JOINT STATEMENT OF

MIEKE EOYANG

DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CYBER POLICY

MAJOR GENERAL KEVIN B. KENNEDY, USAF

DIRECTOR OF OPERATIONS, UNITED STATES CYBER COMMAND

REAR ADMIRAL FOY

DEPUTY DIRECTOR FOR GLOBAL OPERATIONS, JOINT STAFF

TESTIMONY BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY

JUNE 23, 2021

Thank you Chairman Manchin, Ranking Member Rounds, and Members of the Committee. I am pleased to be here with Major General Kennedy, Director of Operations, U.S. Cyber Command (USCYBERCOM), and Rear Admiral Foy, Deputy Director for Global Operations, Joint Staff, to discuss the Department of Defense (DoD) role in addressing the urgent threat of ransomware. I have submitted this joint statement for the record on behalf of all Department witnesses. Before I begin, I would like to remind the Members that we are not able to discuss sensitive military cyber operations in an unclassified setting. We look forward to providing you with additional information in the closed session.

I can say this much, however. The Department recognizes the seriousness of this threat to U.S. critical infrastructure. Although the DoD Information Network (DoDIN) has not fallen victim to ransomware, we are acutely aware of the threat to the private companies that comprise the defense industrial base (DIB) and operationally critical contractors. This is also not just a DoD-centric concern. The recent Colonial Pipeline and JBS compromises have demonstrated ransomware's potential to disrupt the everyday lives of Americans. Ransomware is a threat to our national security, and thwarting ransomware actors effectively requires a whole-of-government response that is coordinated with the private sector and our international partners.

I applaud the Members for your bipartisan leadership to ensure that the U.S. Government is able to counter this threat. I understand that each of the States, which you represent, has suffered at least one ransomware incident involving essential public functions, including those furnished by municipal governments, schools, and airports. As demonstrated by the incidents affecting the Pleasant Valley Hospital in West Virginia and small law firms in South Dakota, ransomware hurts people and disrupts lives. These particular ransomware incidents happened recently, but the list of American ransomware victims is long and grows each day, as the threat becomes more pervasive. I look forward to working with you as we take up the cause of mitigating these disruptions to Americans' daily lives.

President Biden has made it a priority to address the ransomware threat. This made clear the U.S. position that attacks on, and disruption of, our critical infrastructure, through the use of ransomware or other cyber means, are not acceptable. And in May, after the Colonial Pipeline incident, the President signed an executive order to improve our Nation's cybersecurity. The order calls for Federal agencies to work more closely with the private sector to share information, to strengthen cybersecurity practices, and to deploy technologies that increase resilience.

Addressing the threat of ransomware will be a challenge. Part of this challenge is the increasingly blurry line between nation-state and criminal actors. We have seen some governments let government-employed hackers "moonlight" as cybercriminals for personal benefit, which is not how responsible States behave in cyberspace. Our adversaries have also created permissive environments for criminal ransomware gangs, allowing them to operate from within their borders and shielding them from prosecution so long as they avoid targeting the host country's businesses and government systems. This is sometimes evident in ransomware code, as gangs operating in Russia design their malware to avoid infecting computers where Russian is the default language. The administration has been clear that this is not acceptable, and that responsible countries must take action against criminals who conduct ransomware activities from within their territory.

We cannot, however, expect these financially motived crimes to cease in the immediate term. The Department currently works to counter the ransomware threat as part of our mission to defend the Nation in cyberspace. We do this as part of whole-of-government efforts, but DoD has several distinct roles in this effort.

First, the Department gains insights about hostile cyber actors through Hunt Forward Operations on allied and partner nation networks. We use those insights to improve our own security posture and to enable appropriate actions by our

partners, domestically and internationally. We are also prepared to take authorized actions to stop or degrade adversary activity.

Second, we take actions to increase the security and resiliency of the DIB and operationally critical contractors. The DoD Cyber Crime Center (DC3) and its DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE) have prioritized ransomware reporting and content briefings in support of DoD's DIB Cybersecurity Program Partners—emphasizing impacts, implications, and threat mitigations.

Third, the Department continuously defends the DoDIN from **all** malware, including ransomware. Our cyber forces regularly hunt for adversaries on the DoDIN. And, as I mentioned previously, we continue to leverage the insights gained by operating on foreign networks to improve our cyber defenses, and we continue to strengthen our partnerships with the Federal Bureau of Investigation and the Department of Homeland Security in order to improve the cyber defenses of Federal, State, and local governments, as well as those of the private sector.

The Department has the capability and capacity to ensure the security and resiliency of its own networks and to conduct operations in support of the Joint Force. Thus far, ransomware perpetrators appear to be financially motivated and therefore to have targeted private industry for financial gain. These are crimes.

The Department stands ready to support our colleagues in the Federal Bureau of Investigation in their pursuit of these criminal actors. Further, the Department may provide assistance, when requested, to the Department of Homeland Security (DHS), which has the lead for protecting domestic critical infrastructure.

In closing, I would like to thank the Members once again for your bipartisan leadership to enable the U.S. Government to counter cyber threats to our national security. As the Department works to support its interagency partners in defending the Nation against ransomware, we know that Congress is a strong and willing ally in this fight. A whole-of-government response is necessary to address the ransomware threat effectively, but as the majority of U.S. critical infrastructure is privately owned, combatting ransomware also requires a whole-of-nation response. Thank you for your time today, and I look forward to your questions.