POSTURE STATEMENT OF

GENERAL PAUL M. NAKASONE

COMMANDER, UNITED STATES CYBER COMMAND

BEFORE THE 118TH CONGRESS

SENATE COMMITTEE ON ARMED SERVICES

7 MARCH 2023

(U) Chairman Reed, Ranking Member Wicker and distinguished members of the committee, thank you for your enduring support and the opportunity to represent the men and women of U.S. Cyber Command (USCYBERCOM). I am honored to be here beside Assistant Secretary of Defense Christopher Maier and General Bryan Fenton. I look forward to describing how USCYBERCOM continues to deliver return on investment by using the authorities and resources provided by Congress and highlighting the work ahead for 2023.

(U) Guided by the *National Defense Strategy*, USCYBERCOM focuses on building enduring advantages through campaigning to support Integrated Deterrence. USCYBERCOM acts against foreign adversaries that threaten our nation and expands capability through cooperation with federal, private and allied partners. We seek to outmaneuver our adversaries as they look for opportunities to exploit the United States' dependence on data and networks in critical infrastructure, the Defense Industrial Base and private industry.

(U) USCYBERCOM is the nation's premier military cyber force—one whose world-class talent and strategic partnerships defend U.S. interests while delivering warfighting advantage to the Department of Defense (DoD). It executes its mission along four lines of effort to create and maintain advantage against our adversaries:

- We generate insights and options in defense of the nation;
- We secure, operate and defend the Department of Defense Information Network (DoDIN), ensuring mission advantage for the Department of Defense;
- We develop options for full-spectrum cyberspace operations to assist Combatant Commanders and the Joint Force to achieve their objectives; and
- We boost the strength of America's allies and partners in cyberspace.

(U) USCYBERCOM will build up its people, partners and decisive advantage. The Command directs operations through its components. These include the Cyber National Mission Force (CNMF); Joint Force Headquarters-DoD Information Network (JFHQ-DoDIN), the commander for which is dual-hatted as the Director of the Defense Information Systems Agency); Joint Task Force Ares and other Joint Force headquarters elements. The commanders of Army Cyber Command, Marine Corps Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, Air Forces Cyber/16th Air Force and Coast Guard Cyber Command also lead their Service cyber components.

(U) Operational success in the cyberspace domain demands speed, agility and unity of effort. Hence, the roles, missions and responsibilities of USCYBERCOM and National Security Agency (NSA) must be mutually supportive in this mission space. A recent report on the dual-hat leadership structure completed by a Secretary of Defense and Director of National Intelligence-directed Senior Steering Group (comprising defense and intelligence leaders) found "substantial benefits that present compelling evidence for retaining the existing structure." The successes that USCYBERCOM and NSA have experienced in defending our elections, in engaging ransomware actors, and in many other missions with the other Combatant Commands,

rest on the alignment of USCYBERCOM and NSA. The Senior Steering Group highlighted these accomplishments for the Secretary of Defense and Director of National Intelligence, finding that the dual-hat structure is in the best interests of USCYBERCOM, NSA and the nation. Success in protecting the national security of the United States in cyberspace would be more costly and less decisive with two separate organizations under two separate leaders. The enduring relationship is vital for both organizations to meet the strategic challenges of our adversaries as they mature their capabilities against the United States.

(U) Present and Future

(U) USCYBERCOM persistently engages adversaries, countering cyber actors and their affiliates who are seeking to harm the United States, its interests and its allies. Skilled and dangerous cyber actors exist, many of them serving foreign military and intelligence organizations. USCYBERCOM provides options to counter malicious actors who exploit cyberspace to support their intelligence operations, steal intellectual property, promote violent extremism, impair democratic processes, coerce perceived rivals and fund transnational illegal conduct.

(U) The *National Defense Strategy* named the People's Republic of China (PRC) as our military's pacing challenge. The PRC combines authoritarianism with a revisionist foreign policy and stands as the only competitor with both the intent and power to reshape the global order to its advantage. Its rapidly modernizing military is building capabilities far in excess of China's defense needs while supporting Beijing's coercive diplomacy. Competition with the PRC takes place on a global scale, and although that contest remains below the threshold of armed conflict, it is nonetheless strategic in its effects and its implications. PRC-sponsored cyber actors represent a sophisticated and growing threat to the United States' and allies' interests.

(U) China is learning from Russian actions in Ukraine and elsewhere. The *National Defense Strategy* calls Russia an acute threat to the free and open global system, noting that Moscow flouts international norms with its destabilizing actions. Russia's aggression in Ukraine threatens the peace and stability of Europe. The U.S. and our allies are working to ensure the strategic failure of their attempt to change the status quo by violence.

(U) Russia's military and intelligence cyber forces are skilled and persistent. Russia has attempted to influence elections, through malign activities, in the United States and Europe and has enabled intelligence collection on a global scale. Moscow has a high tolerance for risk and collateral damage in its cyber operations. This boldness is evident in Russia's indiscriminate cyberattack on Viasat satellite communications in Ukraine and across Europe in support of the invasion of Ukraine last year.

(U) Russia and Ukraine are engaged in a complex struggle in cyberspace that includes significant support from independent actors. Before the crisis unfolded, USCYBERCOM partnered with U.S. European Command (USEUCOM) and Ukraine by deploying "hunt forward" cyber experts to assist Ukraine's efforts to harden their networks against Russian aggression. Since the crisis began, USCYBERCOM has focused on defending secure

communications capabilities at USEUCOM and Ukraine – ensuring the posture of our nation's nuclear command and control and strengthening DoDIN defense.

(U) The *National Defense Strategy* emphasizes our enduring commitment to deterring aggression in the Middle East and promoting stability in East Asia. Iran remains a destabilizing force in its region, and its cyber actors are proficient and aggressive. Tehran's paramilitary and intelligence forces sponsor a variety of malicious cyber activities against Iran's neighbors and against the United States, as we saw in last year's midterm election. Pyongyang also maintains cyber forces supported by North Korean information technology workers dwelling in other countries. They remain a threat, although much of their recent activity has been devoted to evading international sanctions by stealing cryptocurrency for the regime's use.

(U) Non-state actors also remain a threat in cyberspace. International cybercrime, often organized or executed by actors in Russia, continues to be a concern. USCYBERCOM and NSA enable efforts by the Department of Treasury, the Federal Bureau of Investigation (FBI) and other partners to disrupt ransomware, cryptocurrency theft and other criminal activities. In addition, violent extremist groups are also active in cyberspace. The Islamic State in Iraq and Syria, al Qaida and associated terrorist groups maintain the intent to target Americans, although their capabilities have been eroded. Our Marine component, JFHQ-C (Marines), works with allies and partners to disrupt violent extremist group mobilization online and to support diplomatic efforts.

(U) USCYBERCOM is fully engaged in its efforts to defend the DoDIN, disrupt adversary campaigns to harm America and its interests, enhance our partners' defense, and support Joint Force objectives in cyberspace. Authoritarian adversaries feel threatened by the freedoms that democratic states regard as commonplace, and thus they not only deny such freedoms to their own people, they campaign in cyberspace to impugn the legitimacy of democratic societies and to intimidate opposition at home and abroad. As the *National Defense Strategy* suggests, it will take a whole-of-government – and indeed, a whole-of-nation – effort to bend this trajectory back toward international respect for the principles of the United Nations Charter.

(U) Defense of the Nation

(U) Defending the nation is paramount among our missions. It means defending our military systems, networks and the critical infrastructure that enable national security. Every Combatant Command's operational plan across the Department assumes that our commanders will be able to leverage data and communicate orders and data rapidly and securely across the battlefield. In this regard, USCYBERCOM plays a crucial role in the defense of military systems, networks and data.

(U) USCYBERCOM and NSA collaborated in defense of the 2022 midterm election. Foreign attempts to meddle in our electoral process via cyber means escalated in 2016 and have persisted in every election cycle since. USCYBERCOM expects them to continue into the future as the prospect of distracting our leaders, pitting Americans against one another on divisive issues and undermining public trust in the democratic process is too tempting for foreign

adversaries. USCYBERCOM seeks to render these campaigns inconsequential, in conjunction with the FBI and Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS/CISA) partners.

(U) In 2022, USCYBERCOM and NSA teams staffed a combined Election Security Group (ESG) to coordinate cybersecurity, intelligence and operations. The efforts of the ESG enabled DHS and the FBI, among other domestic partners, to defend electoral processes and take action against foreign actors working to subvert the midterms. The 2022 midterms progressed from primaries to certifications without significant foreign malign influence or interference.

(U) The Cyber National Mission Force (CNMF) played an important role in the defense of the midterms and is vital to many of our other efforts as well. CNMF conducts missions to counter malicious cyberspace actors and covers both the offensive and defensive aspects of our defend-the-nation mission set. USCYBERCOM established the CNMF as a subordinate unified command on December 19, 2022 at the direction of the Secretary of Defense. Elevating the CNMF to the status of a sub-unified command not only recognized the importance of its enduring mission, it gave the CNMF greater ability to manage its personnel and readiness and to request manpower, funding and resources through DoD processes.

(U) Since 2018, the CNMF has deployed hunt forward teams 40 times to 21 countries to work on 59 networks, generating insights and imposing costs on common adversaries. These partner-enabled operations have exposed malicious cyber activity by China, Russia, Iran and cyber criminals; made partner-nation networks more secure; increased our global cybersecurity partnerships; led to the public release of more than 90 malware samples for analysis by the cybersecurity community and ultimately kept us safer here at home. In competition, there is no substitute for sharing accurate, timely and actionable intelligence to expose adversarial activity with like-minded domestic and international partners.

(U) Last year, we created a combined USCYBERCOM-NSA China Outcomes Group to oversee this shift. The China Outcomes Group aligns components in USCYBERCOM and NSA, enhances intelligence insights, improves cybersecurity and delivers operational outcomes for the nation. Resources are prioritized and focused on deterring and countering the PRC's aggressive behavior.

(U) Cyberspace is a global domain. Adversaries often penetrate privately-owned networks and devices, using ever-increasing technical capabilities to disrupt operations or gain illicit value via activities such as intellectual property theft, targeting of personal information and installation of ransomware. USCYBERCOM is working under recently expanded statutory authorities and aligning efforts with NSA's Cybersecurity Directorate to bolster companies' ability to defend themselves against exploitation by cyber actors. This collaboration and broad sharing of insights with the private sector provides mutual benefits. An example of this is our UNDERADVISEMENT program, which links cybersecurity expertise across industry and government, leading to several operational successes as well as pointing the owners of victim systems toward threats that they can eradicate. In conjunction, NSA's Cybersecurity Directorate runs its Cybersecurity Collaboration Center to share best practices with industry partners and gain additional insights into the technical challenges they are encountering.

(U) Strategic Initiatives

(U) The success of our operations to support the *National Defense Strategy* depends on training and readiness. We have prioritized improving the readiness of our cyber forces since USCYBERCOM became a unified Combatant Command in 2018, and there has been progress in the last several years. The staffing and training of our teams are improving. In addition, USCYBERCOM has enhanced its ability to monitor the status of the Cyber Mission Force (CMF) at the team, mission element and individual levels. USCYBERCOM is crafting standards for cybersecurity defenders across the DoD Cyberspace Operations Forces Service-retained cyber forces. The creation of these standards will improve the ability to defend networks while enabling our CMF teams to hunt foreign adversaries where they hide and foster a culture of innovation, collaboration and compliance that USCYBERCOM seeks to build.

(U) Strong partnerships are crucial to cyberspace operations. When working in unison, our diplomatic, military, law enforcement, homeland security and intelligence capabilities make a powerful combination that can disrupt the plans of malicious cyber actors. As we saw in our collective defense of the 2022 midterm election, such effects become even more decisive when we include our allies and foreign partners. Their reach often exceeds our own, especially in host-nation systems. As part of our regional engagement strategy in the Indo-Pacific, we are working closely with partners such as Australia, Japan and South Korea to share information that will impose costs on foreign adversaries. Likewise, we continue to do the same with other partners in Europe and Asia. We are also working to enhance partnerships with academia and industry experts who assist us in concept and capability development.

(U) Implementing USCYBERCOM's Service-like authorities will allow it to deliver priority capabilities with agility and at speed. In Fiscal Year 2024, USCYBERCOM will assume control of the resources for the Cyber Mission Force cyberspace operations and capabilities. Enhanced budgetary control (EBC) gives USCYBERCOM the ability to directly allocate resources for greater efficiencies during the Department's programming phase and ensure they remain aligned with priorities through execution. EBC will lead to better alignment between USCYBERCOM responsibilities and authorities for cyberspace operations.

(U) Expanding USCYBERCOM's role in acquisition is another important step in the implementation of Service-like authorities. The Joint Cyber Warfighting Architecture (JCWA) is USCYBERCOM's premier platform that enables Cyber Operations Forces to conduct full-spectrum cyberspace operations. The Under Secretary of Defense for Acquisition and Sustainment is granting USCYBERCOM greater technical responsibility and authority to direct the development, integration and fielding of critical capabilities and infrastructure in the JCWA. Included in the Fiscal Year 2023 National Defense Authorization Act is a provision directing the establishment of a Program Executive Office (PEO) within USCYBERCOM. This PEO would assume Service-like acquisition decision authority for JCWA program components by Fiscal Year 2027.

(U) USCYBERCOM depends on support from the National Guard and Reserve. Service cyber components employ Reserve Component personnel to support operations and reinforce

relationships with government agencies, increasing the synergy between USCYBERCOM and these organizations. In addition, Army Cyber Command benefited from the expertise of civilian data scientists during their mobilizations to support research and development projects that would not typically be possible with traditionally-trained active duty forces. National Guard components on State active duty, and in the State Partnership Program (SPP) work in various efforts to protect state, industry and foreign-partner systems. The SPP offers additional capacity to support increased cyberspace security cooperation activities in support of national defense strategy objectives. We gain valuable insights from the specialized expertise that Reserve Component personnel can bring from their civilian jobs in industry and academia, and such ties have helped us build partnerships across America.

(U) USCYBERCOM recognizes its challenge to grow and develop its military and civilian workforces. Cyber Excepted Service (CES) allows USCYBERCOM to offer cyber professionals opportunities to use their skills and contribute greatly to the national security of the United States. Since CES implementation began, USCYBERCOM has seen positive improvements to the recruiting and hiring timeline.

(U) Enhancing diversity, equality and inclusion is a priority. USCYBERCOM and NSA cannot afford to overlook or neglect talent wherever it resides nor can we allow workplace challenges of any sort to discourage professionalism or inhibit creativity. Our impact for the nation depends on fostering a wide range of viewpoints and free-ranging debate to encourage innovation and problem-solving, and we will not tolerate harassment in any form or behavior that stifles civil discourse.

(U) Conclusion

(U) Success for USCYBERCOM will be measured by how effectively foreign adversarial actors are prevented from achieving their strategic objectives. USCYBERCOM will counter adversaries in competition to defuse crises, deter conflict and prevail against aggression. Aligning efforts of both USCYBERCOM and NSA is essential to achieving these goals and is in the best interest of the nation. It all starts with people—the men and women of USCYBERCOM working with NSA and partners here and abroad—We win with People.

(U) Last year saw significant maturation for USCYBERCOM, but our work is not done. In 2023, we must continue to focus on our people, our partners and our ability to deliver decisive advantage. We must improve readiness, bolster our resilience and maintain a culture of continuous improvement. We have and will continue to deliver warfighting advantage for the Joint Force and partners throughout the full spectrum of competition, crisis response and conflict. We are doing so by executing our Service-like authorities to build and sustain campaigns in and through cyberspace and the information environment.

(U) USCYBERCOM's efforts to defend against and contest adversary campaigns in and through cyberspace have been enhanced by the support of this Committee. Designing our campaigns to stay in constant contact with foreign adversaries (persistent engagement) and synchronizing Offensive and Defensive Cyberspace Operations with DoD Information Network Operations are the critical initiatives that allow USCYBERCOM to maintain its advantage in

cyberspace. These concepts will continue to be key to our effectiveness and are necessary to outmaneuver and outpace our adversaries wherever they are.

(U) The men and women at U.S. Cyber Command are grateful for the support this Committee has given to our Command. We can only succeed with a strong partnership with Congress. Thank you, and I look forward to your questions.