STATEMENT OF

GENERAL PAUL M. NAKASONE

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

SENATE COMMITTEE ON ARMED SERVICES

14 FEBRUARY 2019

Chairman Inhofe, Ranking Member Reed, and distinguished members of the Committee, thank you for inviting me to represent the men and women of US Cyber Command (USCYBERCOM). I am honored to lead them, and grateful for the opportunity to highlight their accomplishments. Our Command has seen a year of change and progress, featuring the elevation of USCYBERCOM to a unified combatant command with an expanded mission and additional authorities and responsibilities, and the completion of the build of 133 teams in our Cyber Mission Force (CMF). We have transitioned from building the force to ensuring its mission readiness, and in 2018 we enhanced that by opening our new, state-of-the-art Integrated Cyber Center. Enabled by changes in law and policy, we have produced defensive and offensive operational successes. My testimony will summarize threats and opportunities in our strategic environment, explain how we prepared ourselves to meet them and what we did, and explain our priorities for the future of a USCYBERCOM that enables our partners and acts in cyberspace to defend the nation.

USCYBERCOM's task is to plan and execute global cyberspace operations, activities and missions to defend and advance national interests in collaboration with domestic and international partners across the full spectrum of competition and conflict. Our responsibilities include providing mission assurance for the Department of Defense by directing the operation and defense of the Department's information systems (what we call the DoDIN); deterring or defeating strategic threats to national interests and infrastructure; and helping the combatant commanders achieve their missions in and through cyberspace. This fiscal year we are executing a budget totaling roughly $610 million. Our full-time personnel amount to 1,520 military and civilians, plus contractors. This January we had 4,406 Service members and civilians in our Cyber Mission Force, building to a total of 6,187 people. We also have both Guard and Reserve personnel on active duty serving in our forces.

USCYBERCOM comprises a headquarters organization that directs operations through its components. These include the Cyber National Mission Force (CNMF); the Joint Force Headquarters-DoD Information Network (JFHQ-DoDIN); and Joint Task Force Ares; plus our Joint Force headquarters elements, each of which is paired with one of the Services' cyber

components. Those Service components are Army Cyber Command, Marine Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, Air Force Cyber/24th Air Force, and U.S. Coast Guard Cyber.

Our efforts and our continued success depend upon the support of the Congress and of this Committee. Thank you in advance for the assistance you are providing us in 2019 as we pursue opportunities in five areas: (1) Supporting strategic competition; (2) Establishing a warfighting ethos across the Command; (3) Improving the readiness of our cyber forces; (4) Enhancing partnerships across government, allies, and the private sector; and (5) Deploying improved operating infrastructure.

The Strategic Environment

Cyberspace is a contested environment where we are in constant contact with adversaries. The nation faces threats from a variety of malicious cyber actors, including non-state and criminal organizations, states, and their proxies. We see near-peer competitors conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage. USCYBERCOM ensures two critical capabilities against these threats: it <u>enables</u> partners in whole-of-nation efforts to build resilience, close vulnerabilities, and defend critical infrastructure; and it <u>acts</u> against adversaries who can operate across the full spectrum of cyberspace operations and who possess the capacity and the will to sustain cyber campaigns against the United States and its allies.

Renewed Strategic Competition. The *National Security Strategy* (2017) emphasized the emergence of great-power competition and noted its spread into cyberspace. In implementing that guidance, the Department issued the *DoD Cyber Strategy*, which described the environment we face:

> *We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace <u>that pose long term strategic risk to the Nation as well as to our</u>*

> *allies and partners. China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States' growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation* [emphasis in original].

I assess we are seeing what we term *corrosive threats*, in which malicious cyber actors weaponize personal information, steal intellectual property, and mount influence campaigns. Such measures have had and will have strategic effects on our nation and allies.

Changes in Strategic Guidance and Authorities. USCYBERCOM has recently improved the scope, speed, and effectiveness of its operations with the help of legal and policy changes. I want to thank Congress for its support of DoD's cyberspace operations as reflected in provisions of the FY19 National Defense Authorization Act (NDAA) that enhanced our agility to execute missions consistent with law. We also received updated policy guidance that, in conjunction with the NDAA provisions, significantly streamlined the interagency process for approval of cyber operations and thus facilitated recent activities.

The *DoD Cyber Strategy* asserts that the Department has a significant role in defending the nation. To be effective in doing so, the *Strategy* mandates that DoD components "defend forward, shape the day-to-day competition, and prepare for war," enabling the Department "to compete, deter, and win in the cyberspace domain." We must be active because inaction on our part cedes advantage to capable adversaries willing to flout international law and impose their own norms of cyber conduct. In keeping with guidance to defend forward, the Department is aiming to take the initiative against those who act against us. The *DoD Cyber Strategy* states that the Department must be prepared to defend assertively the functioning of even non-DoD

critical infrastructure systems -- whether at home or abroad -- that are essential to project, support, and sustain Departmental forces and operations worldwide. In practice, this means confronting our adversaries from where they launch cyber attacks and developing robust capabilities that are responsive to Defense Support to Civil Authorities (DSCA) activities.

A New Operating Construct. We are implementing the *DoD Cyber Strategy* through the strategic approach of persistent engagement, which includes partnering with other US Government elements to build resilience into US networks and systems, defending against malicious cyberspace activities as far forward as possible, and contesting adversary attempts to disrupt our nation's key government and military functions.

Our operators, analysts, developers, leaders, and support personnel, enabled by new and modified policy guidance, are operating more effectively in coordination and partnership with other agencies, partners, and allies. Last fall we supported US European Command (USEUCOM), US Northern Command (USNORTHCOM), the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and others to defend the integrity of America's 2018 mid-term elections. Working together under my command, USCYBERCOM and the National Security Agency (NSA) undertook an initiative known as the Russia Small Group to protect the elections from foreign interference and influence. By enabling our fellow combatant commands and other partners, USCYBERCOM assisted the collective intelligence and defense effort that demonstrated persistent engagement in practice. The tight links between USCYBERCOM and NSA created a mutually beneficial, intelligence-operations cycle that let us rapidly find and follow leads, discover new information, and create opportunities to act in conjunction with partners. Additionally, our co-location in the new Integrated Cyber Center optimized our collaboration for efforts of this nature. We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts. We shared information through DHS with state election officials to help identify vulnerabilities and improve threat warning. We also enabled Department of the Treasury and FBI actions in conjunction with the private sector, for instance by posting foreign malware for the first time to VirusTotal, a private site for crowdsourcing analysis of cyber threats. Finally, working with

USEUCOM, and with the consent of several European countries, we sent defensive teams forward to conduct operations in support of our mission to help secure the mid-term elections.

Opportunities and Challenges for US Cyber Command

I note the progress we have made during the past year and see opportunities ahead, with corresponding challenges as well. We have achieved much under the *National Defense Strategy*'s commitment to prioritize investments in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations. We must use our recent successes to inform future activities, ensuring that accomplishments are not isolated events but parts of a larger trend of improved operational proficiency.

Supporting Strategic Competition. Cyberspace is a domain in which opponents can attain strategic results without using armed force. Our adversaries in cyberspace are acting and taking risks in seeking to gain advantage without escalating to armed conflict; they are conducting campaigns to gain cumulative advantage (these include theft of intellectual property and personal information, malign influence and election interference, efforts to circumvent sanctions, and probes and positioning to threaten critical infrastructure).

We see evidence of such cyber campaigns in many places, such as the foreign efforts to find vulnerabilities in the Department of Defense's Information Network. JFHQ-DoDIN used its authorities to direct global Department of Defense network operations, security, and defense. By operationalizing the network sensors, they assessed effectiveness and risk through focused data analysis. This in turn helped improve the fidelity of our sensors and analytics, showing us the risks and the requirements for mitigation. The data JFHQ-DoDIN collected in this effort proved that state-sponsored adversaries in cyberspace are conducting rapidly evolving campaigns to hamper the routine functions of the DoDIN and to find seams in its defenses. DoDIN protections are robust, but we must continue to innovate in our data collection and analysis to build resilience and counter the dynamic nature of adversary threats.

In the face of strategic competition in cyberspace, USCYBERCOM brings unique advantages in planning, deconflicting, executing, and assessing cyberspace operations at-scale.

Our efforts in defense of the 2018 elections taught us the value of persistent engagement to contest adversary campaigns, the power of enabling partners, and the ability to impose costs. The *DoD Cyber Strategy* notes we cannot afford inaction – our values, economy, and society are exposed and we must assertively respond at all levels. USCYBERCOM is working with the combatant commands, DHS, FBI, across the Intelligence Community, and in conjunction with private sector and foreign partners to improve understanding and act to contest and frustrate adversary cyber activities. Through persistent engagement we identify and close vulnerabilities in DoD networks, act to contest threats, and enable partners in building resilience and in the defense of the nation. These steps complement and support national efforts to prepare for conflict, to deter adversaries, and to establish cyber norms while we simultaneously support combatant commanders in contingency operations.

Supporting the Combatant Commands and Establishing a Warfighting Ethos. A competitive mindset is needed to prevail in a deeply competitive domain. Such a mindset also helps us prepare to fight and win the nation's wars. To support combatant commanders and their missions we are engaged in a growing variety and number of activities, from planning to intelligence missions to operations in and through cyberspace. We bring to the combatant commands a wartime ethos reinforced by daily contact with cyber adversaries.

Our cyberspace operations support kinetic and information operations against terrorists across several regions. We are employing cyber capabilities to improve force protection, bolster intelligence, understand and shape the information environment, and disrupt the operations, command and control, and propaganda of several insurgent and terrorist groups in support of US Central Command (USCENTCOM), US Africa Command (USAFRICOM), and US Special Operations Command (USSOCOM). Cyberspace operations in places like Iraq, Syria, Yemen, and Afghanistan today integrate and synchronize cyberspace and information operations with kinetic missions, with each enabling the other for offensive, force protection, and intelligence purposes. Our persistent engagement with this adversary for the past several years shows the continuing value of our command in being able to operate across all of these regions against the key enablers for these groups (e.g., media, finance, and foreign fighters). In this context, we have expanded the remit of our Joint Task Force Ares, and shifted its chain of command from

Army Cyber Command to Marine Corps Forces Cyberspace Command while maintaining its principal task of operating against the Islamic State. JTF-Ares has also embarked on a special mission partnership with NSA to act together as a hub for whole-of-government cyber planning in the ongoing counter-terror fight (thus further demonstrating the value of the USCYBERCOM and NSA partnership).

The maturation of the Cyber Mission Force has increased the number and proficiency of the cyber units working to protect the networks and weapons systems that combatant commands rely on to perform their missions. Each combatant commander controls organic Cyber Protection Teams (CPTs) that work in conjunction with local and regional cyberspace security providers and administrators. The expertise and databases at USCYBERCOM tie these teams together and greatly increase their collective power. US Indo-Pacific Command (USINDOPACOM) and US Forces Korea have hosted frequent visits of our teams and experts to assist in surveying and hardening their military critical infrastructure in advance of any contingencies in East Asia and the Western Pacific. US Transportation Command (USTRANSCOM) has benefitted from similar assistance in support of its global operations and commitments. In Europe we assisted USEUCOM, NATO allies, and other partners to secure their networks from foreign interference. Finally, our efforts helped US Southern Command (USSOUTHCOM) and USNORTHCOM in election security, border security, and disaster recovery efforts.

Evolving national and departmental guidance creates opportunity for timely cyber operations in support of the combatant commands and in our role in the Chairman of the Joint Chiefs' global integration efforts. This includes both planning cyberspace operations support to trans-regional campaigns and prioritizing the allocation of high-demand, low-density cyber assets across the commands and in all phases of conflict. The Department and the Chairman have clarified the command and control of cyberspace forces, and in accord with this guidance we are building "cyberspace operations integrated planning elements" (CO-IPEs) at each combatant command.

The new, Service-like authorities and responsibilities that USCYBERCOM gained as result of elevation are similar to those authorized for USSOCOM on behalf of the nation's Special Operations Forces. USCYBERCOM is the Department's Joint Force Provider and Joint Cyberspace Trainer for cyberspace forces. In these roles, we develop strategy, doctrine, and tactics; prepare and submit program recommendations and budget proposals; exercise authority, direction, and control over the expenditure of funds; validate requirements; establish priorities for requirements for cyberspace capabilities, forces, training, and operations; and ensure the inter-operability of equipment and forces. We are working with the Department to build approaches across the force and leverage these new responsibilities to better measure, access, and improve the quality and readiness of the entire cyber force.

Improving Readiness. The rapidly evolving cyber domain makes achieving and maintaining force readiness a challenge. Similar to other Department forces, the readiness of our cyber forces can be understood as a two-part equation. First, we are evaluating the readiness of the teams that the Services (under their man, train, and equip missions) present to the Command. Second, we are studying the readiness of those teams to perform the missions they have been assigned by USCYBERCOM, something we refer to as "mission posture."

The Cyber Mission Force completed its build in May 2018, and we started formally reporting team readiness in the Defense Readiness Reporting System (DRRS) shortly afterward. USCYBERCOM is working with the Services to ensure that they present cyber forces that meet a common, joint standard so that the Soldiers, Sailors, Airmen, and Marines coming to the Command have proficiency with foundational cyberspace tools, techniques, and procedures. As part of that plan, the Services recently assumed the training mission for personnel in the CMF that USCYBERCOM (together with NSA) had overseen during the build. We are refining training curricula and standards, as well as simplifying and updating course requirements so we can ensure the right number complete their training with the appropriate skills.

The second part of the equation—mission posture—is not as accurately reflected by traditional metrics. Thus we are developing metrics that go beyond those traditionally used in order to capture cyber-unique requirements such as authorities, accesses, capabilities, and

intelligence. Such dependencies are not always measured in conventional DoD readiness reporting, yet they play a critical role in generating successful cyber operational outcomes. Our goal is to ensure operational proficiency in our CMF teams by taking an appropriately holistic view of readiness and applying resources to shortfalls. Working with the Services and the Department, we will develop and institutionalize the changes necessary for us to accurately measure and maintain team and mission readiness across the CMF.

To help sustain an advanced cyber force, all of the Services are applying hiring and retention incentives (especially for high-demand, low-density skill sets) as well as utilizing the flexibility in managing talent that Congress recently granted us by authorizing the new Cyber Excepted Service. The retention of top talent—particularly in some critical, high-skill jobs—is a significant concern because it will be crucial to our continued success. We track attrition closely, as the competition with the private sector and other government agencies for talent will be an enduring challenge. An important element of building certain low-density skill sets, moreover, is outreach to and utilization of our Reserve Component.

Underpinning our readiness are the operational lessons we learn from continuous operations in cyberspace. Operations in support of JTF-Ares and the counter-terrorism fight, the security of the 2018 midterm elections, and ongoing support to combatant commands across both the defensive and offensive mission sets, are improving our training, informing how we structure our teams, and indicating how best to employ our capabilities and teams.

Enhancing Partnerships. Securing the nation in cyberspace requires whole-of-nation efforts and effective collaboration with allies. It is a priority for USCYBERCOM to expand its ability to collaborate effectively with other government agencies, the private sector, academia, and allies. We must do this because they directly and indirectly complement and enhance our warfighting capabilities; indeed, enabling our partners is a key element of persistent engagement. We are working with a range of partners who support, enable, and assist our operations.

The National Security Agency is our most important partner; the strength of this relationship will remain critical to the defense of the nation. The Agency's world-class

expertise, technical capabilities, and accesses are crucial to USCYBERCOM's success. The USCYBERCOM-NSA relationship is proving mutually beneficial as the Command has matured. Indeed, I believe the speed and agility that USCYBERCOM and NSA demonstrated in joint operations to defend last fall's elections is evidence of the mission benefit of unity of effort and direction, the close proximity between USCYBERCOM and NSA, and our joint focus on outcomes for the defense of the nation.

USCYBERCOM works daily with partners in DHS, FBI, and other federal agencies, sharing information and intelligence, as the U.S. government furthers efforts to work even more effectively with the private sector. Since May 2018 we have worked to broaden these ties, both at the leadership and the action-officer levels. I have mentioned last fall's whole-of-government effort to defend the mid-term elections, but our collaboration with interagency partners is continuous and far broader. We interact constantly with the US Coast Guard's cyber forces and have Coast Guard senior officers integrated in USCYBERCOM. In addition, the CYBER GUARD exercise last year included USCYBERCOM, DHS and FBI elements practicing a whole-of-government response to an incident involving the nation's critical infrastructure.

We see growing partnerships with industry (particularly in critical infrastructure sectors like energy and finance) as a natural extension of such relationships. Working with the DoD-Chief Information Officer and NSA, USCYBERCOM has developed a Pathfinder program with DHS, sector-specific agencies, and select critical infrastructure partners to share threat information, conduct collaborative analysis of vulnerabilities and threats, and mitigate those risks. This whole-of-nation collaboration is crucial to our ability to deter or defeat strategic threats to US national interests and infrastructure. This is a complex mission in both technical and policy terms, in part because our work in this field occurs at the request of and in collaboration with federal government partners, particularly DHS and FBI. Recent changes to our policy guidance -- especially those crafted in agreements with these and other agencies – have brought clarity to this process. By partnering with DHS, FBI, and sector-specific agencies we are building persistent presence to improve the resilience and the defense of our nation's critical infrastructure.

USCYBERCOM has been active with current and prospective foreign partners, especially countries contemplating or building their own cyber forces. We have integrees from our "Five Eyes" partners (including a Canadian brigadier general) on the Command staff. USCYBERCOM in FY 18 conducted bilateral cyber exercises with France, Estonia, and Japan, while two dozen countries sent observers to our annual CYBER FLAG exercise last June. We also provided advanced training to a FVEY partner via our first Foreign Military Sales case, and provided defensive operations guidance to Singapore. Lastly, we maintain robust operational relationships with a variety of international partners in the continued fight against violent extremist organizations globally.

We are building strategic depth in our cyber forces with assistance from the Reserve Component, and in so doing are assisting the whole-of-nation effort to secure our networks. Reservists serve in positions across our headquarters staff, the Cyber Mission Force, and our Service cyber components, as well as playing vital roles in our exercises and training for defending critical infrastructure. Indeed, our Reserve strategy seeks innovative ways to utilize the Reserve Component in unique missions. Finally, Reserve Component personnel not only bring important skill sets to USCYBERCOM, they also enhance our efforts to create cybersecurity coalitions of public and private partners, particularly with industry innovators.

Our engagement with the National Guard Bureau and the 54 state and territorial Adjutant Generals is continuous. We created a framework for DoD to sponsor access to classified information for National Guard personnel supporting local and state election systems while in a State Active Duty status (this was done in coordination with DHS and the National Guard Bureau). We are also exploring options with the National Guard State Partnership Program (SPP), which fosters trust with foreign militaries through bilateral engagements with roughly 70 partner nations. While our Command develops our global partnerships in the cyberspace domain, my intent is to work through the geographic combatant commands in growing theater security cooperation efforts.

Deploying Infrastructure. The Command depends on innovative cyber tools and capabilities in crafting strategic and tactical options for senior leaders. The DoD Chief

Information Officer and the Services are making necessary investments, in both funding and in finding the right people to develop and maintain cyber tools and capabilities. These Service investments need to continue and be balanced against global mission requirements. Such investments feature the right mix of capabilities for USCYBERCOM to achieve its readiness goals and generate successful mission outcomes.

Our cyberspace forces require a comprehensive, integrated cyberspace architecture to achieve and sustain the insight, agility, and lethality necessary for maintaining competitive advantage against near-peer adversaries. Over the past year we have developed the Joint Cyber Warfighting Architecture (JCWA) to guide capability development priorities to this end. The JCWA has five elements: common firing platforms at our four cyber operating locations (each operated and employed by our Service cyber components) using a comprehensive suite of cyber tools; a "Unified Platform" for integrating and analyzing data from both offensive and defensive operations with intelligence and partners (including the private sector); joint command and control mechanisms for situational awareness and battle management at the strategic, operational and tactical levels; sensors that support defense of the network and drive operational decisions; and a Persistent Cyber Training Environment where teams can train and even rehearse missions under realistic conditions. The JCWA is not a fixed future state, but rather an adapting set of capabilities continually evolving along with technological change, operational outcomes, and shifting threats. The Department has leveraged the architecture to make critical JCWA program investments that, when realized, will allow us to not only gain advantage in competition with cyber adversaries, but also to fight and win in conflict.

Acquisition authorities are also a critical enabler for us. I thank this Committee and Congress for extending our tailored acquisition authority through FY 2025, and will work with the Department to implement and recommend refinements. That extension allows us to craft more contract actions under our current authorities rather than having to leverage existing contracts held by other partners. In FY18 we executed 32 contract actions totaling $43 million, and we could reach as much as $75 million in this fiscal year. Our acquisition priorities include the geographically distributed set of redundant and reliable infrastructures noted above as well as a virtual arsenal of capabilities (comprising both open-source and high-end tools);

implementation of cloud and engineering services in support of a big data platform; foundational architecture portions of the Command's continuous monitoring capabilities; and a competitive cyber tool contract. Cyber tools can be highly perishable, unlike conventional munitions, but they are also like munitions in that, as they are expended, we must continuously invest in their development and procurement.

Conclusion

Thank you again for inviting me here today on behalf of U.S. Cyber Command. Your continued support is vital to the work we do, both to enable our partners and to act in cyberspace on behalf of our nation. USCYBERCOM made significant progress in the past year. We have been elevated to a Combatant Command and are maturing in our new responsibilities. All of our Cyber Mission Force teams are built and, in conjunction with the Services, we are working to enhance and sustain their readiness. The Department is investing in essential operational infrastructure and is committing additional resources to build the Joint Cyber Warfighting Architecture that the Command needs. Enabled by new law, policy, and mission guidance, we are conducting operations every day – both to support combatant commands and forces engaged overseas, and to contest cyber adversaries in defense of the nation. Persistent engagement initiatives, like the operations conducted in partnership across government, with allies, and with the private sector in defense of the 2018 elections, will cumulatively impose cost on our adversaries and change their risk calculus for future operations.

Looking ahead, the work we have done to date may soon seem both crucial and preliminary. We are in continuous daily contact in cyberspace with capable adversaries determined to erode our nation's strategic advantages. Our efforts to act against them and to enable our partner combatant commands, government agencies, and allies have helped to defend our nation and its interests. Those efforts, however, must rapidly become more agile, more capable, and more sustainable. My vision for the Command encompasses a continuous role for our forces in making our fellow combatant commands and our whole-of-nation partners even more effective in competition with adversaries and in preparing for and acting in conflict.

We have much work ahead, of course, and your continued endorsement and assistance are both necessary and gratefully appreciated. Our people are superb. They merit your trust, and, with your support, USCYBERCOM will continue to meet every challenge, in both competition and conflict.