, ma'am.

I would say the use of the high-altitude balloon is just one more tool, as I've mentioned earlier today, with regard to the CCP's toolbox, they use everything at their disposal, and a high-altitude balloon is just one more of them. It's also seen as perhaps a provocative action of theirs, the same way they are engaged in provocative activities in South China Sea and Taiwan Straits.

So with regard to the vulnerabilities, there's certainly some concern about the imagery that may have been collected or that's possible to be collected from such a balloon, over critical infrastructure, over military installations and such. But at this point, I'm not in a position to say any more about what those individual vulnerabilities are.

I would defer to my colleagues at the FBI, and specifically in DoD, who have oversight of the actual balloon and are engaging in the actual research and analysis of the tools that were on it.

Ms. GREENE. OK, well, Ms. Murphy, I would ask you then—I guess you are deferring to Ms. Murphy? Is that correct?

Mr. KAHANGAMA. Ma'am, not necessarily Ms. Murphy, but the other folks at the FBI who are working with element of DoD to provide some——

Ms. GREENE. All right, well, I will ask all three of you, since all of you receive taxpayer-funded paychecks, just like I do, how do you think the American people feel about a spy balloon going all the way across the country taking pictures of God knows what—the American people have no idea. They wanted it shot down, screamed for it shot down. So what do we have to say to the American taxpayers who work very hard for the money that they earn, pay the IRS their tax dollars that pay all of our paychecks, pay for this building, the lights that turn on, and all of the research and everything to do with this entire thing? I will go one at a time. What do you all have to say to the American people on that failure?

Ms. Murphy.

Ms. MURPHY. I'd say the FBI is working very hard to protect the American people.

Ms. GREENE. Do you think the American people trust the FBI, Ms. Murphy?

Ms. MURPHY. Yes, ma'am, I do.

Ms. GREENE. I am going to tell you they don't.

Sir.

Mr. KAHANGAMA. I would say that the high-altitude balloon posed a threat and it was shot down, and we are working with the investigative agencies to determine the specifics of that.

Ms. GREENE. Thank you.

Mr. DURHAM. Ma'am, I would say that the people at I&A, the analysts there are working diligently to ensure that we share any and all threat information with those individuals across the Nation who are in position to mitigate those threats.

Ms. GREENE. Well, the tragic news for our country is China has already collected everything they need and their mission was successful while our Government's mission failed the American people.

Mr. Chair, I yield back.

Chairman PFLUGER. The gentlelady's time has expired.

I would like to thank the witnesses for your time, for your service, for coming to this committee and talking about a very important issue.

Mr. BISHOP. Mr. Chairman, before you close, could I be recognized for unanimous consent request?

Chairman PFLUGER. Yes.

The Chair recognizes——

Mr. BISHOP. Just briefly. I am sorry, Mr. Chairman.

To submit for the record *New York Post* article, May 18, 2023, "Democrats attack FBI Whistleblowers—Giving Cover to the Agency's Abuses."

Thank you, Mr. Chair.

Chairman PFLUGER. So ordered. Thank you.

[The information follows:]

ARTICLE SUBMITTED FOR THE RECORD BY HONORABLE DAN BISHOP

DEMOCRATS ATTACK FBI WHISTLEBLOWERS—GIVING COVER TO THE AGENCY'S ABUSES

By James Bovard, Published May 18, 2023

Updated May 18, 2023, 9:57 p.m. ET

Congressional Democrats revealed a new Federal crime Thursday: having the same name as anyone who tweeted derisively about the Jan. 6 Capitol Clash.

Rep. Linda Sanchez (D–Calif.), vice chair of the House Equality Caucus championing LGBTQI+, sought to demolish FBI whistleblower Marcus Allen for retweeting a post asserting "Nancy Pelosi staged January 6."

When Allen repeatedly stated that wasn't his Twitter account, Sanchez berated him for interrupting her tirade.

After she finally seemed to admit it wasn't his account, she demanded to know if Allen agreed that Pelosi staged Jan. 6. Allen said no, and Sanchez's time expired.

This epitomizes how Congressional Democrats treated FBI whistleblowers in Thursday's House Weaponization of the Federal Government Subcommittee hearing.

Rep. Stacey Plaskett (D–Virgin Islands), the ranking Democrat, howled, "My colleagues on the far right are on a mission to attack, discredit and ultimately dismantle the FBI."

She claimed Republicans "have brought in these former agents, men who lost their security clearances because they were a threat to our national security—who out of malice or ignorance or both have put partisan agenda above the oath they swore to serve this country and protect its national security."

The Durham report this week exposed the FBI's brazen machinations to rig the 2016 election.

But all the FBI's sins have been expunged, at least for Team Biden supporters.

It was unclear Thursday whether Congressional Democrats consider FBI critics to be traitors or heretics or maybe both.

Allen, an FBI staff operations specialist who served two tours in Iraq with the Marines, was suspended without pay after the FBI condemned him for having "conspiratorial views in regards to the events of January 6th."

His crime? As part of his research task, he forwarded a link to an open website that said "Federal law enforcement had some degree of infiltration among the crowds gathered at the Capitol." (Which it did.)

But you can't blame Marcus Allen for the FBI's bizarre Boston bus dragnet.

FBI Washington Field Office pressured the FBI Boston office to open investigations on 138 bus passengers who traveled to DC Jan. 6, 2021, merely because "two individuals [on the buses] entered restricted areas of the Capitol that day."

Boston FBI officials responded by asking for video showing the wrongdoing, especially since there was no evidence the passengers had even entered the Capitol.

FBI Washington replied that it couldn't supply video because it might disclose undercover agents or confidential human sources in the crowd.

In lieu of providing evidence, FBI bosses wanted agents across the Nation to presume anyone who was suspected was automatically guilty.

Rep. Matt Gaetz declared, "Violence on January 6 doesn't justify weaponizing the government against people who were innocent and did nothing wrong."

FBI Special Agent Garret O'Boyle, a 101st Airborne Division member and veteran of the Iraq and Afghanistan wars, was suspended after he was compelled to divide a single domestic-terrorism case into "four different cases" to bolster the Biden narrative of a vast terrorist threat.

Boyle testified that FBI management "creates an Orwellian atmosphere that silences opposition and discussion."

A committee staff report declared that "the FBI appears to be complicit in artificially supporting the Administration's political narrative" that domestic violent extremism is "the 'greatest threat' facing the United States."

Another witness was Steve Friend, a 12-year FBI veteran and SWAT team member who was suspended without pay in September after complaining the FBI was falsifying data on domestic terrorism.

Friend lamented last year the leftist tilt of FBI management: "There is this belief that half the country are domestic terrorists and we can't have a conversation with them. There is a fundamental belief that unless you are voicing what we agree . . . you are the enemy."

FBI Assistant Director Christopher Dunham says Friend was suspended after he "downloaded documents from FBI computer systems to an unauthorized removable flash drive" and refused to participate in Jan. 6 cases.

Rep. Thomas Massie (R–Ky.) condemned Democrats for disparaging the witnesses.

Massie groused, "Big business is working with the government to weaponize against the American people."

He hammered Bank of America for sending the FBI a list of all its customers' charge or debit cards used in Washington between Jan. 5 and 7, 2021.

Massie complained that anyone who had ever purchased a firearm with a Bank of America card was "elevated to the top of the list"—even if the purchase occurred in Iowa in 1999.

The FBI denies retaliating against whistleblowers.

But O'Boyle bitterly declared, "The FBI will crush you . . . and your family, if you try to expose the truth about things they are doing that, are wrong."

O'Boyle told the committee: "I never swore an oath to the FBI. I swore my oath to the Constitution."

Perhaps someone should remind House Democrats that, likewise, their oath was to the Constitution and not to the FBI.

Unfortunately, the FBI can count on a vast Praetorian Guard on Capitol Hill to prevent Americans from learning how their rights and liberties have been trampled.

James Bovard is the author of 10 books and a member of the USA Today Board of Contributors.

Chairman PFLUGER. The Members of the subcommittee may have some additional questions for the witnesses, and we would ask the witnesses to respond in writing to these in a reasonable amount of time. Pursuant to committee rule VII(D), the hearing record will be open for an additional 10 days.

Without objection, this subcommittee stands adjourned.

[Whereupon, at 4:14 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN AUGUST PFLUGER FOR JILL M. MURPHY

Question 1. Mexican transnational criminal organizations are the main producers for U.S.-consumed illicit fentanyl, using PRC-sourced primary materials. The CCP has appeared to back away from cooperative agreements on counternarcotics issues with the United States after the U.S. Government took action to condemn the CCP genocide of Uyghurs in the Xinjiang Ugyhur Autonomous Region. Given the devastating toll illicit fentanyl is taking on Americans, what are you doing to mitigate the endless flow of this and other dangerous drugs into our country?

Answer. Response was not received at the time of publication.

Question 2. China has proven to be an adept and persistent threat to U.S. economic competitiveness, utilizing intellectual property theft, control over supply chain, and illicit trade to advance their goals in this space. Can you give specific examples of what the FBI and DHS are doing to directly counter threats to the U.S. economy emanating out of China?

Answer. Response was not received at the time of publication.

Question 3. The former director of the National Counterintelligence and Security Center, Bill Evanina, testified before this subcommittee in March that the theft of intellectual property by the PRC costs America as much as $500 billion a year. What are each of your agencies doing to mitigate the catastrophic impact of this theft?

Answer. Response was not received at the time of publication.

Question 4. Working in Washington DC, we are all too familiar with the "revolving door" concept. One issue we have seen as part of the CCP's influence campaign has been to create strategic business ties with people in high positions within Government and top connections in the business world. Can you talk about some of the main sectors of Government the CCP is trying to influence through this practice?

Answer. Response was not received at the time of publication.

Question 5. The CCP has taken advantage of our relaxed laws regarding public-sector officials entering the private sector—TikTok has been hiring former members of the U.S. intelligence community with significant intelligence backgrounds from the CIA, FBI, NSA, and even our military. What kind of threat does this pose to our own intelligence?

Answer. Response was not received at the time of publication.

Question 6. During the hearing on May 23, 2023, I asked how the Manhattan-based Chinese police station, operating as a provincial branch for the Ministry of Public Security (MPS)—an organization that belongs on the Commerce Entity List for its implication in human rights violations and abuses of Uyghurs, was founded on U.S. soil. You promised to respond to this question and others in our April 24th letter to DHS and FBI in a Classified setting. I resubmit this question now, with the expectation that you will fulfill your promise to provide the answer in a Classified setting in a timely manner.

Answer. Response was not received at the time of publication.

Question 7. According to the USDA, the estimated value of U.S. farmland owned by entities in the PRC, jumped more than 20-fold in a decade, from $81 million in 2010 to nearly $1.9 billion in 2021. Moreover, Chinese companies appear to be strategically buying land near sensitive military sites across the United States. What is your assessment of the counterintelligence threat of these purchases by China and other foreign adversaries?

Answer. Response was not received at the time of publication.

Question 8. In 2018, the Department of Justice announced the China Initiative to combat the CCP's relentless campaign to steal U.S. secrets, technology, and cutting-edge research. In March 2022, FBI Director Christopher Wray said the bureau had more than 2,000 China-related cases and was opening a new China-related case every 12 hours. Despite this clear need for a mission focusing on CCP threats, the

Department of Justice ended the initiative in favor of a broader approach to countering nation-state threats, despite that the People's Republic of China in particular poses serious and persistent threats to U.S. national security interests. By the Department of Justice scuttling its China Initiative, do you agree that it can send the wrong message to FBI field agents that the Department of Justice no longer prioritizes threats from China?

Answer. Response was not received at the time of publication.

Question 9. On May 12, 2023, Special Counsel John Durham released a report on Matters Related to Intelligence Activities and Investigations Arising out of the 2016 Presidential Campaigns. Special Counsel Durham found that the FBI moved too quickly with its investigation of Trump's 2016 campaign and relied on uncorroborated evidence when launching its investigation. Given the significant resources and scale of that investigation, how much ground was lost detecting real-world threats such as those posed by the CCP against the United States while the FBI was preoccupied with the investigation of the Trump campaign?

Answer. Response was not received at the time of publication.

Question 10. At the hearing, I asked you whether you read Special Counsel Durham's report in which you responded that you "haven't had time." Since the hearing, have you now familiarized yourself with the report and the report's findings involving matters related to the FBI's counterintelligence division?

Answer. Response was not received at the time of publication.

Question 11. Special Counsel Durham found that an "objective and honest assessment" of the evidence "should have caused the FBI to question not only the predication for [the investigation] Crossfire Hurricane, but also to reflect on whether the FBI was being manipulated for political or other purposes. Unfortunately, it did not."[1] Do you have any reason to disagree with the Special Counsel's finding?

Answer. Response was not received at the time of publication.

Question 12. Special Counsel Durham found that "the matter was opened as a full investigation without ever having spoken to the persons who provided the information," and the FBI launched the investigation without "any significant review of its own intelligence databases,"[2] as well as without "collection and examination of any relevant intelligence from other U.S. intelligence entities." Moreover, the FBI's investigation began without conducting any interviews of "witnesses essential to understand the raw information," that the Bureau had obtained, and without using "any of the standard analytical tools typically employed by the FBI in evaluating raw intelligence."[3] First, do you have any reason to disagree with the Special Counsel's findings? Second, as the deputy assistant director of counterintelligence at the FBI, do these findings concern you?

Answer. Response was not received at the time of publication.

Question 13. Special Counsel Durham concluded that the FBI "failed to uphold their mission of strict fidelity to the law."[4] First, would you agree that the FBI's conduct in this matter was improper and should never have happened? Second, as the deputy assistant director of counterintelligence at the FBI, will you commit to assuring us that going forward the FBI is not going to busy itself pursuing politically-motivated investigations?

Answer. Response was not received at the time of publication.

Questions From Chairman August Pfluger for Iranga Kahangama

Question 1. Mexican transnational criminal organizations are the main producers for U.S.-consumed illicit fentanyl, using PRC-sourced primary materials. The CCP has appeared to back away from cooperative agreements on counternarcotics issues with the United States after the U.S. Government took action to condemn the CCP genocide of Uyghurs in the Xinjiang Ugyhur Autonomous Region. Given the devastating toll illicit fentanyl is taking on Americans, what are you doing to mitigate the endless flow of this and other dangerous drugs into our country?

Answer. Response was not received at the time of publication.

Question 2. China has proven to be an adept and persistent threat to U.S. economic competitiveness, utilizing intellectual property theft, control over supply chain, and illicit trade to advance their goals in this space. Can you give specific examples of what the FBI and DHS are doing to directly counter threats to the U.S. economy emanating out of China?

---

[1] Special Counsel John Durham, *Report on Matters Related to Intelligence Activities and Investigations Arising out of the 2016 Presidential Campaigns* at 305 (May 12, 2023).
[2] Id. at 9.
[3] Id.
[4] Id. at 17.

Answer. Response was not received at the time of publication.

Question 3. The former director of the National Counterintelligence and Security Center, Bill Evanina, testified before this subcommittee in March that the theft of intellectual property by the PRC costs America as much as $500 billion a year. What are each of your agencies doing to mitigate the catastrophic impact of this theft?

Answer. Response was not received at the time of publication.

Question 4. DHS Secretary Mayorkas announced the "90-Day sprint" to focus resources on China, which is long overdue. Given that Chinese leadership openly views the United States as an adversary and for decades has utilized the weight of its civilian research and commercial sectors, along with the military and defense industrial sectors, to gain every available advantage over U.S. competition, can you please explain how a "90-Day sprint" is going to manifest into something more permanent to truly counter these determined and unrelenting efforts?

Answer. Response was not received at the time of publication.

Question 5. The CCP continues to exploit vulnerabilities in American academic society to exploit U.S. research and development, especially through Confucius Institutes. While most of the original Confucius Institutes at American campuses have been shuttered as the U.S. Government has started to take action against them, similar programs simply called by a new name have replaced them. Moreover, many American universities retain relationships with Chinese universities that support the CCP strategy of Military-Civil Fusion. What action is DHS taking to counter this new wave of Confucius Institutes and Chinese universities and the counterintelligence threat posed to American academic research and development?

Answer. Response was not received at the time of publication.

Question 6. China poses a major cyber-espionage threat with the capability to cause major disruption to the U.S. homeland's critical infrastructure. Given the reality that the Chinese may unleash these capabilities in a future conflict over Taiwan, the South China Sea, or other disputes, what is your office doing to prepare our critical infrastructure to withstand such a cyber attack?

Answer. Response was not received at the time of publication.

Question 7. The CCP has weaponized technology to access sensitive commercial and Government data in the U.S. homeland through companies like Tik Tok and DJI drones. Under the 2019 Chinese National Intelligence Law, all Chinese organizations and citizens are required to support, assist, and cooperate with state intelligence work. What is being done to counter this threat given that many Americans from our youth to even police departments utilize these platforms, often unaware of the potential espionage threat to data that presents?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE DINA TITUS FOR IRANGA KAHANGAMA

Question 1. Secretary Mayorkas' "90-Day PRC threats sprint" requires reports from various DHS departments on the threats posed by China. Can you please tell us what you anticipate DHS will elicit from this report? What kinds of actionable steps are we going to see from this "Sprint"? Will reports on findings across DHS be available to Members of Congress so we can help determine how we are best positioned to help this effort?

Answer. Response was not received at the time of publication.

Question 2. Reports over the last several months have found that despite import restrictions put in place by Congress (the Uyghur Forced Labor Prevention Act), certain Chinese e-commerce companies may be exporting apparel to the United States that contains cotton from the Xinjiang Uyghur Autonomous Region. The CBP executive assistant commissioner, who oversees the Office of Trade, has said that: "[DHS's] goal for the forced labor laws [is] to prevent merchandise from being made with forced labor in the first place, and we will not rest until we achieve that goal." What is DHS doing, beyond just screening goods, that will help the United States achieve this broader goal, as stated by CBP's executive assistant commissioner?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN AUGUST PFLUGER FOR TYRONE DURHAM

Question 1. Mexican transnational criminal organizations are the main producers for U.S.-consumed illicit fentanyl, using PRC-sourced primary materials. The CCP has appeared to back away from cooperative agreements on counternarcotics issues with the United States after the U.S. Government took action to condemn the CCP genocide of Uyghurs in the Xinjiang Ugyhur Autonomous Region. Given the devastating toll illicit fentanyl is taking on Americans, what are you doing to mitigate the endless flow of this and other dangerous drugs into our country?

Answer. Response was not received at the time of publication.

Question 2. China has proven to be an adept and persistent threat to U.S. economic competitiveness, utilizing intellectual property theft, control over supply chain, and illicit trade to advance their goals in this space. Can you give specific examples of what the FBI and DHS are doing to directly counter threats to the U.S. economy emanating out of China?

Answer. Response was not received at the time of publication.

Question 3. The former director of the National Counterintelligence and Security Center, Bill Evanina, testified before this subcommittee in March that the theft of intellectual property by the PRC costs America as much as $500 billion a year. What are each of your agencies doing to mitigate the catastrophic impact of this theft?

Answer. Response was not received at the time of publication.

Question 4. Southwest Border crossings by Chinese nationals numbered 430 in Oct. 2022, 1,400 in Feb. 2023, and 3,200 in April 2023. Traditionally, discussions on Southwest Border security have focused on incoming Mexican and Central American nationals. Can you tell the committee why border crossings by Chinese nationals have surged specifically during the last 2 months?

Answer. Response was not received at the time of publication.

Question 5. There has been recent reporting about the increase in quality and quantity of luxury counterfeit products such as "superfake" handbags, many of which come from China, becoming a pervasive and costly problem for the high-end U.S. retail industry. Is the Nation State Threats Center engaged on this problem, and if so, what is being done?

Answer. Response was not received at the time of publication.

Question 6. The CCP has forcibly detained more than 1 million ethnic Uyghurs in reeducation camps, and an estimated 100,000 Uyghurs are said to be working in forced labor conditions, making goods that are sold across the global economy for artificially low prices. Apart from the inhumane and exploitative practices, forced labor places legitimate manufacturers at a competitive disadvantage. What is DHS doing to ensure our American companies are competing on an even playing field?

Answer. Response was not received at the time of publication.

Question 7. The COVID–19 pandemic highlighted risks to American economic prosperity in a globalized system that is dependent on the People's Republic of China (PRC). There were months-long shortages for goods including personal protective equipment and critical minerals. Can you speak about what DHS is doing to ensure that supply chains are stable and protected for critical items and resources going forward?

Answer. Response was not received at the time of publication.

Question 8. According to the USDA, the estimated value of U.S. farmland owned by entities in the PRC, jumped more than 20-fold in a decade, from $81 million in 2010 to nearly $1.9 billion in 2021. Aside from the potential counterintelligence threat these land purchases present, PRC acquisitions of U.S. farmland have raised serious concerns for American food supply chains and water usage. Is this something DHS is engaged in?

Answer. Response was not received at the time of publication.

Question From Honorable Dina Titus for Tyrone Durham

Question. Reports over the last several months have found that despite import restrictions put in place by Congress (the Uyghur Forced Labor Prevention Act), certain Chinese e-commerce companies may be exporting apparel to the United States that contains cotton from the Xinjiang Uyghur Autonomous Region. The CBP executive assistant commissioner, who oversees the Office of Trade, has said that: "[DHS's] goal for the forced labor laws [is] to prevent merchandise from being made with forced labor in the first place, and we will not rest until we achieve that goal." What is DHS doing, beyond just screening goods, that will help the United States achieve this broader goal, as stated by CBP's executive assistant commissioner?

Answer. Response was not received at the time of publication.

○