Statement by

Ms. Melissa Dalton

Assistant Secretary of Defense for

Homeland Defense and Hemispheric Affairs

Office of the Secretary of Defense

Before the 117th Congress

Committee on Armed Services

U.S. House of Representatives

March 8, 2022

Introduction

Chairman Smith, Ranking Member Rogers, and distinguished Members of the Committee: Thank you for the opportunity to testify before you today.

As the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs, I am the principal civilian policy advisor to the Secretary of Defense and the Under Secretary of Defense for Policy on a range of matters, including homeland defense, mission assurance, defense support of civil authorities, Western Hemisphere affairs, and the Arctic and global resilience.

The Office of the Under Secretary of Defense for Policy produces guidance for the Department of Defense (DoD), including the Combatant Commands, to align resources, activities, and capabilities in support of National Security Strategy and National Defense Strategy goals. This includes developing force posture policy and strategy and overseeing implementation.

Today, I would like to emphasize two key points after briefly assessing the array of national security challenges to the homeland. First, DoD is working to understand, raise awareness of, and energize attention and preparedness to prevent, mitigate, and respond to national security threats to the homeland, namely from state-based strategic competitors. Second, to address and build resilience against these threats, DoD is reviewing, renewing, and modernizing our approach to partnerships in DoD's homeland defense missions, both within DoD and with other Federal departments and agencies; international allies and partners; State, Local, Tribal, and Territorial Governments (SLTT); and private sector partners.

National Security Challenges

Today we face a rapidly evolving array of adversary military capabilities, exacerbated by emerging technologies that pose intensified threats to the U.S. homeland. As the Interim National Security Strategic Guidance makes clear, the United States faces challenges from state and non-state adversaries that target the homeland, including our elections, intellectual property and technology, and infrastructure, through malicious cyberattacks and disinformation

campaigns, as well as naturally occurring hazards like climate change and infectious disease. These threats and challenges can put at risk the Department's ability to defend the homeland, project power, and counter aggression.

People's Republic of China (PRC) and Russia: The PRC is the pacing challenge for the Department. Largely through its ongoing program of licit and illicit acquisition of others' technology, the PRC is rapidly advancing and integrating its capabilities, which could allow the PRC to hold our homeland at risk in multiple domains and to disrupt our ability to mobilize, project, and sustain the joint force. Russia poses an acute challenge to the United States and our allies and partners. Russia has carried out a multiyear influence operation campaign aimed at exacerbating societal divisions in the United States to weaken our democracy. Russia's decision to undertake an unprovoked, unjustified, and premeditated further invasion of Ukraine has already resulted in loss of life and human suffering, threatens global peace and security, and constitutes a threat to the national security and foreign policy of the United States.

Other Persistent State Threats: Regional rogue regimes like Iran and the Democractic People's Republic of Korea (DPRK) continue to pose distinct, persistent challenges as both pursue game-changing capabilities at the expense of the welfare of their own people. Iran has attempted to execute influence campaigns in the homeland, including during the 2020 U.S. Presidential Election. DPRK focuses its malicious activity on exploiting international financial systems to steal money, allowing it to evade United Nations sanctions.

Cyber: The United States faces cyber threats from China, Russia, Iran, DPRK, their proxies, and non-state actors, including cyber criminals, all of which carry out operations daily against the United States, including targets at all levels of government and private entities. China and Russia are among our most sophisticated cyber competitors and conduct persistent malicious cyber campaigns to threaten U.S. strategic interests. Their malicious campaigns include exfiltrating sensitive information from U.S. public and private sector institutions to erode the Nation's economic vitality. And Russia has conducted cyber-enabled information operations that challenge our democratic processes. Over the past three election cycles, Russia, Iran, and other

countries sought to undermine U.S. voter confidence and promote the strategic interests of those countries.

Further, China and Russia are both adept at carrying out cyber espionage and other operations and have integrated cyber activities into their military and national strategies. As we are witnessing in Ukraine, Russia is employing its cyber capabilities prior to, and in conjunction with, its ground invasion to target online services at the Ukrainian Ministry of Defense, state-owned banks, and other entities. Iran has demonstrated the capability and intent to target the United States in cyberspace, and Iranian cyber actors are improving their ability to deliver disruptive and destructive attacks.

Cyber criminals are employing ever more sophisticated capabilities and tactics to extort, steal, or otherwise advance their malicious aims. Ransomware attacks, in particular, are increasing in both scope and sophistication as malicious actors experiment with new business models, such as the provision of ransomware infrastructure as a service that can be bought or leased. Last October, President Biden hosted ministers and representatives from the European Union and more than 30 countries who recognized that ransomware is an escalating global threat with serious economic and security consequences. Thus, the Department is working with other Federal departments and agencies to prepare to respond to cyber operations against a wide range of U.S. targets, including critical infrastructure.

Central and South America: The Western Hemisphere's relative stability can be maintained only by building strong, robust defense and security relationships with partners and allies in the region, both physically and in cyberspace. We know too well that competitors from outside the hemisphere seek to foster instability and to interfere with democracy in this region. We also know that transnational criminal organizations and other illicit actors in this hemisphere enable corruption, undermine the rule of law, and erode democratic institutions, at the expense of the health, safety, and well-being of the people of North and South America.

Natural and Man-made Hazards and Resilience: Concurrent with these national security challenges, our nation also faces the challenge of natural and man-made hazards. These

hazards do not respect international or national boundaries in our increasingly interconnected world, nor do these hazards wait for ongoing crises to be resolved before striking. Last year, the U.S. homeland endured 58 major disasters caused by natural hazards, including hurricanes, wildfires, and flooding. Over the last two years, the outbreak of a global pandemic has claimed the lives of more than 936,000 Americans. We are also seeing increasing demands on the force to provide support to civilian authorities, most notably in the form of States using their National Guard personnel to respond to wildfires, which are increasingly a year-round rather than seasonal problem. The number of National Guard personnel days dedicated to fighting wildfires increased from 14,000 in fiscal year 2016 to more than 176,000 in fiscal year 2021. Supporting our civilian partners at the Federal Emergency Management Agency and State and local governments is necessary to protect our homeland from these threats. However, increased demands on the force pose opportunity costs as the force cannot simultaneously train and deploy for other defense missions. Hazards such as these are increasingly overwhelming Federal, State, and local responders. More generally, reliance on support from DoD is greater now than it has ever been, and is increasing (e.g., in 2011, DoD supported 97 requests for assistance from nine Federal partners; in 2021, DoD supported 241 requests for assistance from 14 Federal partners).

Even as we grapple with diverse security challenges from state and non-state actors, we must also account for transboundary challenges, such as climate change. Climate change threatens to worsen the severity of climate-related hazards such as hurricanes, floods, and wildfires both at home and abroad, with significant implications for U.S. national security and defense. Domestically, in recent years we have sustained billions of dollars in damage from climate-related disasters to important military installations, such as Tyndall Air Force Base in Florida, Marine Corps Base Camp Lejeune in North Carolina, and Offutt Air Force Base in Nebraska. Damage to installations potentially undermines the ability of our military to carry out mission critical activities and diverts substantial resources to repairs.

Climate impacts are also felt around the world, including on our hemispheric neighbors in the Americas. The National Intelligence Estimate from last fall noted the particular vulnerability of a number of Central American and Caribbean countries. Governments and their civilian populations in the region face increasing vulnerability due to the impacts of climate change,

including from hurricanes and droughts. Devastating storms pose acute challenges to human security while chronic droughts undermine livelihoods, with potential spillover consequences from increased pressures for migration.

Climate change is also affecting the Arctic acutely, creating uncertainty about the scope and nature of human and state activities in the region. Russia, which is the largest Arctic state, is engaged in a multi-year military buildup and ongoing pattern of bellicosity. The PRC has also clearly stated its interest in gaining diplomatic and economic stakes in the region. The PRC is building its ability to operate in the Arctic by expanding its small icebreaker fleet and conducting regular scientific research expeditions.

DoD's Approach to Homeland Defense

DoD's top defense priority is to protect the security of the American people and to defend the homeland. The Department's approach to advancing our priorities and addressing these interconnected challenges is "Integrated Deterrence" – working seamlessly across warfighting domains, theaters, the spectrum of conflict, other instruments of U.S. national power, and our network of alliances and partnerships to apply a coordinated, multifaceted approach to alter our competitors' perceptions of the potential costs and benefits of aggression. The resilience of our critical infrastructure and capabilities at home strengthens deterrence of competitor aggression.

Multi-Domain Homeland Defense: DoD integrates its efforts across domains to defend the U.S. homeland. In the air domain, DoD and our Canadian Forces partners provide for the air defense of North America against airborne threats through NORAD. In the maritime domain, DoD employs naval forces to detect, track, interdict, and defeat maritime threats from hostile nation-states and non-state actors at a maximum distance from the U.S. coastline. DoD also provides global maritime situational awareness, enabling timely, accurate decision-making to counter emergent maritime threats, and enabling a coordinated threat response among Federal partners through the Maritime Operational Threat Response process.

DoD is working closely with Canada to implement the next steps in NORAD's modernization, as agreed to on August 17, 2021. This builds on the U.S.-Canada Roadmap

signed by President Biden and Prime Minister Trudeau on February 23, 2021. NORAD modernization will improve NORAD's ability to detect, deter, and defend against aerospace threats and to detect maritime threats to North America. USNORTHCOM and U.S. Indo-Pacific Command (USINDOPACOM) are responsible for homeland defense and defense support of civil authorities in their respective areas of responsibility.

DoD is working to understand, raise awareness about, and energize attention and preparedness to prevent, mitigate, and respond to national security threats to the homeland. Central to this effort is building the resilience of critical capabilities, such as the services provided by U.S. critical infrastructure sectors, particularly non-DoD owned capabilities on which we rely, in the homeland. Because these are generally not DoD assets, this requires close cooperation with our partners in other Federal departments and agencies, the international community, SLTT governments, and the private sector to address requirements or vulnerabilities and build resilience. This includes reviewing, renewing, and modernizing our approach to partnerships in DoD's homeland defense missions.

For example, in recent months we have worked closely with USNORTHCOM to more clearly and specifically understand our homeland critical infrastructure needs and how they relate to, intersect with, and in some instances diverge from those of our interagency and private sector partners. The general recognition that the homeland and its infrastructure are at risk from our adversaries is no longer sufficient. To effectively counter these risks, we must understand in detail what is most important, to whom, when, and why, and the threats and hazards they are subject to from our adversaries, malign actors, or naturally occurring disasters.

To achieve this, we are expanding our information-sharing efforts so that, both within the Department and with our external partners, we have a common understanding of our infrastructure priorities and the threats they face. Additionally, through a recent initiative we are institutionalizing the capability to conduct the deep, data-driven analysis required to understand our and others' critical infrastructure dependencies and interdependencies. These efforts will, in time, help inform our own understanding of threats to the homeland and, by extension, enable us to make effective policy and operational and resource allocation decisions that build critical infrastructure resiliency.

Cyber: In the cyberspace domain, DoD is responding to cyber threats in two ways. First, DoD is taking the necessary steps to ensure that we can fight and win wars even while under attack in and through cyberspace. The Joint Force's ability to fight through disruptions to its network and systems is a foundational requirement for U.S. national security and underpins our approach to integrated deterrence, which depends on the United States' ability to employ the full range of national security tools even in a contested cyber environment.

Second, DoD executes cyberspace operations to enable its partners and to act, when necessary, to disrupt cyber threats. Working with both public and private partners is vital in the cyberspace domain. DoD is principally reliant on other entities to grant insights into cyber threat actors operating on non-DoD U.S. systems, information that we, in turn, leverage to take actions overseas to stop those threats.

Protecting our democracy from foreign-based attacks, malign influence, and election interference is a DoD top priority. The Department of Defense stands ready and postured for whole-of-government election defense support. More broadly, DoD collaborates closely with other Federal departments and agencies to coordinate operations, share information, and leverage unique technical expertise. The Department of Homeland Security's (DHS's) Joint Cyber Defense Collaborative is a step in the right direction to ensuring that, as a Federal Government, we can work with our private sector partners to respond to cyber threats to the U.S. homeland. As the Sector Risk Management Agency for the Defense Industrial Base (DIB), DoD also partners directly with DIB companies to protect our military advantage by raising the sector's collective cybersecurity and resilience posture by eliminating barriers to effective coordination while maximizing information transparency to ensure our partners have effective tools to mitigate risk.

Defense Support of Civil Authorities: DoD has a long history of leveraging its substantial capabilities and capacity not only to defend our nation, but also to support Federal, State, and local partners in their missions, such as in protecting our nation's critical infrastructure against cybersecurity threats, election security, securing our borders, and responding to man-made and natural disasters and public health emergencies. Examples of DoD support of civilian

authorities in 2021 and early 2022 include responding to and providing support to the whole-of-government responses to COVID-19, climate-related incidents such as storms and fires, and Operation Allies Welcome, and providing support to DHS along the Southwest Border.

COVID-19: DoD continues to support the national response to the COVID-19 pandemic. In 2021, DoD supported approximately 118 requests for assistance. As of February 28, 2022, DoD has 63 teams totaling 1,424 personnel identified to support hospitals and medical centers in need of staff augmentation. Based on our nation's pandemic response, we have gained a better understanding of the limitations of our nation's medical response capabilities and capacities, particularly with an event that creates demands for capabilities across the whole nation nearly concurrently.

The United States must be prepared to face biological threats from naturally occurring, accidental, and deliberate sources. Global travel, trade, climate change, and potential misuse of emerging biotechnologies creates the risk of biological threats endangering lives and disrupting society, the economy, and the food supply of the homeland. DoD is not isolated from the impact of biological threats, and must plan for ways to operate in a biologically challenged environment. The Department is conducting an internal Biodefense Posture Review; we anticipate this review will inform DoD roles and priorities for addressing biological threats to the Force and in supporting the broader federal biodefense enterprise.

Climate Change: The Department will have to remain vigilant in the face of escalating climate-related disasters in the hemisphere. Given how climate change is reshaping the geostrategic environment, exacerbating existing risks and creating new challenges for U.S. national security and defense, DoD is integrating climate considerations into major planning documents, including the National Defense Strategy, Guidance for the Employment of the Force, and the Chairman's Risk Assessment, as well as other DoD core guidance. We are discussing climate change and climate resilience cooperation during bilateral and multilateral meetings and conferences. Closer to home, in 2021, DoD also supported 66 requests for assistance to respond to a winter storm in Texas, four hurricanes or storms (e.g., Hurricane Henri, Hurricane Ida, and Tropical Storm Peter), tornados in Kentucky, and multiple wildland fires.

Operation Allies Welcome: Over the past year, DoD also has provided considerable support to our Federal partners through Operation Allies Welcome to care for more than 80,000 Afghan evacuees. To accommodate this large influx of evacuees, the Department provided temporary housing, medical, and other associated support at eight domestic military installations while Afghan evacuees completed medical screenings, vaccinations, and resettlement paperwork. Although such support on military installations has now ended, DoD will continue to provide humanitarian support for Afghan evacuees at a non-DoD facility.

Southwest Border Security: DoD has supported DHS's border security mission at the southwest border for 17 of the last 21 years. In 13 of these 17 years, the duration of DoD support was for the entire fiscal year, and at all times was provided on a non-reimbursable basis. Currently approximately 2,500 military personnel are deployed to the southwest border, supporting U.S. Customs and Border Protection (CBP) detection and monitoring activities, and providing intelligence analysis, aviation, command and control, and other support to CBP.

Although DoD recognizes that its support has been helpful over the years, it is important that our partners have sufficient capacity and capability to perform their missions, so that DoD can focus on its mission and be available when there truly is a temporary, exigent emergency. It is important that other departments and agencies have the capacity and capability to perform their own missions so that our nation is more secure and resilient. An over-reliance on DoD support could become an acute challenge in a scenario where DoD's capabilities and capacity are needed elsewhere for DoD's national defense missions. DoD is working with our partners to transition from DoD support to their organic capacity and capabilities.

Defense Partnerships in the Western Hemisphere

As emphasized in the Interim National Security Strategic Guidance, the vital national interests of the United States are inextricably bound to the fortunes of our neighbors and partners in the Western Hemisphere —and especially with Canada and Mexico. To address shared threats, DoD must continue to maintain strong partnerships with the defense and security ministries and the militaries of our neighbors in the Americas. Our partnerships are based on the

bedrock principles of support for democratic institutions, civilian control of the military, and respect for human rights and dignity.

We are at a strategic inflection point, with the opportunity to forge deeper bonds within our hemisphere through defense engagement and strategic security cooperation. The strength of these partnerships will make a pivotal difference in our collective ability to successfully address the challenges we face. DoD continues to host and participate in strategic defense dialogues, defense and military exercises, seminars, and senior leader engagements. We continue to advance our defense relationships with strong allies and partners such as Canada, Mexico, Colombia, Brazil, and Chile. We have expanded our cooperation with Caribbean and Central American defense and security partners to support their regional security objectives, strengthen their defense capabilities, and help to make the air and maritime approaches to the United States more secure. We also participate in regional and hemisphere-wide defense and security venues, such as the North American Defense Ministerial, the Inter-American Defense Board, and the Conference of Defense Ministers of the Americas, which Brazil will host in July.

Secretary Austin directed DoD to align its priorities and capabilities to address a changing and dynamic threat landscape, including the impacts of the COVID-19 pandemic, the influence of global competitors such as the PRC, and persistent threats such as transnational and non-state illicit actors. He expects the Department to address these challenges based on a sober assessment of our strategic needs and in recognition of the importance of working together with our allies and partners.

The COVID-19 pandemic is just one example of the importance of international partnership. The pandemic caused significant challenges across the hemisphere with political, economic, and public health effects likely to be felt in the region for years to come, with second and third order effects for our partner nations' militaries. USNORTHCOM and USSOUTHCOM deserve recognition for outstanding work in the region in delivering COVID-19-related assistance to our partners over the past two years, including more than two dozen field hospitals, personal protective equipment, medical and non-medical supplies, disinfectants, test kits, ventilators, and cold storage devices.

DoD continues to provide support for humanitarian assistance and disaster response. Several of the militaries in the hemisphere have lead responsibility for disaster response within their countries, including those that are linked to climate impacts, such as powerful storms in the Caribbean. Nearly all of the hemisphere's militaries provide some level of critical support to their nation's response to these hazards. We recognize the value and importance of mutual support for mission success in a humanitarian or disaster response scenario. For example, in August 2021, USSOUTHCOM played a critical supporting role in the U.S. Government's response to the 7.2 magnitude earthquake in Haiti. DoD provided air transport and logistics to facilitate critical life-saving operations in hard-to-reach areas of southwest Haiti by rapidly deploying planes, helicopters, and ships to the affected area. We were not alone, as other countries' militaries in the hemisphere also provided support and relief to Haiti, including by delivering humanitarian supplies and donations.

We also see increased concerns across the hemisphere about the threat of malicious cyber activity, and, thus, see an increased demand for cyber, information sharing, and science and technology cooperation in the region. Many partners seek expanded cooperation and information-sharing with us to protect national networks. In response, we are developing new opportunities to help partners improve their cyber and network defense capabilities, so they can deter, detect, and defend against cyber threats. This network of partners is key to achieving our shared goals for a free, secure, and prosperous Western Hemisphere.

Arctic: In the Western Hemisphere, we are also focused on our northern borders and the Arctic region. In consultation with U.S. allies and partners, DoD is examining its strategy, posture, and equipment to protect the U.S. homeland, to ensure a stable and open Arctic, to deter aggression, and to preserve our economic interests in the region as conditions there continue to evolve. DoD continues to maintain a watchful approach to the Arctic region, and is prioritizing working with allies and partners to build domain awareness and advance capabilities through training and exercises such as the forthcoming COLD RESPONSE exercise hosted by Norway. The new Ted Stevens Center for Arctic Security Studies, a DoD Regional Center, will support DoD's ability to evolve our strategic approach to the Arctic as conditions warrant. Defending the

U.S. homeland requires DoD to closely monitor the evolving situation in the Arctic region, and be prepared to evolve strategy, posture, and equipment as required to deter aggression, support allies and partners, ensure stability, and preserve U.S. interests.

Conclusion

Mr. Chairman, Ranking Member Rogers, and distinguished Members of the Committee, in conclusion, the homeland and the Western Hemisphere face increased and evolving threats from state and non-state actors – adversarial actions that undermine stability and democratic institutions, cyber threats, an escalating climate crisis, and threats to critical infrastructure. To address these shared challenges, we will continue to raise awareness and increase preparedness with our partners in and out of government to prevent, mitigate, and respond to national security threats to the homeland, build resilience, and advance U.S. national interests in the Western Hemisphere. Thank you for the support of Congress and for your continued commitment and support of the women and men of the Department of Defense. I look forward to your questions.