STATEMENT OF

THE HONORABLE LUCIAN NIEMEYER

ACTING ASSISTANT SECRETARY OF THE NAVY
(ENERGY, INSTALLATIONS AND ENVIRONMENT)

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS
AND CAPABILITIES AND SUBCOMMITTEE ON READINESS

of the

HOUSE COMMITTEE ON ARMED SERVICES

OCTOBER 16, 2019

Good afternoon Chairmen Langevin and Garamendi, Ranking Members Stefanik and Lamborn, and distinguished members of the Subcommittees. Thank you for the opportunity to discuss the programs and policies within the Department of the Navy to improve the resilience of our installations, ranges, and infrastructure.

Since the release of the National Defense Strategy (NDS) in February 2018, we have revised our priorities to ensure that our installations, the platforms from which we generate and project naval power, are resilient to an ever-growing range of threats. Installation resilience represents a multi-domain, multi-dimensional challenge. It is present in the physical and virtual operating space, requiring the Department to address threats in one or more areas individually or simultaneously.

We are continually assessing the impacts on mission resiliency from an increasingly complex security environment defined by rapid technological changes and challenges from adversaries in every operating domain. Many of the risks and vulnerabilities we must address today did not exist a decade or even five years ago. While concerns of installation resilience have in the past focused on natural impacts, the range of adversary threats today represent a growing and even more demanding challenge.

The NDS outlines two threat imperatives that are guiding our assessment and prioritization of installation resilience:

1) **The homeland is no longer a sanctuary.** America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated.

2) **Today, every domain is contested - air, land, sea, space, and cyberspace.** For decades, the United States has enjoyed uncontested or dominant superiority in every operating domain. We could generally deploy our forces when we wanted, assemble them where we wanted, and operate how we wanted**.** That is no longer the case.

As a result, we continue to make difficult choices and prioritize competing resilience requirements to field lethal, resilient, and rapidly adapting naval forces capable of defeating any threat. The Department defines installation resilience as the ability of naval platforms around the world to accomplish their missions despite the actions by adversaries or other events to deny, disrupt, exploit, or destroy installation-based capabilities.

Looking to the future, the quality of installation resilience directly impacts the entire spectrum of military operations from force development through power projection and force sustainment. The Department is tackling these challenges holistically across six broad categories of resiliency: contingency, energy and water, data and network, control systems cybersecurity, physical security, and environmental resilience. In addressing these requirements, the Department incorporates requirements for resiliency as a crosscutting consideration for our installation planning, design, construction and sustainment processes rather than as a separate program or specific set of discrete actions.

Contingency Resiliency

The Department's ability to protect our Nation's interests and those of our allies around the globe requires the resilience of our main operating bases to increase; the survivability of expeditionary advanced bases, forward operating bases, and cooperative security locations are equally important.

The Department sees a significant long-term risk to the resiliency of our installations domestically and around the world from the exertion of political will to limit access to, or operations from military bases and on ranges. The NDS addresses this imperative by prioritizing the strengthening of our alliances and attracting new partners as crucial to our strategy, providing a resilient, asymmetric strategic advantage. This concern is particularly acute overseas as adversaries employ various forms of coercion, activism, or economic levers to influence host nations or allies to limit cooperative security activities with the United States and access to ports, facilities, airfields and other infrastructure. We remain engaged in a series of initiatives to sustain worldwide access to infrastructure critical for the Department of the Navy to protect open sea lines of communication and other national objectives for our country and our allies.

Our adversaries also have the ability to strike the large centralized concentrations of forces we have assembled around the world. In response, we are prioritizing the authorities, policies, and resources needed to transition from large, centralized, unhardened infrastructure to smaller, dispersed, resilient, adaptive basing in multiple theaters that includes active and passive defenses. We have initiatives underway to develop new locations within the Europe and Indo-Pacific regions for the placement of forces. These initiatives will include measures to mitigate risks in cyberspace and use of foreign telecommunications infrastructure and port facilities. We will need to quickly construct facilities needed to support rapid force dispersal and protection.

While we have prioritized military construction requirements for munitions deliveries to theater, we still have significant challenges with resilient storage for new generations of high-yield munitions in theater.

We must also address resilient and agile logistics to include access to fuel around the world and on future battlefields. We are in the process of prioritizing facility requirements for prepositioned forward fuel, stocks, and munitions, as well as non-commercially dependent distributed logistics and maintenance to ensure logistics sustainment while under persistent multi-domain attack.

The Department of the Navy is integrating advanced technologies and concepts, to include cyber protection, in energy demand reduction, power generation & distribution, as well as fuel surety and distribution in order to enhance the effects of combat power to produce decisive results.

Energy & Water Resiliency

A revolution of technological change in our country is occurring, and it is driven by artificial intelligence, robotics, autonomous systems, machine learning, advanced telecommunications and additive manufacturing. These changes impact both society and our Nation's security and have ONE common critical enabler – electricity. As energy does more, we also NEED MORE electricity to power new generations of vehicles, sensors, robots, cyber forces, directed energy weapons and artificial intelligence. The quality of electricity will matter too – the Navy's future infrastructure, weapons systems, and communications will be controlled by systems sensitive to fluctuations in voltage or frequency. On the battlefield, future warfighters will need exponentially more energy with rapid recharge and resupply

capabilities to adapt and prevail in future conflicts. Our adversaries are already seeking to counter these superior technologies with low technology, inexpensive approaches designed to deny, disrupt or attack our energy supply and distribution systems both at home and on future battlefields. They are also using access to energy as a coercive tool to influence political decisions regarding alignments with U.S. policies and interests. Most alarmingly, our infrastructure is being tested and probed today; cyber threats to our electrical grid are real and growing.

The Department's mission assurance is a key input into defining installation resilience requirements and ultimately mission critical energy and water resiliency gaps. Our dependence on the public and private sector means they too must be integrated into the installation resilience defense team.

During FY19, the Department of the Navy conducted energy resiliency planning at fifteen high priority bases resulting in Installation Energy Plans that identify resilience gaps on and off the installation. The Navy is executing over 20 critical power energy resiliency projects (>$15M) to install, repair, or upgrade various generation, switchgear, control, and uninterruptable power systems for Fleet and other mission critical activities that provide special warfare, satellite, computer, and radio / telecommunications capabilities around the globe. Additionally, the Navy saved over $20M through the execution of 55 Mobile Utility Support Equipment missions to provide energy resiliency in support of mission critical and Fleet readiness requirements, and natural disaster relief.

The Department's robust mission assurance assessments have highlighted resilience, reliability, and cybersecurity gaps both on and off the base. As a result, the Department has implemented energy focused governance processes to mitigate its highest priority energy resilience gaps (e.g., the Energy Mission Integration Group). By bringing multiple resiliency issues into an integrated Navy and Marine Corps planning and governance process, the Department is able to pursue innovative solutions involving communities, industry, and other Federal agencies.

As an example at Marine Corps Air Station Miramar, through a series of initiatives and aggressive execution, we now have the ability to operate the base for up to three weeks without commercial power. The new power plant for our Navy base at Guantanamo Bay incorporates a multi-fuel power solution using liquefied natural gas (LNG) as its primary fuel. This solution enables this remote outpost to operate for 30 days (dependent on loads) without refueling; and finally, if LNG supplies were disrupted the system is capable of operating on diesel fuel.

We are pursuing similar goals for other critical platform installations for both the Navy and Marine Corps.

Moving forward, we are building upon our successes by expanding the use of Congressional authorities to acquire energy resiliency through Inter Government Support Agreements (IGSA), Other Transaction Authority (OTA), Utility Privatization (UP), Energy Savings Performance Contracts (ESPC), Utility Energy Service Contracts (UESC), Enhanced Use Leases (EUL), and the Defense Community Infrastructure Program. The Department is also appreciative of Congressional support for the Energy Resilience and Conservation Improvement Program (ERCIP) that allows us to target military construction funds to projects that are moving the needle on our energy resiliency and conservation goals.

Installation resilience depends on innovation and flexibility to use a vast array of fuel resources effectively and efficiently. We are pursuing all types of energy sources and have reached out to local utility service providers and experts in the private sector to collaborate on initiatives to reduce vulnerabilities, add redundancy, or improve energy management. The Department is also considering working with the Department of Defense (DOD) to explore the feasibility of stationary micro-reactors to provide long-term energy resiliency to our U.S.-based installations and is working with the recently established Navy Battery Development and Safety Enterprise Office to participate in the development of enterprise-wide battery standards and the safety of lithium-ion batteries. Additionally, the Department is exploring a digital twinning effort to include creating digital replicas for utility and telecommunications to support new platforms and major modernization efforts.

In pursuit of our goal to improve our access to sustainable water sources in drought-prone areas, we are working on cooperative regional management action plans and a review of water rights to benefit both the Department and local communities that want to continue to enhance local economic development. To meet the committee's interest in increased water conservation, we have recently stepped up our collaboration with industry leaders to improve water conveyance systems to reduce loss, recapitalize aging infrastructure and meet installation mission requirements.

Data and Network Resiliency

In response to the increased role data and information play in maintaining our maritime competitive advantage, the Secretary of the Navy recently ordered the establishment of a new Special Assistant for Information Management and Chief Information Officer (CIO). The CIO is supported by two three-star deputies aligned to the services with four subordinate directorates including: a Chief Technology Officer to design a fully integrated digital mission capability platform; a Chief Data Officer to harness the power of raw data; a Chief Digital Innovation Officer to leverage emerging technology to deliver transformative capabilities; and a Chief Information Security Officer to protect data and information, regardless of where it resides.

The newly empowered CIO is chartered with developing and implementing an overall vision and strategy to guide the department over the next five years to modernize our technology, apply current and emerging technology to bring winning, transformative capabilities to our Sailors, Marines, and civilians, and defend our information by leaning in on cyber hygiene and operations.

From an installations perspective, we are tackling cybersecurity for Information Technology (IT) and Operational Technology (OT) separately. This integration of IT and OT data and network resiliency is the foundation for moving our installations to smart technologies, artificial intelligence and increased automation required to deliver efficiency and optimize the talents of our Sailors and Marines.

Our Nation has historically thrived upon the spirit of entrepreneurship and innovation to tackle bold infrastructure initiatives, and rapidly enhance economic prosperity in every corner of our country. These initiatives have also required collaboration with States and local communities to manage the impacts of rapid development. We now have a new opportunity to collaborate on the national development of small cell technology and a Fifth Generation (5G) network. In fact, collaboration is critical to our national security to reduce the threat of foreign cyberattacks to this revolutionary new infrastructure.

5G has the potential to significantly enhance our Nation's security by supporting new capabilities, intelligence sharing, and synchronized effects. The Department could use backbone 5G networks to upgrade training, planning, logistics, and unit performance at all its bases around the country. We know that

future militaries will depend on the quality and speed of the decisions, enabled by software, data, and artificial intelligence through wireless networks. Whichever country dominates 5G will gain an economic and military edge.

With a revolution of new 5G-enabled military capabilities, decisions of where to locate those new technologies, and the supporting industries, will be impacted by the security and resiliency of local power and telecommunications networks. The military value for the "base of the future" will depend on the availability and relative security of a small cell telecommunications infrastructure. As such, States and local communities have an economic stake in national defense and must take an active role now during permitting processes to ensure the development of local 5G infrastructure minimizes security risks.

In consultation with the Wireless Infrastructure Association and its members, we are in the process of updating a series of policies that will guide the secure deployment of wireless broadband, including small cell technologies on Navy and Marine Corps installations to ensure cybersecurity of 5G infrastructure. In February 2019, we authorized Navy and Marine Corps installations to participate in First Net. We believe participation in First Net will improve and enhance coordination among all first responders serving Navy and Marine Corps installations regardless of whether they report to the Department of the Navy, another federal agency, a State, County, City, or Tribe. We view our participation as truly a win-win.

Control Systems Cyber Resiliency

The rapidly advancing technology to enable smart cities and industries has outrun the security needed to protect our lives, privacy, and resources. The Department increasingly depends on integrated, digital control systems to govern and monitor many aspects of military installation and platform operations. Millions of control systems convert virtual commands into physical actions. Control systems enable every type of weapon system to respond to human or virtual commands. These control systems are vital to the operation of all U.S. critical infrastructure from dams, power plants, water systems, electricity distribution, to the oil and gas main pipelines we depend on, with 90 percent owned and operated by private industry. While digital technology improves efficiency, it adds risk and increases vulnerability to cyber exploitation or attack.

Recent intelligence and government warnings cite control system cybersecurity as a critical national security vulnerability with threats ranging from hostile governments, terrorist groups, and malicious intruders to disgruntled employees. Control systems are vulnerable to data theft, service manipulation or denial. In addition, cyber-attacks targeting building management systems can result in the incapacitation of key systems and infrastructure. In extreme cases, unsecured control systems can be exploited, threatening privacy, safety, and lives on our installations, in our homes, in our cars, and in nearly every public gathering place. Adding to the concern, any mobile device connected to publicly available networks affords bad actors millions more entry points for these types of attacks.

Responding to these challenges, the Department has engaged to reduce our risk and vulnerability starting with enterprise-wide inventories, cyber-hygiene initiatives, and deployment of an enterprise architecture to provide control system security and monitoring. The Navy has deployed a control system test-bed working with the private sector to enable rapid design, testing, integration and deployment of control system technologies at our bases. As a result, this year the Navy successfully built a framework to assess and reduce the risk of cyber vulnerabilities for facilities related control systems. The Navy has prioritized its investments and efforts towards cyber securing the facility control systems supporting its Defense and Task Critical Assets. To date, the Department has secured 144 of 187 known mission critical facility related control systems, with the rest currently in various stages of the Risk Management Framework process with a projected completion date of FY21.

Finally, the Department of the Navy is leading the DOD effort to detect, respond, and recover from cyberattacks to control systems by piloting the initial phases of DOD More Situational Awareness for Control Systems (MOSAICS).

Physical Security Resiliency

Keeping pace with current and emerging threats to the physical security of our installations and assets is criticality important to ensure continuity of our mission and the protection of personnel. Our most important capability continues to be the men and women of our Navy and Marine Corps Security Forces and we are committed to ensuring they have the training and equipment necessary to perform their jobs. In addition to well established anti-terrorism and force

protection standards, the Department is leveraging rapidly advancing physical security technologies to enhance the effectiveness of our Security forces as well as counter unique and emerging threats to Department assets. As an example, both the Navy and Marine Corps are moving out rapidly to deploy Counter-Unmanned Aircraft Systems (cUAS) at mission critical locations to mitigate the rapidly developing "drone" threat. Likewise, both the Navy and Marine Corps are employing the Defense Biometrics Identification System (DBIDS) at our installation gates and access control points to ensure personnel and visitors are properly vetted prior to coming aboard our installations.

We also include within the realm of physical security resilience the ability to test, train, and operate in areas free from foreign surveillance. In CY2018, the Navy was directly involved in 48 cases to protect equities related to capabilities, technologies, and the supply chain or in close proximity to sensitive areas through the Committee on Foreign Investment in the U.S. (CFIUS). We appreciate the passage of the Foreign Investment Risk Review Modernization Act (FIRRMA) to expand working interagency processes to identify, review, and advise about impacts of intended real estate transactions that could pose a national security threat to the Department's training, testing, and operations.

Finally, because the threat environment is continually changing and it is imperative that we apply our investments to counter the most current and emerging threats, the Navy and Marine Corps have developed robust Mission Assurance programs and aggressive installation assessment schedules. The specific purpose of this program is to provide Department of the Navy leadership with the most current threat assessment and vulnerability analysis for our installations and recommend solutions to ensure maximum return on future investments in personnel, technologies, and projects.

Environmental Resiliency

The DON faces an array of challenges for installations and ranges to be environmentally resilient. We consider the impacts of extreme weather, rising sea levels, land subsidence, wildfires, droughts, and incompatible development as factors restricting or altering our ability to train, test, and operate.

Most recently, we are recovering and restoring critical weapon system test and development capabilities at Naval Air Weapons Station China Lake in the

aftermath of earthquakes that struck outside Ridgecrest, California in July 2019. In our review of damage, it is starkly clear those modern facilities designed with seismic features fared far better than older facilities previously built to code, but lacking special engineering features based on current understanding of earthquakes. As we proceed with design and construction efforts this year, we will be engineering stronger, more resilient facilities capable of withstanding future earthquakes and other threats.

We approach these challenges within a fixed topline that forces us to prioritize investments among a myriad of competing mission requirements. It is difficult to predict where the next hurricane, flood, tornado, or earthquake will hit. As a result, we prudently respond to unique environmental conditions during the planning and design of a facility by addressing the location of a facility, wind and snow loading, the placement of building systems and special structural considerations. We are also working with regions and communities to develop comprehensive engineering plans to reduce the impacts of flooding and geological subsidence. In some cases where we have waterside bases built on fill material that is eroding, we must work with local communities to restore sea walls.

The Department regularly updates its building requirements, known as Unified Facilities Criteria (UFC) to reflect updated or more stringent industry and local standards. For example, recently the Master Planning and High Performance and Sustainable Building Requirements UFC were updated to incorporate additional weather considerations.

Competition for air, land, sea space, electromagnetic spectrum, and other forms of encroachment continues to present a challenge to the resiliency of our ranges and the need for larger hazard areas to execute training, testing, and operations to meet NDS requirements. The Department appreciates the reliable support of Congress for the Readiness and Environmental Protection Integration (REPI) program, which we successfully use to reduce pressure from competing land uses and impacts to natural resources near installations and ranges.

Many environmental resiliency challenges require collaboration with local communities, States, other federal agencies, and industry leaders to develop regional plans to protect military capabilities. As an example, we are working closely with the State of California to ensure that future renewable energy development off the coast and in the Eastern part of the State will not negatively impact critical DOD training and testing ranges. Our goal is to support the

development of all energy sources while ensuring the resiliency of range capabilities that are required to support future generations of weapon system development.

The Navy has implemented a robust environmental compliance program for at-sea training and testing activities to ensure the Navy can meet its Title 10 responsibilities while balancing the need for environmental stewardship and conservation. Through implementation of the at-sea program, the Navy conducts training and testing activities in ways that minimize impacts to natural, cultural and other environmental resources to ensure the continued resiliency of the environment to support vital Navy missions. The Navy has worked diligently with environmental regulators to provide safeguards to important species and habitats, while preserving access to vital ranges, operating areas, and airspace, and providing the operators with flexibility in how they execute training and testing requirements to support rapidly changing operational demands.

The Department also implements a comprehensive conservation program under the Sikes Act, Endangered Species Act, and other environmental laws to conserve, enhance, and restore natural resources while achieving no net loss to the military mission. We have proactively engaged with federal agencies to ensure that their actions taken to promote environmental resiliency, such as the listing of endangered species, designation of critical habitat, and establishment or expansion of National Marine Sanctuaries and Monuments, are accomplished in ways to protect national security interests.

Our experience is that the resiliency of our installations is enhanced by integrating into, and not competing with, the environmental and economic activities of our surrounding communities. Over time, this resiliency has been tested by communities concerns about our military activities, even where Congress or regulators have provided specific designation for military readiness use or in areas historically used for naval operations. With shared long-term vision, planning and development, we continue to address and resolve community concerns and execute infrastructure projects, implement force movements, avoid financial obligations for mitigation measures, and maintain full naval training, testing, and operations.

Conclusion

The threats challenging installation resilience are multi-faceted, extending across domains and technical disciplines that require highly integrated and holistic solutions. The contributing factors are complicated, and interwoven into a threat continuum, whether energy reliability, C-UAS, digital controls, or environmental impacts. The broad spectrum of threats to our installations represent risks to the Navy and Marine Corps operating environment, missions, and the ability of built infrastructure to support force generation and power projection. Mitigating these risks must be prioritized among competing Department priorities. Absent stand-alone remedies, we rely on the application of appropriate mitigation and resiliency measures during the development of installation requirements to build a stronger and more adaptive platform to deter aggression and project power. The Department will continue to work with Congress, industry leaders, and our community partners to maintain the flexibility we need to evaluate risks both inside and outside our fence lines, and incorporate mitigations to those risks into various planning and management processes.

We appreciate the opportunity provided by your committees today to discuss initiatives to improve the resiliency of the Shore Domain. We hope to use this opportunity to continue to partner with Congress on actions to address our priorities. Installation resilience, in all its dimensions – those described here and emerging threats we have not yet encountered – is inextricably linked to the readiness and lethality of naval power to represent, and if necessary, defend America's interests anytime, anywhere.

End of statement