Thomas S. Warrick
Atlantic Council Senior Fellow and Director, Future of DHS Project
October 25, 2023, "An Examination of the Iranian Regime's Threats to Homeland Security"

Mr. Chairman, Ranking Member Thompson, members of the House Committee on Homeland Security, thank you for the honor to testify today on the Iranian regime's threats to homeland security. I have forty years' experience addressing challenges from Iran, starting in the private sector in 1981 with the Iran-U.S. Claims Tribunal and the aftermath of the Iran hostage crisis. I served ten years at the U.S. State Department, including working to counter Iranian influence. I served more than eleven years at the Department of Homeland Security (DHS), most of that as Deputy Assistant Secretary for Counterterrorism Policy, where countering the Iranian regime's actions as the leading state-sponsor of terrorism was one of our foremost counterterrorism priorities. For a time, I was DHS's senior-most Iran expert. I am proud to have served under four presidents of both parties. Today, I'm a senior fellow at the Atlantic Council and director of the Future of DHS Project, working on a number of initiatives to strengthen the Department of Homeland Security. I co-lead our Counterterrorism Study Group and am the convener of the Experts' Coalition on Borders, Immigration, and Trade. Our work supports the extraordinary efforts of the men and women of DHS and throughout the homeland security enterprise to keep our country safe.

How We Should Address Iran's Threat to the United States

I'm going to summarize the threats that the Iranian regime poses to the United States homeland, but first, I would make two short points. The Hamas terrorist attack on October 7 ranks among the world's worst terrorist attacks in modern history. In addition to the more than 1,400 Israelis killed, at least thirty-one American citizen deaths make this one of the worst terrorist attacks against Americans since the Pulse nightclub attack in Orlando, Florida, in 2016. American resolve, as shown by the President's and the Congress's bipartisan support for Israel, and President Biden's deployment of two aircraft carrier battle groups to the eastern Mediterranean, are an essential response to this terrorist attack and a warning to Iran and Lebanese Hizballah. Americans have a stake in what will come after Hamas's military defeat. The United States is already in discussions with the Israelis and other allies over the future of Gaza, to ensure these terrorist attacks do not repeat in a few years—and to ensure that Iran does not determine the future of Gaza. There is a role for our homeland security agencies in supporting this. But Iran's role in funding, arming, equipping, and helping train Hamas terrorists is something that our government must, and will, address. Iran'

Second, today's hearing takes place against the background of unprecedented efforts by the Iranian people, women and men, to fight for greater freedoms and justice against the current Iranian regime. We should acknowledge the historic importance of this struggle, which is led by Iranians and should have the support of all Americans. The Iranian regime has chosen to make the United States an adversary. The Iranian people want to make different choices.

Turning back to the subject of this hearing, I want to leave you with four important points.

First, Iran poses a threat to the security of the United States, including here in the homeland. We should not think of Iran as a purely Middle Eastern security challenge. That's why today's hearing is important. The phrase "great power competition" is the organizing principle for our national security agencies, but it has its limits. While China and Russia are "great powers," and they *do* pose the greatest challenges to American security, Iran is not a great power but is nevertheless a serious challenge, and not just because of its nuclear program and its threat to overseas American allies like Israel and our Arab partners. **Iran and its proxies are currently carrying out a campaign of hybrid warfare against the United States and our allies.** I'm not the only one saying this: the Director of National Intelligence likewise warned of Iran's hybrid approach to warfare in the 2023 Annual Threat Assessment.

This requires vigilance here at home, including from the private sector. North Korea is a challenge, too, but Iran poses a unique, multi-dimensional threat that requires us to think in 3-D technicolor, not just two-dimensional black and white. Given that chess originated in Iran, I've often heard the criticism that the United States plays checkers while the Iranian regime plays chess. Now is the time for the United States and our allies to start playing three-dimensional chess.

Second, we need to address the threat from the Iranian regime on a sustained, bipartisan basis. We will not succeed with a policy that changes radically if the White House or the Congress changes. A consistent, sustained, bipartisan response is how the United States won the Cold War. It took the United States decades of sustained, bipartisan effort, working with U.S. allies around the world, and including efforts both at home and abroad, to win the Cold War without a hot war with the Soviet Union. We are approaching the challenge from China today with a similar bipartisan approach, including some excellent work here in the Congress. We need to build a sustainable, bipartisan strategy to address the threat from the Iranian regime. We need to play defense by protecting the homeland, including American citizens and the private sector, from Iran's destabilizing actions. Both protecting Americans at home and turning Iran away from its destabilizing ambitions and its state-sponsorship of terrorism will require a sustained, bipartisan effort, working with U.S. allies, and with an eye towards strengthening security, including in the private sector.

Third, one of the lessons the United States needs to embrace after October 7 is that strategic surprise is still possible. Even the State of Israel, with all its focus, technology, and capabilities, was surprised by Hamas's attack on October 7. The so-called "Iron Wall" between Israel and Gaza did not protect Israel's citizens from the October 7 attack. What happened on October 7 is well past any effort to analogize it to 9/11 or Pearl Harbor. The United States is thirty-five times the size of Israel. ***On a proportional basis, the number of Israelis killed on October 7 is more than half the number of Americans killed during the whole of the Vietnam War***—and Israel suffered most of those deaths in a single day. The Iron Wall was not enough—we should learn that lesson, too. Today in the homeland security enterprise, every watch and warning officer, and every strategic planner in the U.S. government, should be using red cells to look for vulnerabilities, including those we have not focused on. The Iranian regime is precisely the kind of threat that deserves this attention, especially in the areas of cybersecurity and countering Iranian disinformation. I will have more to say about these points below.

Fourth, I urge this committee to understand Iran's peculiar sense of symmetry. Understanding Iran is a challenge, but Iran is far from incomprehensible. Eighty-four years ago this month, Winston Churchill famously described the Soviet Union as "a riddle, wrapped in a mystery, inside an enigma." What everyone forgets are his next words: "Perhaps there is a key. That key is Russian national interest." Churchill was one of the most clear-eyed leaders in history about the Soviet Union. We need to be equally clear-eyed about the Iranian regime. The Iranian regime is not ten feet tall, and the Iranian Islamic Revolutionary Guards Corps' Qods Force, while dangerous and committed, is not lurking behind every tree.

Instead, we need to understand **Iran's peculiar sense of symmetry.** Let me give several examples. The day after the January 2, 2020 strike that killed Qasim Soleimani, Iran's Supreme Leader Ali Khamene'i gave his Supreme National Security Council a written order to "strike America directly and in exact proportion to the attack," two sources told the New York Times. Other Iranian military leaders made similar statements. In May 2018, when the United States started a "maximum pressure" campaign to reduce Iran's oil exports, which Iran considered economic warfare, Iran showed it could reduce U.S. allies' ability to export oil, first in May and June with attacks on tankers and a Saudi pipeline, then with the September 14, 2019 Abqaiq attack that halved Saudi oil exports.

Iran's sense of symmetry is more pronounced in cyberspace. After the "Stuxnet" malware that targeted Iran's Siemens industrial control systems came to light in June 2010, Iran developed its own cyberattack capability that it used in 2013, three years later, to target U.S. infrastructure. On July 30, 2012, new U.S. sanctions targeted Iranian banks. Two months later, Iran ramped up denial of service attacks, whose main targets were—US banks. In August 2012, Iran's surprise "Shamoon" attack deleted 35,000 hard drives at Saudi Aramco, described as "the biggest hack in history." What got less publicity is that in early 2012, "Wiper" malware deleted data on Iranian Oil Ministry and National Iranian Oil Company computers.

The symmetry can be positive and negative: When the Iran nuclear deal was in force, Iranian cyberattacks appeared to decrease. When the Trump Administration began its 2018 "maximum pressure" campaign, Iranian cyberattacks increased within 24 hours. On June 20, 2018, after Iranian attacks on civilian tankers, President Trump retaliated by cyberattack. Private U.S. businesses noticed a further increase in Iranian cyberattacks.

And while the United States supports the cause of human rights and freedom in Iran, we cannot be surprised when the Iranian regime thinks this gives it a license to try to interfere in democratic processes here in the United States. There is, of course, absolutely no moral equivalency in the two situations—none. But the Iranian regime does not think this way, so we need to be prepared. We should not be deterred from pursuing what is right. One essential part of the response to Iran's peculiar sense of symmetry is that we must raise our defenses to the level where the Iranian regime's efforts to target our security, and especially our democratic processes, all fail.

This list could go on. But while Iran and its proxies are capable of tactical surprise, as Hamas achieved on October 7, it is possible for the United States and our allies to put in place defensive measures to protect the American people, and to help our allies, from the threats that Iran poses. Later I will discuss several specific steps Congress can take to help this.

The Iranian Regime's Threats to the United States Homeland

Let me briefly categorize the most significant threats from the Iranian regime towards the U.S. homeland.

1. **Targeted assassinations and terrorist attacks in the United States homeland, and plots to kill or kidnap Americans here or overseas.** The Iranian regime is responsible for plots to kill or kidnap American citizens who are critics of the regime, and against former American officials. There is every reason to expect such plots to continue. Disrupting these plots will require continued vigilance from the Federal Bureau of Investigations (FBI), which has the lead in disrupting such plots. Other parts of the U.S. intelligence and law enforcement communities also play vital roles.

   Cooperation among U.S. law enforcement agencies has proven extraordinarily effective in disrupting these plots. For example, in 2011, an extremely small number of IRGC Qods Force (IRGC-QF) officers tried to use Mansour Arbabsiar to assassinate Saudi Arabian ambassador Adel Al-Jubeir in a Washington restaurant. The plot was uncovered by agents of the Drug Enforcement Administration. The advance passenger information systems by which Arbabsiar's travel was tracked were developed by the Department of Homeland Security's Customs and Border Protection. Arbabsiar was arrested by the FBI when his flight between Mexico City and Amsterdam landed at New York's John F. Kennedy airport. Arbabsiar pled guilty and cooperated with authorities in helping obtain evidence against other IRGC officers involved in the plot. He is now serving a 25-year sentence in Federal prison in Marion, Illinois. Cooperation among our law enforcement and homeland security agencies has proved successful at uncovering plots by Iran and its proxies.

   In a more recent example, a U.S. citizen in California, four Iranian regime operatives, and an Eastern Europe criminal syndicate were charged with attempts to kidnap and kill an American citizen who was publicly critical of the regime's human rights abuses. This resulted in a guilty plea on material support charges for the one accused who was here in the United States and the arrest of three members of the Eastern European crime syndicate. Others are still wanted for their role in these plots.

   Iran's proxies Hamas and Lebanese Hizballah are also trying to build up a presence here in the United States. Here, again, cooperation among U.S., state, and local law enforcement has proved effective in uncovering and disrupting such plots. Continued vigilance will be essential.

2. **Cyber-threats from Iran are certain, and ongoing.** The Office of the Director of National Intelligence said in its 2023 threat assessment that "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data. Iran's opportunistic approach to cyber attacks makes critical infrastructure owners in the United States susceptible to being targeted…." This is an area where Iran could pull off a strategic surprise. Of particular concern is Iran's willingness to target U.S. private sector entities. Today, most government systems are better defended, as are the major firms that form the backbone of America's digital economy. But the companies that are the "fingers" and "toes" are not as well protected. The March 2023 National

Cybersecurity Strategy will help when it is fully implemented. However, since so much of the nation's critical cyber infrastructure is in the hands of the private sector, we need, as a nation, to ask if we are adequately invested in cybersecurity.

3. **Iranian disinformation operations pose an increasing challenge.** This is an area where Iran could pull off a strategic surprise. Early Iranian disinformation efforts were clumsy, but their attempt to exploit racial polarization in Florida in the 2020 election showed a significantly greater sophistication than before. I am not as concerned about actual Iranian threats to voting infrastructure, but Iranian disinformation efforts in the runup to the 2024 election are worth our attention in order to ensure that they get exposed and disrupted.

Seven Steps the United States Congress Can Take

Let me close with seven ways in which Congress can help strengthen America's defenses against today's multi-dimensional threat from Iran.

1. **Work towards a bipartisan consensus to address the Iranian threat** both at home and abroad.

2. **Focus on the most significant urgent threats, starting with increasing cybersecurity in the private sector.** The governmental security partner for most private sector firms in the United States is the DHS Cybersecurity and Infrastructure Security Agency (CISA). In 2021, John Katko, then the ranking Republican on this committee, said the Cybersecurity and Infrastructure Security Agency should play quarterback for cybersecurity, and should be funded like one. He called for CISA to become a $5 billion agency in five years. CISA is now funded at half that level. While we focus, rightly, on specific cyber threats like ransomware and the potential for nation states like China and Iran to carry out cyberattacks against critical infrastructure, we are not engaging in the debate as to whether we as a country are devoting the right level of resources to cybersecurity, both the levels of private sector and governmental spending. Governmental spending on cybersecurity may be the purview of the appropriations committees, but encouraging the private sector to do more to protect computer systems from Iranian and other hostile attacks is something that this committee should continue to urge as an urgent matter.

3. **Renew the authorization of DHS's Countering Weapons of Mass Destruction office.** This office does vital work in coordinating training and the procurement of equipment to prevent low-probability, high-impact attacks using weapons of mass destruction. I do not need to remind this committee that Iran is one of the few countries in the world that has actually used chemical weapons, during the Iran-Iraq war in the 1980s. Iran's nuclear ambitions are well past the level of technology required to build dirty bombs—conventional explosives with radiation enhancements. DHS needs the CWMD office re-authorized, and it also needs an authorized Office of Health Security. I know this committee has done its job and the bill is now held up in the Senate, I believe by a single Senator. I urge this committee to engage to break the logjam and send a bipartisan reauthorization bill to the President right away.

4. **Renew Foreign Intelligence Surveillance Act section 702 with changes.** As my former government colleague Jon Darby, former director of operations at the National Security

Agency, and I wrote in The Hill in September, "We can unequivocally state that Section 702 is the most timely, impactful, and cost-effective authority to obtain foreign intelligence on terrorists, spies, weapons proliferators, cyber attackers and nation-states that pose threats to the United States and our allies. History will judge us harshly if we unilaterally give up an important intelligence advantage against those who are trying to harm us." I understand some in Congress have concerns, particularly over past FBI practices, and these do need to be addressed, but without requiring a judge to be sitting at the elbow of every government analyst working on national security cases. Given the threats we face from Iran and elsewhere, we cannot let the vital authority of section 702 lapse at the end of this year. This is the wrong time for Congress to be sending the message said in 1929, "Gentlemen do not read each other's mail."

5. **Enact the House language in the Intelligence Authorization Act on the collection authority of DHS's Office of Intelligence and Analysis (I&A).** Section 435 of H.R. 3932 calls for an assessment by the Inspector General of the Intelligence Community on the collection authority of DHS I&A. It is particularly concerning that the comparable Senate language prohibits DHS I&A from doing any collection whatsoever. It is true that DHS I&A needs to be particularly conscious about respecting boundaries so that its actions do not infringe on Americans' constitutional rights to free speech and the right to counsel, and I believe that Under Secretary Ken Wainstein agrees with this principle. But to deny I&A any ability to collect information relevant to border smuggling and trafficking, for example, goes farther than it should. When this language comes to conference between the House and the Senate, the House should stand firm on this particular issue.

6. **Extend authorities to counter unmanned aerial systems (UAS).** Congress needs to ensure that Federal counter-UAS authorities, which were extended in the continuing resolution, do not lapse at the end of this year. Drones were precisely one of the technologies that Hamas used to deadly effect against the Israeli Iron Wall in Gaza. This committee should be concerned about what Iranian operatives or Iranian proxies might try to do with unmanned aerial systems here in the United States. It is vital for the security of the homeland that Congress and the administration resolve the competing versions of this bill before counter-UAS authorities lapse at the end of the year.

7. **Renew the Chemical Facility Anti-Terrorism Standards (CFATS) program,** which expired on July 28, 2023. This important program gives DHS the authority to enforce security standards for the nation's chemical plants, to make it harder for terrorists to get access to those facilities. Here again, the House has done its work in passing a bipartisan bill, and there is a bipartisan bill in the Senate that is being held up, I believe by a single Senator. I urge this committee to engage to break the logjam and send a bipartisan reauthorization bill to the President right away.

Mr. Chairman, I thank you and the committee for your time and look forward to answering your questions.