[H.A.S.C. No. 116–46]

RESILIENCY OF MILITARY INSTALLATIONS TO EMERGING THREATS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

MEETING JOINTLY WITH

SUBCOMMITTEE ON READINESS

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

HEARING HELD
OCTOBER 16, 2019

U.S. GOVERNMENT PUBLISHING OFFICE
39–804 WASHINGTON : 2020

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

JAMES R. LANGEVIN, Rhode Island, *Chairman*

RICK LARSEN, Washington
JIM COOPER, Tennessee
TULSI GABBARD, Hawaii
ANTHONY G. BROWN, Maryland
RO KHANNA, California
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
CHRISSY HOULAHAN, Pennsylvania
JASON CROW, Colorado, *Vice Chair*
ELISSA SLOTKIN, Michigan
LORI TRAHAN, Massachusetts

ELISE M. STEFANIK, New York
SAM GRAVES, Missouri
RALPH LEE ABRAHAM, Louisiana
K. MICHAEL CONAWAY, Texas
AUSTIN SCOTT, Georgia
SCOTT DesJARLAIS, Tennessee
MIKE GALLAGHER, Wisconsin
MICHAEL WALTZ, Florida
DON BACON, Nebraska
JIM BANKS, Indiana

Shannon Green, *Professional Staff Member*
Peter Villano, *Professional Staff Member*
Caroline Kehrli, *Clerk*

SUBCOMMITTEE ON READINESS

JOHN GARAMENDI, California, *Chairman*

TULSI GABBARD, Hawaii
ANDY KIM, New Jersey, *Vice Chair*
KENDRA S. HORN, Oklahoma
CHRISSY HOULAHAN, Pennsylvania
JASON CROW, Colorado
XOCHITL TORRES SMALL, New Mexico
ELISSA SLOTKIN, Michigan
VERONICA ESCOBAR, Texas
DEBRA A. HAALAND, New Mexico

DOUG LAMBORN, Colorado
AUSTIN SCOTT, Georgia
JOE WILSON, South Carolina
ROB BISHOP, Utah
MIKE ROGERS, Alabama
MO BROOKS, Alabama
ELISE M. STEFANIK, New York
JACK BERGMAN, Michigan

Jeanine Womble, *Professional Staff Member*
Dave Sienicki, *Professional Staff Member*
Megan Handal, *Clerk*

CONTENTS

Page

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

Prepared Statements:

Documents Submitted for the Record:

[There were no Documents submitted.]

Witness Responses to Questions Asked During the Hearing:

[There were no Questions submitted during the hearing.]

Questions Submitted by Members Post Hearing:

RESILIENCY OF MILITARY INSTALLATIONS TO EMERGING THREATS

House of Representatives,
Committee on Armed Services,
Subcommittee on Intelligence and Emerging Threats
and Capabilities, Meeting Jointly with the
Subcommittee on Readiness,
Washington, DC, Wednesday, October 16, 2019.

The subcommittees met, pursuant to call, at 2:55 p.m., in room 2118, Rayburn House Office Building, Hon. James R. Langevin (chairman of the Subcommittee on Intelligence and Emerging Threats and Capabilities) presiding.

OPENING STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, CHAIRMAN, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

Mr. Langevin. The subcommittee will come to order. I want to welcome everyone to this joint hearing today with the Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities and the Readiness Subcommittee. Today we will examine the resiliency of our military installations to emerging threats. Holding this hearing has been a priority of the subcommittee for the past several months, and I want to, in particular, thank Ranking Member Stefanik for her bipartisan cooperation to this hearing, and also I am thankful to my friends Chairman Garamendi and Ranking Member Lamborn for working so diligently in making this hearing possible.

So we are here today to ensure the Department is prepared to account for and address vulnerabilities—physical and digital—to our military installations at home and overseas. This includes the effects of climate change, energy dependence, land management, and cyber incidents, among others, on the threat assessments, resources, and readiness of our Nation's military. This also includes the risk to conducting operations both today and in the future.

This subcommittee as well as the Readiness Subcommittee have conducted rigorous oversight into installation resilience, but I continue to be concerned about what the Department is doing to ensure our installations are able to withstand ever-increasing threats from malicious cyber activities and severe climate events among other things. When it comes to our Armed Forces, we as a Nation have not given these threats to our installations the attention that they deserve. So I would like to remind those in attendance that this hearing marks 1 year since the Department suffered nearly

$10 billion in damage from just two extreme weather events at Tyndall Air Force Base and Camp Lejeune.

Now, I could not think of better examples of the perils our defense infrastructure faces from climate change, perils that will only increase as we pump more greenhouse gases into our atmosphere. So our committee has acted on a bipartisan basis to acknowledge these risks, but I must say I am disappointed in the Department's response to our oversight. By way of example, the initial accounting of at-risk bases we received did not even include Camp Lejeune or Tyndall Air Force Base at all. If those are the low-risk bases, one can only wonder what we are likely to see soon from the installations the Department identified as being of particular concern. So we need a clear accounting of the risks, with dollar figures attached, or else we will continue the cycle of throwing good money after bad, which is not only fiscally irresponsible, but places our service members and readiness at risk.

So I also want to make it clear to everyone that we will be holding an IETC [Intelligence and Emerging Threats and Capabilities] Subcommittee hearing specific to the emerging threat of climate change later this year.

Now, in addition to the threats posed by extreme climate events, the threats presented by attacks on cyber and energy infrastructure, by both state and nonstate actors, continue to grow and evolve at a rapid pace. So, these threats can target critical infrastructure on our military installations, including electric grid, water supply, or even medical facilities. An attack on our electric grid could have profound effects on the ability of the force to carry out critical missions. So we must increase the resilience of operational technology on installations, ensure we sufficiently focus on securing cyber-physical systems as well as traditional IT [information technology] infrastructure. So I am interested in hearing more about how the Department is building cyber resilience at installations at home and abroad.

It is incumbent upon the Department and Congress to ensure that we are properly preparing for these threats to installations, and I look forward to hearing from our witnesses on this topic. Before I turn to Ranking Member Stefanik, in the interest of time it has been agreed upon with the chairs and ranking members of the committee that we are going to forgo the witnesses' statements, since we have those for the record, and we are going to be going right into questions. So, with that, I would like now to turn it over to Ranking Member Stefanik, and then we will, in turn, hear from Chairman Garamendi and also Ranking Member Lamborn for their remarks.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 41.]

STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

Ms. STEFANIK. Thank you, Jim. I would like to start by thanking Chairmen Langevin and Garamendi, as well as my fellow ranking member, Mr. Lamborn, for holding this important hearing today to discuss resiliency of the Department of Defense installations and facilities. And welcome, of course, to our witnesses. We have a lot of ground to cover, so I will keep my remarks short.

As I think about resiliency of military installations and infrastructure, I am concerned about shortfalls in both the physical and digital domains. First, we remain vulnerable to extreme weather events and climate change. We have seen these events adversely impact public safety, our economic security, and our national security. Our intelligence community continues to assess that global environmental degradation and climate change are likely to fuel competition for resources, economic distress, and social discontent across the globe through 2019 and beyond. And we continue to experience extreme weather events at home, including in my own district in northern New York.

We must, therefore, factor in these environmental changes when discussing resiliency of military installations, and I look forward to hearing from our witnesses exactly how we are planning for these extreme weather events and climate change.

Second, and equally as important, I continue to have concerns about installation and infrastructure vulnerabilities in the digital domain. Congress, and indeed this very committee, had the foresight to understand these challenges, and 3 years ago we directed the Department to conduct a comprehensive review to evaluate cybersecurity vulnerabilities of DOD [Department of Defense] infrastructure. Unfortunately, this review and the subsequent corrective actions remain far from complete, and we are still incredibly vulnerable to attack. I feel we have not yet identified the scale and scope of our problems, let alone begun to mitigate our most concerning shortfalls. When we consider resiliency, we must remember that advances in information technology, cybersecurity, and information assurances are primary prerequisites for the future of warfare. These enabling technologies form the foundation where information and data are a strategic resource to be protected, preserved, and fully actioned. Only then will we be able to leverage evolutionary and even revolutionary technologies such as AI [artificial intelligence], 5G, high-performance computing, and even quantum computing. This future begins and ends with our facilities and installations, which will be our greatest resource or our weakest links. I look forward to discussing today how we can work together to ensure that resiliency in both physical and the digital domain is prioritized so that we are prepared for these challenges in our increasingly complex digital age. Thank you, and I yield back.

[The prepared statement of Ms. Stefanik can be found in the Appendix on page 43.]

Mr. LANGEVIN. Thank you, Ranking Member Stefanik.

I would like now to turn to the chairman of the Readiness Subcommittee, Mr. Garamendi, for his statement.

STATEMENT OF HON. JOHN GARAMENDI, A REPRESENTATIVE FROM CALIFORNIA, CHAIRMAN, SUBCOMMITTEE ON READINESS

Mr. GARAMENDI. Thank you, Jim. I really appreciate the opportunity to be here with you to work with you on this extremely important issue, and your committee and the Ranking Member Lamborn, who is on the other side. Installation resiliency is the foundation to readiness. Our bases and infrastructure investments must be able to withstand to the maximum extent possible the spectrum of resiliency threats from energy disruption, cyberattack, natural disasters, floods, fires, hurricanes, you name it—oh, earthquakes, too.

Both of our subcommittees have put in a lot of time into this, and we are going to continue doing it. Over the last year, we have seen the aftermath of extreme weather events such as Hurricanes Florence and Michael, and flooding at Offutt, and earthquakes at China Lake, and fires along the way, billions of dollars of damage. In fact, I think when we add it up, the entire year's worth of MILCON [military construction] construction could be consumed in just four natural disaster events at our bases.

Going forward, I know that my committee will insist that we be forward-looking, that we do assessments of the threats, from sea-level rise to weather events, and so that even the roofs get repaired. You know, maintenance, folks, rather important. Installation resiliency in its broader—is much broader than weather resiliency. The recovery from the disasters is equally important. I am interested in hearing what our witnesses have to say, and I want to thank them for their written reports. When taken together—and perhaps, Mr. McMahon, this is your task, to pull all of these together—if they were all done by all departments, it would be a very, very good—not start, but well down the path.

I have questions about the Department's preparedness for energy disruptions and cybersecurity. You have just heard that. We want to be sure that we are on top of those issues. Energy, water, sanitation, you name it, all of these things are important and all of this has to be taken into the account that we reduce our dependency and reduce our energy consumption along the way. A lot of things to do. The written testimony is excellent. I ask that all of us pay attention to it, and I would ask the four witnesses, when they go back to their jobs, some of which won't be there very long—we will take that up later—but when you go back, that you read the testimony from the brother and sister services. I think you will find it useful. And then inculcate that into your work. Thank you very much. I yield back.

[The prepared statement of Mr. Garamendi can be found in the Appendix on page 45.]

Mr. LANGEVIN. Thank you, Chairman Garamendi, I would like to now turn to Ranking Member Lamborn for any comments he may have.

STATEMENT OF HON. DOUG LAMBORN, A REPRESENTATIVE FROM COLORADO, RANKING MEMBER, SUBCOMMITTEE ON READINESS

Mr. LAMBORN. Well, thank you, Chairman Langevin, Chairman Garamendi, and Representative Stefanik for calling this joint subcommittee hearing on such an important topic. Installation resilience has always been important to our national defense, but given the dynamic and evolving nature of the threats we face, it is becoming even more critical. Most of our installations rely, at least in part, on power generated in nearby communities. At the same time, the Armed Forces have invested significantly in renewable energy. I am very interested to hear from our witnesses today regarding their efforts to improve energy resilience and efficiency on our military installations, as well as to protect it from capable and cunning adversaries.

Having recently visited all four bases damaged by storms and earthquakes that we are addressing in our fiscal year 2020 National Defense Authorization Act, I am also concerned about getting our work done quickly to fund the $5 billion necessary for reconstruction.

Without this funding, the critical missions will continue to be negatively impacted, including the air sovereignty and F–22 training missions at Tyndall Air Force Base; one-of-a-kind Navy research testing missions at China Lake; runway operations, tanker simulator, and critical missions of the 55th Wing at Offutt Air Force Base; and the Marines at Camp Lejeune and Cherry Point continuing to operate after approximately 800 buildings were compromised, with 500 severely damaged.

And we also owe it to our military families to ensure that the privatized military family housing is fully restored. The damage in North Carolina and Florida continue to create a burden for these families. So I look forward to hearing from our witnesses about how they are ensuring that we plan effectively, build to appropriate building codes, incorporate lessons learned from recent disasters, and inspect work on new construction to ensure that it meets specifications. Thank you for your testimony today, and I yield back.

[The prepared statement of Mr. Lamborn can be found in the Appendix on page 46.]

Mr. LANGEVIN. Thank you, Ranking Member Lamborn.

With that, now, because again of the delayed start due to votes, we are going to forgo the witnesses' opening statements. We are going to go right into questions. Before doing so, I would like to introduce the individuals that we have with us today.

Mr. Robert McMahon, Assistant Secretary of Defense for Sustainment. Mr. McMahon, it is good to see you again. Thank you for being here. I understand that you are going to be leaving the Department next month, and I just want to take this opportunity to thank you for your many decades of service to the country both in uniform and in your current role now, and I wish you well in your next chapter. Thank you for being here today.

[The prepared statement of Secretary McMahon can be found in the Appendix on page 47.]

Mr. LANGEVIN. Next, Mr. John Henderson, Assistant Secretary of the Air Force for Installations, Environment, and Energy.

[The prepared statement of Secretary Henderson can be found in the Appendix on page 59.]

Mr. LANGEVIN. Next, Mr. Alex Beehler, Secretary of the Army for Installations, Energy, and the Environment.

[The prepared statement of Secretary Beehler can be found in the Appendix on page 70.]

Mr. LANGEVIN. And then also Mr. Lucian Niemeyer, Acting Assistant Secretary of the Navy for Energy, Installations and the Environment.

[The prepared statement of Mr. Niemeyer can be found in the Appendix on page 82.]

Mr. LANGEVIN. Thank you all for being here today. I look forward to a robust discussion today, and with that, I am going to recognize myself for 5 minutes. Members will be recognized after the chairs and ranking members in the order of seniority and attendance. So, with that, let me begin.

So the climate has changed significantly over the last decade, and—several decades, and it is going to continue more—to change more in the coming years. All of the services have incurred climate-related debt because installations were built with risk assessments that did not reflect the reality of today or the increased threats of the future. So my question is, what is your assessment of the unmitigated climate risk you face in your legacy installations in terms of dollars and cents, and what methodologies do you use to determine those risks?

Secretary MCMAHON. Mr. Chairman, I will begin and provide my comments, and I will give my peers the opportunity as well. First, thank you to you and Chairman Garamendi and both of our ranking members for the opportunity to be here today to talk about something that is equally as important to Secretary Esper, our respective service secretaries, and clearly to the four of us.

As we move forward, to your point, as we look out over the last decade or two decades, the challenges and threats that we face within our installations have grown dramatically. And as you have pointed out, it is climate. It is the challenge that we also face with regards to natural disasters, whether that be earthquakes, whether that be forest fires, whether that be deforestation or drought. In addition, it is the physical—and to Congresswoman Stefanik's point—the digital world as well, so it is this holistic approach that we have to look at when we deal with it.

Specifically to the climate, we have got to acknowledge that the climate is changing, the fact that we have seen, for example, a rise in our seas at the same time that, as we consume water, that we are seeing a degradation in our water supplies and the fact that that is having an adverse effect on our soils and our land as well. And so this holistic impact, as we look at the climate, how do we deal with that?

We look at the way that we proactively put together our standards, our building standards. They need to be continuously updated as we learn about what is occurring with these natural disasters. How do we update that? We need to be more proactive, but we also have to do it in the context that, as we look at the holistic challenges that we face within the Department and our installations, that that is just a single portion of it that we have to deal with. And so we have got to be aggressive with it, with new standards and where we have the opportunity to infuse those standards, and we do that, but we also have to do it in the context of the broader threat that we face.

Mr. LANGEVIN. Do you feel you have an adequate understanding of the dollars and cents involved?

Secretary MCMAHON. I don't. And to that point, recently I have asked the services to come back with an assessment of what that looks like. What I can tell you is, there is $4 billion worth of damage at Tyndall Air Force Base. There is more than $4 billion—or roughly $4 billion of damage at China Lake. So, as you look at that and try to apply that across the enterprise, there is a significant bill out there that I don't think we fully understand or comprehend the full cost of, just on the facilities, let alone when you start talking about counter-UAS [unmanned aerial systems], when you start talking about cyber, and the other elements, and we can throw EMP [electromagnetic pulse] in there as well. And so I don't think collectively we understand what the full assessment is.

Mr. LANGEVIN. Well, it is essential that we continue to drill down on this to get our arms around that because the taxpayers deserve no less, the Congress needs to know this information, and it is the right thing to do for the country and the military.

Secretary MCMAHON. Mr. Chairman, I absolutely agree and I would say that all four of us would agree with you, and it is getting our arms around that, and we are on the road to do that.

Mr. LANGEVIN. Secretary Beehler, Henderson, Niemeyer, do you have anything else to add?

Secretary BEEHLER. Yes, sir. The Army has benefited already from the fact that the U.S. Army Corps of Engineers has developed a climate assessment vulnerability tool using a variety of data from other Federal agencies that are constantly being refined and updated as they receive more and more data. That tool has been used and will continue to be used on an ongoing basis by Army installations as they do their every 5 years update in their installation management plans that certainly will address this issue, and they have been basically prescribed to do so, as well as the installation, energy, and water management plans that are ongoing for all of the major Army installations. And so, through that exercise, we will begin to get a handle on just exactly what the cost and other measures needed to be taken to address extreme——

Mr. LANGEVIN. When do you think those assessments will be completed?

Secretary BEEHLER. Well, at the—on the water and—energy and water plans, they are in three phases. The first phase, which covers the major or top critical mission priority installations of about 22, expected to be done by the end of this calendar year, and then the next tranche within 12 months' time afterwards and the third tranche 12 months after that. The installation management plans are upgraded and reviewed every 5 years. That covers roughly the 150 Army installations. And so, therefore, you have that incorporated at roughly about 30 installation plans a year.

Mr. LANGEVIN. And then, finally, to that followup, so the Army would then be developing strategies for addressing the risks identified from those assessments?

Secretary BEEHLER. I am sorry, sir. I missed——

Mr. LANGEVIN. I said, is the Army then planning to develop strategies once the assessments are completed?

Secretary BEEHLER. Oh, absolutely. And that is the wonderful thing about these several efforts that are going on simultaneously. Each will help the other to become a greater granularity in a way forward.

Mr. LANGEVIN. Well, that is going to be essential for us to follow up on that.

Secretary BEEHLER. Absolutely.

Mr. LANGEVIN. I am going to hold there, and now turn to Ranking Member Stefanik.

Secretary MCMAHON. Mr. Chairman, before you yield on this, I would like to add just one point. Secretary Beehler referred to the climate tool that is being used by the Corps of Engineers. We have just funded for all the services to be able to utilize that up to 15 bases stateside and 10 bases overseas for each of the services, recognizing the value of that tool and making sure that all the services can benefit from it.

Mr. LANGEVIN. Thank you for adding that important point.

Ranking Member Stefanik is recognized.

Ms. STEFANIK. Thank you, I am going to jump right into my opening remarks where I referenced our cyber vulnerabilities. As you know, in fiscal year 2017 NDAA [National Defense Authorization Act], section 1650 required a review of those vulnerabilities, and this review includes information and operational technology such as industrial control systems. So I want to start with OSD [Office of the Secretary of Defense].

Mr. McMahon, can you give us an update on where things stand with respect to implementation of 1650, and tell us what your role in the capacity of OSD is in overseeing this review to ensure we have identified and are correcting cyber vulnerabilities? Because my concern is that we have not yet identified the scale and scope of cyber vulnerabilities in our installations.

Secretary MCMAHON. Congresswoman Stefanik, I would agree with you that we have not fully sized that. As I think you are aware, the Under Secretary for Acquisition and Sustainment Ellen Lord has recently brought on an expert, Ms. Katie Arrington, whose purpose is to oversee cybersecurity for the Department for both acquisition and sustainment. Her focus early on is ensuring that we are considering, as part of the supply chain, what that looks like, but also looking across industrial control systems throughout the Department and is leading that effort in conjunction with the CIO [chief information officer] to give us the appropriate view and understanding of what the threat is and, more importantly, how we deal with that holistically both on the acquisition and the sustainment side.

Ms. STEFANIK. So, when I ask who the lead for 1650 implementation, it is a combination of Katie Arrington and the CIO [Dana] Deasy?

Secretary MCMAHON. As well as in specifically as we get into industrial controls, would be myself.

Ms. STEFANIK. Okay. So the fiscal year 2017 NDAA was a couple years ago.

Secretary MCMAHON. It was.

Ms. STEFANIK. And the fact that we are now getting an answer about who is responsible, what has happened in between?

Secretary MCMAHON. I think what I would tell you is there has been a tremendous amount of discussion about what we need to do in understanding, characterizing what the threat is, what it looks like, the amount of execution, and, to your measure and my measure, is what is actually in place, not the level that I would expect to have at this point in time.

Ms. STEFANIK. So can you provide characterization of what that threat is and what our assessment is?

Secretary MCMAHON. I would be happy to provide that. I would like to take that for the record, to come back to you in detail to answer that.

Ms. STEFANIK. Okay. I think this highlights again my concern with not even understanding the scale and scope, let alone what our mitigation efforts are going to be. So I look forward to getting that response for the record because again we have had years since that language was written in the fiscal year 2017 NDAA, and I was here when we did that.

[The information referred to was not available at the time of printing.]

Ms. STEFANIK. I want to move to Mr. Henderson from the Air Force and then Mr. Niemeyer from the Navy. Both of you addressed this in your written opening statements. How have you both worked to identify digital vulnerabilities, and how much work would you say remains to be done and when do you expect to complete the review?

Secretary HENDERSON. I thank you. For the Air Force, there has been a number of assessments going on, and like Mr. McMahon, in the installations portfolio we focus primarily on the industrial controls piece of that assessment. But there is—across the Air Force, this crosses a number of staff functions that are working on this. So, for instance, there is several cross-functional teams working a number of areas, and I am just going to list a few of them just so that—just to give appreciation for the group of the breadth of assessment that is going on. But they are doing full threat assessments going up to a very highly classified level. There is actually going to be an Air Force senior leader summit on this. Actually, this work is coming to culminate at a summit here in about 3 weeks in the middle of November: these cross-functional assessments going on with weapons system security, something called the Air Force Risk Executive Mission Assurance, which covers 17 programs; supply chain risk management; Air Force control systems, which is a sprint that we are working with, with our A4; mission defense teams that are focused on several areas to include cyber—command cyber readiness inspections; the protection of critical technology; supervisory control and data acquisition, or SCADA systems; and so on. So there is a large group of people working in a cross-functional way to address this holistically with the Air Force, and we expect to bring this to our senior leaders here in about 3 weeks, about the middle of November.

Ms. STEFANIK. Three weeks, okay. So that would be the complete review.

And, Mr. Niemeyer, from the Navy, you have 30 seconds, sorry.

Mr. NIEMEYER. So what we—I think we are leading the services as far as our ability to enclave some of our critical facilities. We started with what we considered to be our tier 1 and tier 2 most critical facilities across Department of the Navy. We have already taken steps to separate those critical control systems in those facilities, and we are now moving towards the long-term mitigation of those systems. We are also looking at assessments at the next level. We have completed hundreds of assessments and started on real-world mitigation efforts to start a short term to isolate the problem and work on long-term solutions.

I will tell you, ma'am—I have been spending a lot of time on this issue—we really need a national policy and a national answer on how we address control system security. I would also like to get to 5G if I can. We are working very aggressively on that, but I am not sure that was the exact intent of your question, but I would love to get there as well.

Ms. STEFANIK. So we can get to 5G later on, maybe with a second round of questions. Again, I just want to highlight my concerns. We wrote the language that was signed into law in the fiscal year 2017 NDAA, and it is concerning to me that the implementation has lagged. So we don't even have our arms around the scope of this problem, let alone the mitigation. I appreciate all the work the service is doing.

I yield back.

Mr. LANGEVIN. Thank you, Elise. I now recognize the chairman of the Readiness Subcommittee, Mr. Garamendi.

Mr. GARAMENDI. First, I want to thank, Jim, you and Ms. Stefanik for the work you have done on cybersecurity. You have really pushed that forward. And I know, Mr. Chairman, you have also pushed the climate issue forward.

I want to really go to the documents that the four of you have submitted to the committee. Mr. McMahon, you have kind of given us a going-away present. And to the services, the same thing. If they were to carry out the things that you laid out in your memo, we would be well down the line on each and every one of these. There are some things that are missing, and we will identify those as we go along. Specifically, in the new NDAA that is hopefully going to get completed in the very near term, there is a requirement that every base have a plan that includes all that we have talked about here, weather related, flood related, other kinds of threats to that base. So we would expect—well, you should expect and your successors should expect, to get what Ms. Stefanik just gave you a few moments ago, and that is, what have you done about this particular issue. Good for her, and for you, not getting it done yet. So I want to just basically put to each of you, among the things that you have written in your—submitted in your testimony, what is the most important? You don't have to answer the cybersecurity. We have already taken care of that piece of it. Let's start at this end of the table and then go down. Mr. Niemeyer.

Mr. NIEMEYER. That would be great, thanks so much, Mr. Chairman, for the question. The most important thing for us is strategic contingency risk. We have a concern worldwide about our access to installations, ports, airfields. From a resiliency long-term aspect that to us is probably the most important factor that allows us to continue to project naval power to protect the sea lanes and to protect our interests for both ourselves and our allies. Right behind that is energy and water security risk, and right behind that is, I would say, data and network risk, and the ability to secure our control systems. Then we have got physical risks. Right now, Department of Navy and our sister services are working a counter-drone, counter-UAS strategy, to look at new kinetic threats to our bases in addition to traditional ones.

And then we also have what we would call an environmental risk, and it is just a range of factors, as you know. We are getting a lot of support from the committee in our response to China Lake. That was an earthquake. You know it is tough to predict where the next earthquake is going to happen or the next tornado or the next tsunami. So we are working on environmental risk from a holistic perspective. We do roll this up into what we call a mission assurance framework. I would love to come back and talk to the staff about how we can get some support from the committee on taking the mission assurance framework, so we are starting at the most critical facilities around the Department of the Navy that support national missions and how we can develop a comprehensive plan to identify the most critical vulnerabilities across the whole domain of threats that face us—not just natural, but we think man-made, or adversary threats are much more substantial. How do we address those for each of our critical facilities?

Mr. GARAMENDI. The new NDAA will give you the direction to do that or the requirement to do that. And I would like to know what you need that you don't presently have to do that, but that will be—come back at us. Mr. Henderson.

Secretary HENDERSON. Yes, thank you. For the Air Force, we are doing something called mission threat analysis. So, instead of doing this threat assessment by base—and a lot of our bases have many different missions on them—we are taking the mission itself and looking at the whole mission chain because it takes a global—it takes a global network of facilities to do some of our missions. So we take the full mission, and we look at the vulnerabilities there. And there is a whole host of threats, as Mr. Niemeyer said, and I won't go back through them, but this isn't just about cyber or just about weather or just about climate. This is the whole vast array of threats facing our installations that we have to look at. And so——

Mr. GARAMENDI. I will let you off there.

Mr. Beehler.

Secretary BEEHLER. Sir, in addition to what has already been mentioned by my colleagues of the other two services, the Army also focuses on the fact that, as the National Defense Strategy from 2018 has said, that the homeland is no longer a sanctuary. And for us that means that our installations are directly part of the battlespace, of the battlefront, and part of the strategic support area. So that is where we——

Mr. GARAMENDI. You have 24 seconds. I am just going to wrap up here. I have read that, and I think the rest of us can read it also. Here is my point and the reason I asked the question: Each of you has set out a set of priorities generally, and then you narrowed it down granularly, the word we use nowadays, to specific actions. Here is what I want you to do for the next month and a half, and that is read your colleagues' work and figure out what you are not doing that they are doing. And if you would stick around another month and a half, Mr. McMahon, I would ask you to do it also or see that they got it done. There is extraordinary opportunity and necessity that your—the other services are involved in that one or the other of you are not doing. And so I want you to—the other, you know, get a big pot of coffee and sit down and read each other's work. The solutions are all there. And you got to tell us what we need to do to give you the tools to carry out those solutions.

With that, I yield back.

Mr. LANGEVIN. I thank the gentleman, and now Ranking Member Lamborn is recognized.

Mr. LAMBORN. Thank you, Mr. Chairman.

Mr. McMahon, I am going to address this to you. Because of sake of time, I can't have everyone answer this question, and I want to thank you for your service to our country as you go into, like the chairman said, your next chapter.

In my recent visits to survey the damage at Tyndall, Offutt, and China Lake, I was struck by how much that advanced planning and up-to-date construction techniques can help mitigate when disaster strikes. So what have we learned from recent natural disasters of all types to make things better in the future, for more resiliency? And I am thinking, for instance, of sacrificial first floors. They are doing that at Offutt. You don't have all the expensive HVAC [heating, ventilation, and air conditioning] and computers on the first floor, in case you have a flood. You put them up higher. So what are some examples of what we are learning?

Secretary MCMAHON. Congressman Lamborn, what I would tell you is, that as we look at the lessons that we have learned, there is a variety of—rather than get into specifics, as you look at we establish our essentially building standards, which is a continuous process to update, we take the lessons that we learned from each of these installations, whether it is the construction, whether it is the roofing, what we are doing on one floor versus another. And roll that in on an annual basis to continuously update what those standards are, to ensure that as we get to the next either rehab or new construction, that those standards are, in fact, reflected in the way that we build the facility.

Mr. LAMBORN. Okay, thank you. And the military has a separate building code that is more stringent than local building codes. Is that correct?

Secretary MCMAHON. The standards that we are utilizing in most cases represent either national or State standards, in some cases, lag a little bit on State, but you would have in some cases actually exceed what those States and national standards are.

Mr. LAMBORN. Okay, thank you. Shifting gears, Mr. Niemeyer, I want to drill down on nuclear energy. The Navy has a long and storied history of small nuclear reactors on vessels, starting 65 years ago, the USS *Nautilus* was launched. So what can you tell us about micro reactors, about their safety and their effectiveness?

Mr. NIEMEYER. So we are working with other services and OSD to partner up with the Department of Energy on a couple of initiatives. We believe that there is a future for micro nuclear technology within the services. And there is a concern within the Navy about staying in what I would call the white world, as far as the technology. But we do believe that there are vendors out there, there are technologies out there, that ultimately could be used on a military installation to island that installation off of commercial power, particularly where we have critical assets, and run it on a very micro reactor, about 5 to 10 meg [megawatt] of electricity, plus another 10 meg of thermal, and continue to run that critical asset without any concern about having the commercial rig go down. So we believe there is a near-term and mid-term goals to get to that, and we continue to work with OSD. Bob's been putting a lot of effort into it and his staff to try to get those vendors to us, talk to us, and eventually get the technology incorporated.

Mr. LAMBORN. And we don't have Yucca Mountain figured out yet. So, with some of the nuclear waste that is in storage, is it possible that some of these new designs can actually use what currently is stored uselessly?

Mr. NIEMEYER. With some adjustments, I think that is one of the things we are most concerned about, is, what is the fuel source going to be? There is an opportunity to deplete uranium. We are asking the vendors that very question: Where would you get it from? What would we need to do to make it useful? Those are the things that we are working with not just the vendors but with the NRC [Nuclear Regulatory Commission] in trying to come up with a plan moving forward.

Mr. LAMBORN. Okay, thank you.

And, Mr. McMahon, I will finish with you. What are we doing with not just natural disasters but attacks on our physical infrastructure? We have talked about cyberattacks, but kinetic attacks or cyberattacks going against the electrical grid; EMP is a possibility that is out there. What are some things we are doing to protect the physical infrastructure?

Secretary MCMAHON. When you talk about physical, one of the things we have not yet mentioned is the UAS threat that we face at all of our installations and how is it that we can create the counter-UAS capability. Secretary Lord has taken that on for the Department, with regards to small counter-UAS activity. We have—the Joint Staff is working larger issues, but that is, how do I protect my installation? With regards to EMP, obviously, earlier this year there was an executive order that provided guidance as to move forward with that. Clearly not every facility needs to be EMP hardened. It is understanding what those are and what are the specific actions that we can take to make that happen, to ensure that that is there for either those installations or those portions of installation where that is critical.

Mr. LAMBORN. Thank you. I yield back the balance of my time.

Mr. LANGEVIN. Thank you, Mr. Lamborn.

Mr. Kim is now recognized for 5 minutes.

Mr. KIM. Thank you, Mr. Chairman. I wanted to just hone in on the "black-start" exercises. I have been very intrigued by this.

And, Mr. McMahon and Mr. Beehler, I just wanted to hear from you, what are the top lessons that we have learned so far from doing these black-start exercises? Mr. McMahon, we will start with you.

Secretary MCMAHON. Congressman, thank you for the question. We are tremendously proud of the effort. As we talk about building resilience, it is understanding, you know, we can do all the tabletop exercises in the world, but when you actually pull the plug, the question is, what actually goes on? And so the investment—and they run somewhere between $250,000, $500,000 per exercise. We have had a total of four thus far. I will let Alex talk a little bit about some of those specifics. We still have two additional that we will do, but the reality is, and perhaps the most important lesson that I have seen is a lack of appreciation and understanding by our senior leaders at the installation level, all the way up to my level, of what we thought was going to happen versus what actually occurred. And then being able to apply those lessons learned down the road as we move forward. Lots of tactical issues, but at the strategic level, I think that is the most important.

Mr. KIM. Go ahead, Mr. Beehler.

Secretary BEEHLER. Sort of amplifying what Mr. McMahon just said, it is the basic verification of backup energy, and also water, whether we really have what we think we have. And if we don't have it, what do we need to do to get it? And there is nothing like doing for verification. And at least on behalf of the Army, we think that, so far, they have been very effective. We have done, as Mr. McMahon said, we have done three through the means of OSD, but we have done others on our own, and we will continue to do more on our own because we believe it has been very effective to show exactly what works, what doesn't work, what needs to be improved and enhanced.

Mr. KIM. Well, I appreciate that. It certainly seems like an operation that really hits where the rubber hits the road and just tries to put this all into reality of what is going to happen. So I am certainly very supportive of the program and glad that it is continuing. In that similar vein, so, in my district, a district with Joint Base Maguire-Dix-Lakehurst, we got crushed by Superstorm Sandy, and that was something that we saw full force there. That base was able to have—the resiliency of that base being able to get up and running 24 hours later was critical not just for the base but for the surrounding community. As you know, that base really served the purpose for being the FEMA [Federal Emergency Management Agency] center for that area. So I guess my question to you, kind of building out from there, when we are talking not just resiliency of the bases but potentially for natural disasters, supporting the community around it, what exercise—are you doing tabletop exercises or real-world exercises planned with FEMA or other organizations? I am just kind of curious, you know, what we have been able to learn from Superstorm Sandy and other places where our military installations end up playing a critical role in the revival of these communities after these disasters. Maybe Mr. Henderson, some of your thoughts, and Mr. Beehler.

Secretary HENDERSON. Yeah, thank you. So, for the defense support to civilian authorities, the Air Force plays a large role in that usually with air transport, offering up logistics hubs and bases and stuff. So we participate with the Department of Defense in support of the FEMA exercises that go on. So I know that is our participation and the exercises that we do in conjunction with FEMA.

Secretary BEEHLER. Sir, a variety of things. One is that we at Fort Bragg participated in a project that I believe was initiated by OSD, but it also included Department of Energy, Department of Homeland Security, and the Federal Regulatory Commission in the development of a defense-critical, electric infrastructure pilot program, to evaluate the resilience of off-post electric infrastructure, you know, support. But more broadspread, each installation does, on an annual basis, an emergency response exercise that by its very nature closely engages the surrounding communities at all appropriate levels. The other thing that we have done on an ad hoc, utility-to-utility connection, is discussions on how appropriately located Army bases—this is particularly relevant to the southeastern area—can help as temporary—I don't know whether staging grounds is perhaps the best term, but really a place where utilities and emergency crews that are going to a scene that has faced hurricanes or severe weather events, and actually use, for whatever period of time, Army base facilities to help them position in the case of a major climatic event.

Mr. KIM. Well, I appreciate that.

Chairman, I yield back.

Mr. LANGEVIN. Thank the gentleman.

Mr. Scott is now recognized for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman.

General McMahon, I hate to see you retire. Thirty-four years in uniform, the best at Robins Air Force Base, I am sure. And for those of you who don't know, he is an exceptionally good production manager. He turned Robins Air Force Base, its efficiency around, and did an extremely good job there, so I want to thank you for that and your work there. And the average IQ of Alabama is about to go way up. I do trust you won't pull for their football teams, though.

I have a couple of questions. You mentioned drones or the UASes. Do the FAA [Federal Aviation Administration] rules that they have, that protect drones, apply to somebody who would perhaps fly a drone over one of our military bases?

Secretary MCMAHON. Congressman, I would rather get into those specifics outside of this environment, if I could push that back to you. I could take that for the record and come back to you.

Mr. SCOTT. That is fine. I just want to make sure that you have whatever authorizations you need and that we don't have any conflict between Federal agencies as sometimes happens.

Secretary MCMAHON. Yes, sir.

Mr. SCOTT. I want to make sure that we have the ability to protect you from that.

Another question, we have the Marine Corps logistics base in Albany, Georgia, the first net zero base in the country. Do we have any other bases that have achieved net zero with regard to energy?

Mr. NIEMEYER. I will take that question. So Albany is actually a shining star within the Department of the Navy as an installation that has truly achieved the energy resilience that we are looking for where, if the grid goes down, we can still conduct the critical missions there at Albany. I look to other Marine Corps installations, also the Marine Corps does seem to be leading the way around the Nation at Yuma in Arizona, at Miramar in California, an amazing effort there combining a series of initiatives over the last 10 years. It truly creates the resiliency we are looking for with that installation, using a variety of fuel sources. I want to make this clear. Within the Department of the Navy, we look at all fuel sources as an opportunity to provide us the resiliency. Miramar is using all those to create a pretty significant capability that, if the lights go out, we could conduct those critical missions in Miramar to launch our aircraft.

Mr. SCOTT. So we have multiple fuel sources but the way—if I am not mistaken, the way the Marine Corps logistics base in Albany, Georgia, achieved that was through a public-private partnership. And are we utilizing the public-private partnerships in other bases as well?

Mr. NIEMEYER. I am sorry, sir. Yes, we are. We look at a whole host of authorities that are available to us thanks to Congress: energy savings performance contracts, service contracts, power purchase agreements. I think my sister services share the desire to want to use all the authorities that are available to us to look at, what is the best comprehensive energy solution for a particular installation? And that takes into account a full range of fuel sources as well as what the community and the private sector can partner up with us on delivering those efficiencies and resiliency.

Mr. SCOTT. My concern is just making sure that you have the flexibility to achieve what needs to be achieved in the most efficient manner possible and that we are not showing preferential treatment to certain types of fuel sources.

Secretary MCMAHON. What I would offer to that, Congressman, is that we are agnostic, especially when we start talking about renewable energy. As you know, with all the installations in the State of Georgia, Georgia Power has come forward and has put solar on each of those to help get us where we need to be. They have helped funded it. And the point of that is, there are opportunities for all of our installations to partner, both in public-private opportunities, but also in the opportunity to be able to create relationships as we look at relationships between the public and private sector where the private sector can come in and help our installations get to where we need to be at little or no cost to the Department.

Mr. SCOTT. I know we talk about energy a lot. Mr. Beehler, you mentioned water. I was glad to hear you mention water as well. I hope that is something that we will focus on going forward. I think we spend an awful lot of time talking about the air, and I don't think we have spent enough time talking about water and making sure that we have access to clean water at our bases. And that when water leaves our bases, that it is as clean as it can possibly be before we reintroduce it to the environment.

Secretary BEEHLER. Absolutely agree. Extremely important and particularly given—and from the standpoint of the Army, the number of Army bases that are in potentially drought area or just an area that receives very little precipitation.

Mr. SCOTT. Gentlemen, thank you for your service.

Mr. LANGEVIN. Thank you, Mr. Scott. Ms. Houlahan is recognized for 5 minutes.

Ms. HOULAHAN. Thank you, Mr. Chair, and thank you so much, sir, for your service. I hope you enjoy your next chapter as well. I come from Pennsylvania, but I did my field training at Tyndall Air Force Base, and so that is a personal special place in my heart. And it struck me during the testimony—and this is largely me pontificating and less a question—$4 billion to restore that base to operation; $4 billion every time something like Tyndall happens. It seems as though we would be well served if we could find $4 billion to try and prevent these kinds of things from happening, from not necessarily a resilience standpoint but actually addressing the root cause of it, which is the climate that is changing around us. And so that is more of a pontification than anything.

My questions are springboarding off Mr. Scott's questions in some ways. My first question has to do with public-private partnerships to the degree that you guys can answer the question with specificity on cyber. He asked questions about energy sources. Do you feel as though you are empowered to be able to pursue public-private partnerships with people in the cyberspace? If not, why not? And if so, can you give me some examples of that and I would welcome any one of you to answer that question.

Mr. NIEMEYER. So we are updating our processes for our full range of interactions with our private partners. I will pick one specifically, energy savings performance contracts [ESPCs]. So, for years, these performance contracts have been used predominantly to find savings in how we install new technology. We are now saying: Okay, in addition to whatever we do with the ESPC, we are going to make ensured it has got an energy resiliency component, that we are making our control systems, that we are making our energy systems stronger as we are implementing these agreements. The private sector is very responsive to that. And I think they are doing an outstanding job of taking what we give as them as a requirement and then coming back with pretty innovative solutions on how we can use these partnerships to enhance not just our mitigation but our understanding of how best to mitigate. So that is just one example. I could go around the Department of the Navy where we work on the ESPCs. We just recently cut the largest one for the naval base we have at Guantanamo Bay and the largest one in the Federal Government, which has significant resiliency measures and steps within that deal. So we are looking across all our energy projects. In the past—I will be honest with you—a lot of our energy projects, particularly for renewables, has not had a resiliency piece to that. Our projects face the grid. They don't allow us to have mission assurance when the grid goes down. That is a problem. So we are looking at our full range of energy portfolio, to what degree those projects can be used to power critical missions if the grid goes down.

Ms. HOULAHAN. Thank you. Any other responses from you all, gentlemen?

Secretary MCMAHON. What I would offer across the entire spectrum as we talk about our ESPCs, we have the opportunity to upgrade, and when we think about that, that is replacing an old boiler with a new kit capacity or an old HVAC system with a new HVAC system. It is the controls, as Lucian alluded to, as part of that as we begin to think differently about what that opportunity is and as we put those contracts in place, being able to leverage not only the capacity and the newness of the new systems but, more importantly, the control systems that go with that, and leveraging as part of the project. And that is part of the new thinking I think we are beginning to see across the board.

Ms. HOULAHAN. Thank you. And with my remaining 1 minute and 30 seconds, I typically ask questions about whether or not you feel as though your workforce is prepared and has the right skill set. I really was impressed by your backgrounds, and clearly you have the right skill set to be sitting in your seats. But do you feel as though you have the right chain of people coming up through the ranks to have these kinds of really critical skills, whether they be cyber, whether they be water expertise, whether they be energy expertise?

Mr. NIEMEYER. I can go ahead and get started with that. First of all, the Department of Navy team is both on the secretariat, and I have actually represented two outstanding leaders from each service—General Chuck Chiarotti and Admiral Ricky Williamson—together we form a team, collective team, that looks at the resiliency challenges across the board. We probably could do better in educating our energy managers, to be more proactive at installation level. We are working collectively across the Navy and the Marine Corps to be able to do that. So those base-level managers are bringing up those ideas to us so we can actually incorporate. So we have still got a little work to do on the education front.

Secretary HENDERSON. For the Air Force, we recently hired a professor to develop a curriculum to help with the education and training of our engineers, our civil engineers, on this industrial controls and the cybersecurity of industrial controls, which is kind of our piece of that. So we are making efforts to take the workforce we have and kind of update their skill set so that we better understand how to install and operate these systems. Additionally, with regard to personnel and having the right personnel, the direct hire authorities that have come through some of these highly specialized, low-density career fields has been very helpful for us in the Air Force.

Ms. HOULAHAN. Thank you, and I am out of time. I yield back. Thank you.

Mr. LANGEVIN. Thank you, Ms. Houlahan.

Mr. Bacon is now recognized for 5 minutes.

Mr. BACON. Thank you, Mr. Chairman.

I appreciate all four of you being here. My first question is directed more to Mr. McMahon and Mr. Beehler, but please jump in if you can add in. I want to talk about the levee system and the permit process that we have to go through. And I have a specific example, but it is not just this example. I hear about it all over. So what we had in 2011, we had the worst flood in about 50 years in eastern Nebraska. I was a commander at Offutt Air Force Base. We worked for months to save the base. Hundreds of thousands of sandbags. FEMA came in afterwards and said: Hey, you need to raise the levees 2 to 3 feet. This was in 2012. And so then our NRD [Natural Resources District] with the State came forward with a proposal that cost $35 million and wanted to get it done, but it took 5 years to get a permit—5 years. And here is the deal, 5 years to get a permit to do $35 million worth of work. We got it all approved finally. In February of this year, we had the worst flood in Nebraska's history. It is going to be a billion dollars in damage. Now, if it was just a one-off incident, I got it. But I hear it from all over the place, all of our mayors, 5 to 7 years is the norm to get a permit. It is inexcusable. It is intolerable. It is bad for the taxpayer. It was bad for our national security. So what can we do to fix this?

So it fell on the Air Force, but I don't want you to—I think it was—it is not just one group, though. It is a cumulative problem. But go ahead.

Secretary HENDERSON. So, first of all, you and I have discussed that specific permit in my previous position. So I am not going to speak on behalf of the Corps of Engineers here, but you and I have a lot of carnal knowledge on that specific situation. I will share your frustration with the permitting process writ large, and whether it is FAA permits, NEPA [National Environmental Policy Act] work that we have to do, even those of us who are in the Corps of Engineers, used to be in the Corps of Engineers, the permits that are involved in there can be very slow, very bureaucratic, and they take a long time. And I would say a lot of that, just from my experience, a lot of that is linked back to, in order to issue those permits in a lot of cases, the NEPA work has to be done. And the NEPA work ends up being the long pole in the tent a lot of times. Specific with the Offutt levees, which have a huge impact on the Air Force base, but the Air Force does not have an equity in that levee. It is owned by the NRD. It is permitted by the Corps in combination with FEMA obviously. So I say that to say, as we have extreme interest in making sure the levee gets upgraded, it makes our installation there more resilient. In that particular case, as you know, in order to get the permits from the Corps, in this case specifically, a 408 permit, the NRD had to run the hydraulics to make sure that any work they were doing on the levees on the Nebraska side of the river weren't going to impact the main river levees on the Iowa side of the river, and that—and then the NEPA work associated with that, and that took a lot of time. And it was a lot of engineering technical work. It wasn't necessarily sitting in anybody's inbox. It was work that had to be done and a lot of back and forth as you know. And so—and that part of the permit process is very frustrating, but it takes a lot of time to get it right. And I would say it is important to get it right the first time. You wouldn't want to do something on one side of a river that has detrimental effects to the public on the other side of the river. And in that particular case on that permit, that took some extra time.

Mr. BACON. I would think, if it is just a one-off, I got it. But I hear about this from—I mean, we have 10 mayors in our district, and I hear over and over again 5 to 7 years to get a permit. And I just think that we can put our brains together here and figure out how to do it, and I would like to work on how we streamline this process because it is good for the taxpayer, and it is unacceptable. We built the Pentagon in 1 year. We got to figure this out.

Secretary HENDERSON. Sir, I got to say, from that perspective, we share your frustration because all of us up here are trying to deliver MILCON projects——

Mr. BACON. Right.

Secretary HENDERSON [continuing]. Projects, and there is usually a NEPA permitting component that we have to comply with——

Mr. BACON. Yeah.

Secretary HENDERSON [continuing]. And it takes a long time. And it is frustrating. I think there is a lot of opportunity there to expedite those.

Mr. BACON. I have one follow-on question if I may because I have only got one more—45 seconds. One of the things I am also concerned about is Russian gas fueling our bases in Europe. It is not a one-off there either. A lot of our bases are doing it. And the new hospital being built at Ramstein is designed to have Russian gas, and we are there because of Russia, and they can just turn it off. And it is a readiness issue. So what are we doing to wean ourselves off that, and what are we specifically doing with the hospital to make sure that we are not dependent on Russian gas?

Secretary MCMAHON. Congressman, two comments on that. First, as you know, we don't dictate what nations, where they source their fuel from, and given—number one. Number two, though, is this entire idea of installation resilience and being able to go off grid gives us the flexibility that if what you just suggested were to occur, we have the ability to respond to that and be able to continue the operations in a way that make sense and allow us to be able to achieve the mission that we have been given.

Mr. BACON. So you can assure us we have that at the new hospital?

Secretary MCMAHON. I am not going to assure you of that, sir, but I am going to assure you that we are working aggressively not only for there, at Ramstein, but every other installation that we have, to be able to achieve that.

Mr. BACON. Okay. Thank you.

I am out of time. I yield back. Thank you.

Mr. LANGEVIN. Thank you, Mr. Bacon.

Ms. Escobar is recognized for 5 minutes.

Ms. ESCOBAR. Thank you, Chairman. I am so grateful to you and the ranking member for this important hearing.

And many thanks to our witnesses today. I reviewed the list of the top 10 Army facilities that are vulnerable to climate change. All of those facilities are in the West or the Southwest, and the threat is listed as drought. And so I am wondering if you can expand on how you all intend to attack that, what the plan is, and what the theory is around assisting—ensure the sustainability of the West and Southwestern facilities vulnerable to drought?

Secretary BEEHLER. Sorry. Ma'am, this is one of the things that will be accomplished through our installations energy and water programs plans that are being done at all of the major Army installations, including all of the ones in the Southwest. They are to address, in effect, your question, which is, how do we ensure at a given installation, adequate water supply, access to water. It also gets incorporated when an installation upgrades and reviews its broader installation management plan, which is done every 5 years for each installation.

As I mentioned earlier, the first tranche of these energy and water plans are due to be completed at the end of this calendar year, which, I believe, includes some of the installations in the Southwest. So we will then have—those installations will have a way forward as to what they need to do to make sure they have good access to water.

Ms. ESCOBAR. One of the installations on that top 10 list is Fort Bliss——

Secretary BEEHLER. Yes.

Ms. ESCOBAR [continuing]. Which is in my district, which obviously has a very sophisticated desal [desalination] plant in the district that has really been focused on ensuring water, not just for the military installation, but for the community. Was that taken into consideration when Fort Bliss was placed on the top 10 list?

Secretary BEEHLER. Well, the top 10 list was looking at threats.

Ms. ESCOBAR. Okay.

Secretary BEEHLER. And it is great that there is this desalination plant, but that doesn't remove the effect of the threat.

Ms. ESCOBAR. Gotcha. Okay. But my followup question to that is, you know, obviously we do want to consider the threats, but also the opportunities.

Secretary BEEHLER. Yes.

Ms. ESCOBAR. And Fort Bliss has, for some time, was being very thoughtful about the opportunities around solar. And it seems to me that all of our Western and Southwestern installations have that same opportunity. And I am wondering how the plan seizes on the opportunity for solar as a major opportunity for renewable and sustainable energy.

Secretary BEEHLER. Well, certainly, as I think we mentioned before, the goal of these plans is for each installation to have the necessary access to energy to carry out critical missions however best means that make sense given the specific installations. So I think, generally, solar is always part of the consideration as long as it can be effectively both cost effective and logistically applied and included. Obviously, I don't know about the specific case of the Fort Bliss plan that is obviously under development, but that is something that I am happy to look into and get back to you with what their thinking is, as it develops. And happy to give a brief.

Ms. ESCOBAR. I appreciate that. I really do believe, especially hearing in this hearing alone, listening to concerns about the grid, and our vulnerabilities with regard to the grid, that we should be showing far more leadership in saying, you know, we are going to draft a plan that leads the way, leads the country in sustainability, and that takes some of those critical threats away because we are leading on that front. So that would be my hope.

Secretary BEEHLER. Thank you.

Ms. ESCOBAR. Thank you.

Mr. LANGEVIN. Thank you, Ms. Escobar.

Mr. Waltz is now recognized for 5 minutes.

Mr. WALTZ. Thank you, Mr. Chairman, and thank you, ranking members. This is, I think, a fantastic hearing and topic. You know, I have a lot—a little bit of skin in this game on the tactical side. I can't tell you how many soldiers are no longer with us because of their supply lines being attacked carting fuel out to remote outposts that, frankly, could have had some panels and a turbine and been much more self-sufficient. Then you magnify that from the tactical to the global and strategic in terms of our supply lines that our fantastic Navy seeks to supply. So could you talk to me for a moment about what we are doing on the tactical sustainability side, particularly for our special operations forces who, as you know, are in anywhere from 60 to 70 countries as we speak today, and allowing them to have portable and tactical sustainment systems?

Mr. NIEMEYER. This is a tough issue, because everything that we have looked at in the past, I know both the Marine Corps and special operations forces and Army forces in the past have looked at what tactical generation can do for us. And any form of tactical generation creates pros and cons. I mean, there is a lot of folks who are concerned that by setting up those solar panels in a remote area, you actually—they are easily spotted and they are easily taken out. So the goal here—and this goes back to the heart of the National Defense Strategy—is, how do you provide agile logistics in a contested environment? And I got to tell you, our adversaries know that that is probably our weak spot. How do we power the next generation of equipment? It is not what we just have today, Congressman. It is what we are looking at—you know, autonomous vehicles, robotics, direct energy programs. What we are going to need in the next 10 years is more energy on the battlefield. That is something that in our research and development we are taking a hard look at what batteries we can use, what can be done for next generations of tactical energy sources that doesn't rely on fuel supplies. It is something we are working very hard on across the Department of Defense.

Mr. WALTZ. Thank you. And please, Mr. McMahon.

Secretary MCMAHON. Congressman, what I would add to that, again at the tactical level, but a very strategic concept is this idea—Mr. Niemeyer talked a little bit about small, modular reactors. There is also an effort within our research and engineering concepts, under Dr. Griffin, to be able to look at the micro capability. Is there something we can actually put in the back of a ton-and-a-half truck that could take forward that would give us, for a forward-operating base as an example, the ability to operate with a micro nuclear reactor. That is——

Mr. WALTZ. What do you need from this committee to move those concepts forward?

Secretary MCMAHON. Moving forward today, quite frankly, many of the challenges that we face are working through some of the regulatory issues. It is a science issue on the micro that we are still trying to work through. But at least at the small nuclear reactor capability, I think we are moving forward. It is just working through the regulatory process that is necessary to get to where we need to be.

Mr. WALTZ. Okay. Thank you for that. And just shifting back to the basing issues, resiliency is something Florida takes very seriously. Obviously, we have to deal with it every year, with storms, with flooding. There are areas of Florida now that are flooding and on a sunny day. The sea level is rising and we have to deal with it. We need to move beyond that debate. In fact, the Governor of Florida, my predecessor in this seat, just named a chief resiliency officer to pull together our statewide strategy. We have a Florida defense task force that is very focused on these issues.

On the Navy side, Secretary Niemeyer, the engineering command issued what I think is a detailed and a comprehensive handbook for installation commanders, "Climate Change, Installation Adaption and Resilience." What step are you taking to ensure installation commanders are actually implementing the recommendations in this handbook in their installation master plans and then also coordinating—because this is a broader issue. This is wetlands. This is offshore. This is seawalls. It is a huge issue that I am trying to deal with the Corps of Engineers as well for properties. How are you integrating locally, and how are you ensuring each installation commander implements those plans?

Mr. NIEMEYER. I mean, that is something we are working on today with the southeast region. The goal here is to allow that installation commander the range of resources and to include that pamphlet and that guidance in addition to other guidance and look at the most critical assets on that installation and what really delivers the projection of that power for the naval base, and use the guidance we have given them to direct resources towards making sure that that particular asset has mission assurance from a full range of threats. So it is really——

Mr. WALTZ. Are you confident they are doing it?

Mr. NIEMEYER. Yes, I am. In their capitalization and installation master plans.

Mr. WALTZ. Great. Thank you so much.

I yield my time.

Mr. LANGEVIN. Thank you, Mr. Waltz.

Ms. Haaland is now recognized for 5 minutes.

Ms. HAALAND. Thank you, Chairman.

And thank you to our witnesses for coming here today to discuss this important issue important to national security. I am glad to see that our national security infrastructure is investing in innovations in resiliency and renewable energy. In my own district, Sandia National Laboratories and Emera Technologies are working through a Cooperative Research and Development Agreement, a CRADA, on microgrids that locally manage energy storage and resources such as solar, wind, and thermal systems. Chairman Adam Smith and I recently visited the pilot project at Kirtland Air Force Base where they will be testing innovations in distributed generation to make units more resilient to weather, physical, and cyber attacks. If one unit goes out, the others could operate independently. If successful, this system could provide highly reliable and renewable power supply. And I will just add that, in New Mexico, we have over 300 days of sun per year, so it makes sense to try it there. This is an excellent example of how our National Labs support innovation and resiliency and renewable energy research development. So Assistant Secretary McMahon, can you describe the DOD's plans to increase research development, test, and evaluation in energy storage, microgrid, and energy resiliency? And does the DOD intend to further expand the energy resilience and conservation investment program?

Secretary MCMAHON. First of all, Congresswoman, we would like to say thank you to the Congress for the support that we have had. A tremendous amount of our innovation, imagination, research, and development comes from the funding that you all have provided us. One of the conversations, as I saw Congresswoman Slotkin come in, talk about PFAS [per- and polyfluoroalkyl substances], PFOA [perfluorooctanoic acid], a lot of our effort in that area as well is coming out of this R&D [research and development]. So the question becomes, do we have the right funding? The answer is we do. We have continued to leverage that for a variety of different innovative areas. You have already covered a couple of those. But what we are doing today gets us to where we need to be, and if additional funding is made available—though I think we have sufficient funding today—we will continue to apply it in innovative ways.

Ms. HAALAND. Excellent. And, again, Assistant Secretary McMahon, can you share your thoughts on how best we can expand the role of our National Labs in public-private partnerships like CRADAs in support of DOD's resiliency efforts?

Secretary MCMAHON. Congresswoman, we talked earlier about the level of experience and knowledge that we have. Clearly, our labs are national treasures, and we continue to leverage those to the best of our ability in terms of research and development. At the same time, many of our universities across the Nation are equally as successful. And so it is a matter of simply ensuring that we are leveraging all of our sources, both our labs and our universities, for the innovative ideas that we need. But, clearly, I think that part of what has made us as successful as we have been are our labs and the innovation that we see coming out of them.

Ms. HAALAND. Thank you so much.

Assistant Secretary Henderson, you mentioned that the Air Force is taking the necessary steps to build resilient installations that are ready to withstand and recover from manmade and natural events. How do microgrids and distributed generation factor into the Air Force's approach to resiliency?

Secretary HENDERSON. Yes, Congresswoman, absolutely. And we do that through—we are doing installation energy and water development plans on each of our installations in conjunction with the master plans that we are doing, and then we are funding any vulnerabilities and gaps in that regard in a priority basis through an investment strategy that we have across the enterprise.

Ms. HAALAND. Excellent. Thank you. One more minute. And back to you, Assistant Secretary McMahon. The Annual Energy Management and Resilience Report for Fiscal Year 2018 showed that the DOD is falling short of its goal to consume 7.5 percent of its energy from renewable sources. What challenges is the DOD facing in attaining this goal, and what does the DOD need to achieve the goal?

Secretary MCMAHON. Congresswoman, what I would offer to you is that we continue to focus—we are agnostic on the type of renewable that we are talking about. But I would share with you an evolution over the last couple of years, as we have looked at the National Defense Strategy and we have begun to consider what occurs in great power competition, and to focus less on renewables as an end in itself, rather becoming a means to an end, and the means to an end is creating that resilience. So we are applying renewables where it makes logical sense to give us that kind of resilience that we need, rather than simply generating renewables for the sake of doing renewables.

Ms. HAALAND. Thank you so much.

I yield, Chairman.

Mr. LANGEVIN. Okay. Thank you, Ms. Haaland. And Mr. Banks is now recognized for 5 minutes.

Mr. BANKS. Thank you, Mr. Chairman. Recently we had Mr. Wilson, the DASD [Deputy Assistant Secretary of Defense] for Cyber Policy, and representatives throughout the interagency testify before this subcommittee regarding internet security. During that hearing, I highlighted the fact that, in DOD's 2019 Digital Modernization Strategy, it states that the DOD utilizes 10,000 operational IT systems. The amount of access points provides enormous vulnerabilities as the DOD moves forward and toward an increasingly internet integrated warfighting posture.

Mr. McMahon, what role do you play in the oversight of physical internet and network security?

Secretary MCMAHON. Congressman, thank you for the question. What I would tell you, I am one of those that lies awake at night as we look forward to the future and see 5G come forward, the threat that it provides to our already capable system, and the fact that more and more systems will be utilizing 5G in the future, where those systems come from, and the infrastructure challenges that we face in terms of espionage, not knowing the source of that 5G capability, and being able to ensure that it is secure. More and more data will be utilized. And so the question becomes, how do we ensure that the infrastructure, in conjunction with the CIO, in conjunction with our new——

Mr. BANKS. Help me out real quick and tell me the specific role that you play organizationally.

Secretary MCMAHON. From my perspective, what I worry about most of all is with installation industrial control systems as it plays directly and then tangentially as we put infrastructure capability in place, our comm [communications] CIO looks at the specifics of that security.

Mr. BANKS. Okay. The witnesses then were not able to tell me that the DOD has a complete inventory of all the items that can access the network in that particular hearing. But in your testimony, you said that your office is developing the framework for identifying the required resources for inventorying, assessing, mitigating, and sustaining facility-related control systems. So, to your knowledge, is there any source that can show internet-dependent resources on military installations?

Secretary MCMAHON. Holistically, I am not aware of that, Congressman.

Mr. BANKS. Okay. DOD CIO Dana Deasy recently said in an interview, quote, The Department will need to do some work to help industry better understand the things that it needs to meet the new challenges in cyber, end quote. Mr. McMahon, how does DOD improve communications with industry in setting clear cyberspace—I am sorry—cybersecurity expectations?

Secretary MCMAHON. As I mentioned earlier, Congressman, the Under Secretary of Defense for Acquisition and Sustainment has put in place a cyber czar, Ms. Katie Arrington, whose responsibility is to look across the acquisition community as well as the sustainment community, looking at all elements of this, to include in conjunction with the CIO, looking at how we are doing business with the acquisition systems, through the supply chain, to ensure that there is security there, and becomes a first step in getting us to where we need to be, in creating, for example, a CMMI-like [Capability Maturity Model Integration] system and capability that all of our suppliers and contractors would have to be able to achieve to ensure a level of security we do not have today.

Mr. BANKS. What would you say that the—what are the—what role do cyber training ranges, like Muscatatuck Urban Training Center in Indiana, play for advancing cyber readiness on the battlefield and on U.S. bases?

Secretary MCMAHON. Clearly, Congressman, all of our cyber ranges provide an opportunity to further educate and train our cyber warriors and make awareness out there. Though I don't think we are at the point that we are fully utilizing them because this is a learning business, if you will, to understand where we are. There are those that are probably much more expert in describing to you how best to utilize those cyber ranges, acknowledging that we see them as critical to the way forward.

Mr. BANKS. Got it. One of the goals from the 2018 DOD Cyber Strategy is to increase cybersecurity accountability. Specifically, the strategy stated, reducing the Department's attacks—attacks surface requires an increase in cybersecurity awareness and accountability across the Department. We will hold DOD personnel and our private sector partners accountable for their cybersecurity practices and choices, end quote. Last question. What kinds of cybersecurity accountability changes have been made since the release of that strategy?

Secretary MCMAHON. What I would tell you is, we are in the midst right now, as I just described, a CMMI-like capability where our OEMs, original equipment manufacturers, our sources of supply, have to be able to put in place the capabilities to attest that they have control over their supply chains, not only at the first tier, second tier, third tier, but down as far as they go, something that I think is a new experience for all of us, as we get to that level of understanding, to be able to understand the lineage of all the parts that we have within our weapon systems as well as within our infrastructure.

Mr. BANKS. Thank you very much.

With that, my time has expired.

Mr. LANGEVIN. Thank you, Mr. Banks.

Ms. Torres Small is recognized for 5 minutes.

Ms. TORRES SMALL. Thank you all for your work, creating resiliency for our military installations.

I have the honor of representing New Mexico's Second Congressional District, which includes White Sands Missile Range. Geographically, it is the largest range in the United States, and it is located in the middle of the desert. It is fundamental to our testing mission, and it has some of the most cutting-edge technological design, research, and testing but it hasn't had a military construction investment for—since the 1970s.

And so a key example of the needs that we have is the information facility—the information systems facility, which was built in 1962. The facility serves as a gateway for all of our communications and data to the outside world and houses critical equipment, providing support for administrative commands and control and testing and evaluation users. The facility is relied upon to provide critical support for modern missile testing, ranging from the Standard Missile-2 and the Patriot Missile System 3 to next-generation weapons systems. But the facility is 57 years old.

So, Assistant Secretary Beehler, would you agree that in the era of big data and technology, a modern information facility is critical for transmitting the vast amounts of data generated during military testing?

Secretary BEEHLER. Yes, I agree.

Ms. TORRES SMALL. Thank you.

And can you please speak to how conducting operations in a 57-year-old facility could stunt the efforts for maximizing installation resiliency?

Secretary BEEHLER. I would be happy—oh, sorry. I am sorry about that.

I would be happy to take that for the record and provide greater detail and also come back with a briefing on that.

[The information referred to was not available at the time of printing.]

Ms. TORRES SMALL. Thank you very much. But, shortly, it generally does impact our cybersecurity.

Secretary BEEHLER. Yes.

Ms. TORRES SMALL. Thank you.

I want to pick up where my colleagues Congressman Scott and Congresswoman Escobar were talking about water because it is a deep need. And as you mentioned, Assistant Secretary Beehler, it is a challenge that many military installations are facing. In fact, I believe it is over half of our military installations that face either current or future drought vulnerability. I wanted to talk more about the work that is being done for the energy and water plans. You mentioned that all of the installations are putting those together now.

Do you know if they are assessing the resources that are available including the quality and quantity of water in nearby aquifers?

Secretary BEEHLER. It is certainly my understanding that they would take that into account because their thrust is access to quality water. So they obviously are going to have to look at the sources from which this water is coming for their use in installations.

Once again, the plans for the first tranche have not yet been completed. When they are, and particularly relevant to the geographical area in which you are interested, be happy to provide that further information, come in with a briefing.

Ms. TORRES SMALL. That is great. That is fantastic because it really is important as we assess what we have available that we are looking at all of the aquifers and what might be available, especially if we are able to do more desalination plants to clean up some of the brackish water as we have seen be so successful in Fort Bliss.

Secretary BEEHLER. Absolutely.

Ms. TORRES SMALL. Shifting to Mr. Niemeyer, I know that there is an energy savings performance contract, and it has been used for water conservation, specifically within the Navy. I would love if you could speak briefly on that and how it has been—if there are any efforts to scale that to other military installations.

Mr. NIEMEYER. Sure. So, yeah, we were able to successfully find savings that allowed us to do some water system upgrades. I do believe that there is a—we can get to water conservation and aquifer management. We could take regional approaches. I think we need to work collectively with our services to see how a series of bases could work regionally to do a common aquifer management plan. That is something that we have been working on for a couple of years. I think there are opportunities around the country.

And also, we need to, and the other services also, use the privatization of water systems as another way, probably for us the most significant way to conserve water over time and to have our partners that we do have privatized citizens who work with those regional water authorities.

So the goal here is to use the whole range of authorities. Yes, I am proud of the ESPC, but that is just one step we have on how we can get much more collaborative with industry and regions on addressing common aquifer management.

Ms. TORRES SMALL. Great. Thank you all.

I yield back the rest of my time.

Mr. LANGEVIN. Thank you, Ms. Torres Small.

Ms. Slotkin is now recognized for 5 minutes.

Ms. SLOTKIN. Great.

Thank you, gentlemen, for being here.

Assistant Secretary McMahon, thank you especially to you and your team for coming to my office and wearing your PFAS task force hat, coming in and briefing us. I sent you a followup letter on October 7th, but just since I have you on the record here, I was just home in my district, and I can't express enough to all of you how important the issue of PFAS around our military bases is to my constituents and the feeling like the Defense Department is dragging their feet on this issue.

I know, when we talked, you still had concerns, but for the record, are we still at loggerheads when it comes to the issue of transitioning off PFAS firefighting foam by 2025?

Secretary MCMAHON. Congresswoman, first, thanks for the opportunity to talk about PFAS, PFOA.

When I talk about the task force, I do it in conjunction with the three gentlemen sitting here. It is weekly. We spent an hour and half today talking about what it is that we do.

As I laid out, since you gave me this opportunity, we are concerned about three things. One, how do we mitigate what we are doing today? How do we ensure that we understand the health of the individuals that may have been affected by this? And then, finally, how do we clean up the messes that are out there today that we go through?

Again, this is a national issue. It is just not a DOD issue. You understand that clearly without any military installations in your district, yet it is a big issue. So, we have got to deal with this. This is a national issue.

With regards to your specific question, we continue to work aggressively to try to find an AFFF [aqueous film forming foam] version that is fluorine-free. On the I think it is the 14th of November in conjunction with my partners, we will hold a summit to go through all of the work that is being done to understand where we are, what the process, what work is being done today, and whether or not we can make that kind of date.

I don't want to commit to you today that I can because I don't know what—where we are, what the work that is being done with the research and development. If we aren't able to do it, it certainly is not due to a lack of effort though.

Ms. SLOTKIN. Can I just—I appreciate that. My understanding is that some of the militaries in Europe have done some good work researching alternatives, and would just urge a real push on this.

The other thing I just want to, if I could have all four of you on the record, since you are all kind of in this together, I know that what I had understood is that the military was no longer using PFAS foam during exercises, that, of course, if we had an emergency, we are reliant on what we have now, but there is no need in places like Camp Grayling in Michigan, Selfridge Air Force Base, in order to use those in exercises.

Can you just confirm for me? Because I have heard conflicting responses on this from rank-and-file folks who are saying that it is still being used. Can I get a yes or no from all four of you? Is PFAS firefighting foam being used in exercises by your respective branches and by the military?

Secretary MCMAHON. I will let the services answer, and then give you an OSD answer.

Secretary BEEHLER. Army, the answer is, no, they are not.

Secretary HENDERSON. For the Air Force, the policy is no. I heard the same things that you are, and we are following up to make sure that everybody hears that loud and clear.

Mr. NIEMEYER. For the Department of the Navy, land-based exercises, absolutely not.

Ms. SLOTKIN. Yes, and we know that on ships we have a special case. We want to make sure, if there is a fire on a ship, we have everything that we need.

Secretary MCMAHON. Categorically, our goal is to make sure that the only time it is used is in an actual emergency, and then it is treated as a spill and cleaned up appropriately, which ought to dramatically reduce any additional exposures until we find that replacement.

Ms. SLOTKIN. And I would just ask, now that we have you guys officially on record, that you do everything you can to try and make sure that we are adhering to that policy way down the chain.

Lastly, as I wrote to you, I have had a lot of firefighters, including Federal firefighters, come and visit me. And they were concerned that there is no representation that I know of on your PFAS task force of Federal firefighters. I thought that was a kind of an easy ask and a kind of a "no duh" that the folks who are using this foam most frequently be represented on the task force.

Can I get your thoughts on that?

Secretary MCMAHON. What I would offer is that our medical folks play an integral role. The firefighters work for the gentlemen sitting to my left, and so that representation is there. Clearly, our attempt is to be as transparent as possible. So, in our minds, up to this point, that representation was taking place through the individuals immediately to my left.

Mr. NIEMEYER. I would also add that, since the Navy is the lead for coming up with a MIL SPEC [military specification] that is going to be an alternative for AFFF, we are reaching out to the military firefighting community to see what is out there, not just what they know, but what they know and sharing with our Federal firefighters and also our private firefighters.

So I would suggest, yes, they probably—they do need a voice. They are represented. They do come through my representatives into the task force meetings weekly to present a concern.

For instance, we do have a concern about meeting that deadline by 2025. We have a lot of equipment we are going to need to replace. It is lot of money. We are talking hundreds of millions, maybe 15 to 20 years to get this done to truly get to the point the committee wants where we are not using AFFF even in residual levels. So those are the types of issues that, yes, our firefighters are clearly passing up to the task force and we are addressing.

Ms. SLOTKIN. I would just say some of the dissenting voices on how the Pentagon is doing have come from Federal firefighters. So the idea of just going that extra step and putting one on the task force, I understand you are hearing them. Just as a former Pentagon official, it probably isn't—the juice isn't worth the squeeze to leave them off, but thank you, gentlemen.

I think my time has expired. So thanks very much.

Mr. LANGEVIN. Thank you, Ms. Slotkin.

And since there so few of us, we are going to do a brief second round. So if you want to stick around, you have additional questions, you are welcome to ask additional questions.

Secretary Henderson, several years ago, the Air Force had requested considerable additional funds to address structural damage to facilities at Eielson Air Force Base resulting from melting permafrost. Last year, Congress directed a detailed assessment of the risks from melting permafrost installations in Alaska, Greenland, and Northern Europe.

Since many of those are Air Force installations, has the Air Force completed those assessments?

Secretary HENDERSON. So I think we are still working on them. What I would like to do is take that for the record, make sure I give you a detailed response of what the status of those assessment are and where we are at. I know we have done a lot of work in correcting the problems caused by melting permafrost, by shoreline erosion also in Alaska, and then the permafrost issues that we are seeing at Thule, Greenland.

In Eielson, for instance, we are having to modify the designs of some of our structures there to use deep pile designs so we can get down and have the support for those facilities against the bedrock. In Thule, Alaska, we are actually going the other way and putting piping systems in to keep the ground frozen underneath there so the ground remains stable.

Then, with the eroding shoreline in northern Alaska for our radar sites and stuff, we are trying to find better predictive models to incorporate what is a better characterization of the changing climate and a number of other factors that is affecting the shoreline erosion there so we can put together a mitigation strategy for that.

I will answer back on what the status of that assessment and that document is, though.

[The information referred to was not available at the time of printing.]

Mr. LANGEVIN. Fair enough. We will look forward to the followup assessment.

I will yield to Garamendi.

Mr. GARAMENDI. I have got you guys now.

First of all, as I said earlier, your papers taken together really cover the entire array of challenges and most of the solutions that are out there, and I am really quite serious about you reading each other's papers and circling those things that you're not doing, that you might very well be doing.

It has been mentioned by two of you, three of you, the Army Corp of Engineers Assessment Program. Could you send some detail on to the committee on what that is?

Secretary MCMAHON. Let me take that for record, Mr. Chairman, and provide that to you.

Mr. GARAMENDI. If you would, please.

[The information referred to was not available at the time of printing.]

Mr. GARAMENDI. Also, as we have discussed before, I think almost individually—well, not quite individually with all of you—the reconstruction plans for the bases that have been decimated—Tyndall, Lejeune, China Lake, Offutt—those plans are in process, as I understand. They are not yet complete. There is a significant pile of money that has been and will be appropriated ahead of the plans, that is, the completion of the plans.

I want to—I will say it very clearly. That money must be spent in a manner that maximizes the resiliency of that base, whichever it happens to be. The standards to be applied must be the strongest standards available in the world, not just in the States, earthquakes specifically and flood standards and so forth.

So we will see those detailed plans as they are completed, but I know the money is already out there in some of the cases and so be aware you don't want to have to come and explain why you didn't build to the maximum standard. Do you? No, you don't. No, you don't. So please keep that in mind as you go about your work on rebuilding.

I do have some specific concerns. Some of this has been shared with the—actually a fellow behind you. There he is. So please pay attention to that.

Also, Mr. Waltz raised a point that we are going to take up going into the future, and that is it is not just the facility. It is the equipment and particularly the transportation equipment that is used on the bases. Part of what is in the NDAA and will be even stronger in the future is energy conservation.

For the Navy, I want to know why you have only built one destroyer with a hybrid system, why you are not building multiple destroyers and other facilities.

You have got an answer for that already, Mr. Niemeyer?

Mr. NIEMEYER. No, I was going take that for the record.

[The information referred to was not available at the time of printing.]

Mr. GARAMENDI. Take it for the record.

I will tell you why. There was insufficient energy generated for both the hybrid system and the electronic warfare systems. And when I asked, “Well, how do you solve that,” the answer was, “Well, we won’t do hybrid.” I am going, “Why don’t you get a bigger generator?” And you will tell me why, Mr. Niemeyer, you are not getting a bigger generator for the ships.

Mr. NIEMEYER. I do know that I have spent a lot of time with my colleagues over in the acquisition world of the Navy trying to determine what is the ideal configuration on a ship. As you know, we are adding a lot of new weapons systems that are all energy draws. We are looking at potentially putting directed energy programs on our ships, huge energy draw. So we have to manage that on the ship.

Mr. GARAMENDI. Yep, that is true. And the biggest energy draw of all is to move the ship. Okay? So the answer was not satisfactory. Send that back.

We are going to miss you, Mr. McMahon. You have been very good to work with, and we really appreciate your work on issues. I am not so sure you are going to be around for our next family housing issue. You jumped on that. I think you jumped on the gentlemen at the table with you, and we will see how well everybody is doing. We are going to come back in December, and we will review the family housing and go at that again and look for progress along the way.

Secretary MCMAHON. Yes, sir.

Mr. GARAMENDI. One of the things that both Jim and I intend to do is, and that is we are not going to forget what we asked you to do last year, and so we will be following up as best we can, and I am sure you will, too.

I think, Jim, I could probably go on for hours here, but I am actually going to get an answer on that destroyer at 5 o’clock.

Thank you so very much, gentlemen. Thank you.

Jim.

Mr. LANGEVIN. Thank you, John.

So, Mr. McMahon, just to follow up on Mr. Kim’s question earlier, the concept of resilience in the context of the logistics, sustainment, and reconstitution, is critical to joint force operations. Has this concept been included in any of the Joint Staff globally integrated exercises?

Secretary MCMAHON. Mr. Chairman, thank you for the question.

As we talk about what do we include in the exercises, we have just completed an energy war game with the INDOPACOM [U.S. Indo-Pacific Command] staff focused specifically on fuel for the INDOPACOM theater. It was the first time we have done something along those lines to look at holistically what that impact is, where our shortfalls were not only in our planning but in the execution. So was it a baby step? The answer is yes. Did we learn how we need to expand that?

But the thought that energy is an integral part of our planning purposes and, more importantly, our tabletop exercises, we underscored that point. And we are going to apply that in the next series of exercises that we do with the Joint Staff.

Mr. LANGEVIN. I hope we will see that expand and broaden to look at other aspects of sustainment and reconstitution. I think that is critically important.

Secretary MCMAHON. We are tremendously proud of what we did there, Mr. Chairman. And although it was a baby step, the fact that we have got that as part of the conversation and applying it to the operational community, in particular the INDOPACOM theater and the challenges there, this was tremendously important for us.

Mr. LANGEVIN. Can you on one other thing—did you have something specific?

Mr. GARAMENDI. Go ahead. Finish now. I do have one more.

Mr. LANGEVIN. Can you please specify just on cyber-related responsibilities of individual installations by service or department, departmental level organizations and components? For example, the Air Force is creating mission defense teams built for cybersecurity of installations, teams that exist outside the Cyber Mission Force.

Secretary MCMAHON. What I will tell you is, Mr. Chairman, that I think we are in the early stages of understanding holistically to look at installations from a cyber perspective. I think there are multiple owners, whether it is the CIO, whether it is us, when we get into the specifics of industrial controls, whether we look at the supply chain, the elements of that from an acquisition process. I think, on a daily basis, we continue to learn, and I continue to underscore the fact that Secretary Lord has identified a cyber czar exactly for the purpose of providing greater clarity of how we move forward with this. I am not sure if that scratched your itch here, but part of this is, quite frankly, we are still getting our arms around the whole discussion. We can—we could put glossy words on it, but we are still trying to figure it out.

Mr. LANGEVIN. This is something else we are going to be following up on.

Anything else you wanted to add?

Mr. NIEMEYER. Mr. Chairman, one specific issue we haven't had a chance to talk much today, and that is the development of a national small-cell infrastructure, 5G technology. We are being very aggressive in providing information to the installation commanders in ultimately how do we both advocate for and receive applications from internet providers who want to install 5G infrastructure on our bases. It is going to be much more extensive than what we have for 4G, and we have some guidance making sure that equipment is secure; it is not necessarily from a foreign manufacturer, but allows us the resiliency we need for future data management.

Mr. LANGEVIN. That is a good segue into my final question. Do you have something to add, Secretary Henderson?

Secretary HENDERSON. I was just going to say with regard to the mission support team, from the Air Force perspective, that is one of a number of holistic initiatives we are taking to look at our missions to include, you know, threats for mission assurance, all the way down to the cyber ties, down to each device that is connected.

From our perspective, from an installations perspective, we are really focused on the installation control systems. And like Mr. Niemeyer mentioned what the Navy had done earlier, as part of that to protect the network from some of the installation control vulnerabilities, we have installed 56 base-level network enclaves to logically segment the control systems from the business network to mitigate those risks.

So, you know, that mission defense team is one of a number of initiatives the Air Force is doing. But that is kind of the one that falls in our installations portfolio, so to speak.

Mr. LANGEVIN. Well, we are going be following up on that, too, and see how, where that expands to and how it unfolds. I think it is important to consider those issues.

Last thing I had, then I am going to turn to Mr. Garamendi for a final question, China appears—and this is going back to the 5G—appears far ahead of us, the U.S., in its development and deployment of 5G. Reuters reported just yesterday that mobile operators in Europe are queueing up to buy Huawei gear for their next-generation 5G networks, despite U.S. concerns that Huawei equipment contains backdoors open to cyber spies, quote. That is end quote.

If local power and telecom companies in Europe employ Chinese 5G networks, how well would the U.S. military be equipped to protect its installations across Europe? And how resilient is our IT infrastructure?

Mr. NIEMEYER. We could spend about 4 hours on that particular answer. Let me try to give you an unclassified, basic view. So we are working on innovative technologies that would allow us to distribute our own 5G network separate from what we might have to rely on in a host nation.

Domestically we need to start working with States to ensure that the concerns that we have with security of 5G network is passed on to the State and community permitting process so that way we don't have States inadvertently installing or permitting or allowing a system to be installed that is going to create a resiliency or threat concern for the Department of Defense.

So it is combination of the base of the future, whether domestic or overseas, needing that secure 5G network. We are working on ways overseas to not have to rely on the host nation 5G network but installing one of our own that we can be much more secure.

Secretary MCMAHON. Mr. Chairman, what I would only add to that is I think all of us in the Department of Defense are gravely concerned about our international partners where there is a 5G system put in, what the vulnerabilities of that are, what the capability for espionage might be, and all the elements associated with that I think are front and center in our minds. I would defer to some of our experts to give you more detail probably in a classified setting, but from our perspective, from an installation perspective and the reliance, for example, on energy from a local industry provider in a foreign country, I think there is some concern about that.

Mr. LANGEVIN. I am glad we are not going into it without blinders on. We need to continue to follow this topic as well.

With that, I will yield to Mr. Garamendi for the last rounds of questions, and then we are going to conclude.

Mr. GARAMENDI. Mr. Chairman, we need to have a classified hearing not only with our committee but also with the Energy and Commerce Committee on this issue of 5G. Not enough time to go into it and probably not the right place to go into it, but we are headed for a very, very serious problem here. So we will see if we can get that together right away. Some of that is also in the NDAA now in a rather controversial way.

Let me see. We have $3.5 billion of military construction projects that are delayed, unfunded, defunded. Uh-huh. So I want the four of you—I think—yeah, we have got the Marine Corps behind you—to tell us within the next 2 weeks what you intend to do with those projects that are defunded. Okay? It is a serious problem. I spent the last—spent a week in Europe on this, and the problem is of paramount importance there. Mr. Putin could not have had a greater gift than the message that the President delivered that we really don't care about European Deterrence Initiative.

So there are projects there. I appreciate the Army particularly coming forward with specific information, also the Air Force, about projects that are defunded, the importance of them, but it is much more than that. So, we don't need to worry about those, that I did have the opportunity to see last week, but the rest of them. So you are going have to restack, and we are going to spend a lot of time on this restacking. So get prepared.

The other thing is—I think I better let it go at that point. You may get me started on something that will get ugly real fast.

So thank you very much, gentlemen.

Jim, thank you for the opportunity for additional questions.

I will look forward to that—week and a half—information. Thank you very much.

Mr. LANGEVIN. Very good. Thank you, John.

I just want to thank Chairman Garamendi and Ranking Member Stefanik and Ranking Member Lamborn, the members of the committee, both committees, for this joint hearing and for our witnesses' testimony. I know there is some followup that you will need to do with us, get back to the committee and do the questions we have asked. Look forward to those answers.

Members may have additional questions that they will submit. We would ask that you would respond to those as expeditiously as possible but want to thank you all for the work you are doing on behalf of the country. This is an important hearing, a good hearing, and a lot of important information we were able to cover.

So, with that, this subcommittee stands adjourned.

[Whereupon, at 4:45 p.m., the subcommittees were adjourned.]

APPENDIX

OCTOBER 16, 2019

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

OCTOBER 16, 2019

Opening Statement
Chairman James R. Langevin
Intelligence and Emerging Threats and Capabilities Subcommittee
Resiliency of Military Installations to Emerging Threats
October 16, 2019

The subcommittee will come to order. Welcome to this joint hearing with the Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities and the Readiness Subcommittee. Today, we will examine the resiliency of our military installations to emerging threats. Holding this hearing has been a priority for this subcommittee for the past several months. I thank the Ranking Member for her bipartisan cooperation on this hearing. I am also thankful to my friend Chairman Garamendi for working so diligently in making today possible.

Let me welcome our witnesses. Mr. Robert McMahon, Assistant Secretary of Defense for Sustainment – Mr. McMahon, it's good to see you again. I understand you are leaving the department next month, so I just want to take this opportunity to thank you for your many decades of service to the country – in uniform and in your role now. Mr. John Henderson, Assistant Secretary of the Air Force for Installations, Environment and Energy; Mr. Alex Beehler, Assistant Secretary of the Army for Installations, Energy and Environment; and Mr. Lucian Niemeyer, Acting Assistant Secretary of the Navy for Energy, Installations and Environment. Thank you all for your willingness to testify on this critical topic.

We are here today to ensure that the Department is prepared to account for and address vulnerabilities – physical and digital - to our military installations at home and overseas. This includes the effects of climate change, energy dependence, land management and cyber incidents - among others - on the threat assessments, resources, and readiness of our nation's military. This also includes the risks to conducting operations both today and into the future.

This Subcommittee has conducted rigorous oversight into installation resilience and I am particularly concerned about what the Department is doing to ensure our installations are able to withstand ever increasing threats from malicious cyber activities and severe climate events. When it comes to our armed forces, we have not given these threats to our installations the attention they deserve. I'd like to remind those in attendance that this hearing marks one year since the Department suffered nearly ten billion dollars in damage from just two extreme weather events at Tyndall Air Force Base and Camp Lejeune. I could not think of better examples of the perils our defense infrastructure faces from climate change, perils that will only accelerate as we pump more greenhouse gases into our atmosphere. Our committee has acted on a bipartisan basis to acknowledge these risks, but I must say I have been disappointed in the Department's response to our oversight. The initial accounting of at-risk bases we received did not include Camp

Lejeune or Tyndall Air Force base at all. If those are the low risk bases, one can only wonder what we are likely to see soon from the installations the Department identified as being of particular concern. We need a clear accounting of the risks – with dollar figures attached – or else we will continue the cycle of throwing good money after bad, which is not only fiscally irresponsible, but places our service members and readiness at risk. I also want to make it clear to my colleagues that we will be holding an IETC hearing specific to the emerging threat of climate change later this year.

In addition to the threats posed by extreme climate events, the threats presented by attacks on cyber and energy infrastructure by both state and non-state actors continue to grow and evolve at a rapid pace. These threats can target critical infrastructure on our military installations, including the electric grid, water supply, or even medical facilities. An attack on the electric grid could have profound effects on the ability of the force to carry out critical missions. We must increase the resilience of operational technology on installations, and ensure we sufficiently focus on securing cyber-physical systems as well as traditional IT infrastructure. I am interested in hearing more about how the Department is building cyber resiliency on installations at home and abroad. It is incumbent upon the Department and Congress to ensure we are properly preparing for these threats to installations and I look forward to hearing from our witnesses on this topic.

And with that, I will now recognize Ranking Member Stefanik, and then we will turn to Chairman Garamendi and Ranking Member Lamborn for their remarks.

Statement of Hon. Elise M. Stefanik
Ranking Member, Subcommittee on Intelligence and Emerging Threats and Capabilities
Hearing on
Resiliency of Military Installations to Emerging Threats
October 16, 2019

I would like to start by thanking Chairmen Langevin and Garamendi, as well as my fellow Ranking Member Mr. Lamborn, for holding this important hearing today to discuss resiliency of Department of Defense installations and facilities.

And welcome to our witnesses. We have a lot of ground to cover so I will keep my opening remarks brief.

As I think about resiliency of military installations and infrastructure, I am concerned about shortfalls in both the physical and the digital domains.

First, we remain vulnerable to extreme weather events and climate change. We have seen these events adversely impact public safety, our economic security, and our national security. Our Intelligence Community continues to assess that global environmental degradation and climate change are likely to fuel competition for resources, economic distress, and social discontent across the globe through 2019 and beyond.

And we continue to experience extreme weather events at home, including in my own district, the North Country of New York. We must therefore factor in these environmental challenges when discussing resiliency of military installations – and I look forward to hearing from our witnesses exactly how we are planning for extreme weather events and climate change.

Second, I continue to have concerns about installation and infrastructure vulnerabilities in the digital domain.

Congress, and indeed this committee, had the foresight to understand these challenges and three years ago directed the Department to conduct a comprehensive review to evaluate cybersecurity vulnerabilities of DOD infrastructure. Unfortunately, this review and the subsequent corrective actions remain far from complete, and we are still incredibly vulnerable to attack.

I fear we have not yet even identified the scale and scope of our problems, let alone begun to mitigate our most concerning shortfalls.

When we consider resiliency, we must remember that advances in Information Technology, cybersecurity, and information assurances are primary prerequisites for the future of warfare. These enabling technologies form the foundation where information and data are a strategic resource to be protected, preserved, and fully actioned.

Only then will we be able to leverage evolutionary – and even revolutionary – technologies such as AI, 5G, high performance computing, and even Quantum computing.

This future begins and ends with our facilities and installations, which will be our greatest resource or our weakest link.

I look forward to discussing today how we can work together, to ensure that resiliency is prioritized so that we are prepared for these challenges in our increasingly complex digital age.

Thank you, and with that I yield back.

Statement of the Honorable John Garamendi
Chairman, Readiness Snbcommittee

"Resiliency of Military Installations to Emerging Threats"

October 16, 2019

Good afternoon. I'd like to start by thanking Chairman Langevin for suggesting that we hold this joint hearing so that our two subcommittees can better understand the emerging threats that our military installations face and what the Department is doing to improve the resiliency and readiness of our infrastructure.

Installation resiliency is a foundational readiness issue. Our bases and infrastructure investments must be able to withstand, to the maximum extent possible, the spectrum of resiliency threats from energy disruptions, cyber-attack, and natural disasters. Both of our subcommittees have put considerable time into examining the threats and actions the Department should consider taking to prepare for the effects of climate change, hearing from think tanks, the Government Accountability Office, and the intelligence community.

Over the last year, we have seen the aftermath of increasingly extreme weather events such as Hurricanes Florence and Michael and the flooding around Offutt Air Force Base in Nebraska, causing billions of dollars in damage. I have been clear that I expect the Department to rebuild these bases thoughtfully and to maximize resiliency. I will insist that the Department be forward-looking in its assessment of the threats related to sea-level rise and extreme weather to ensure tax-payers get the full value of their investment in military infrastructure.

But installation resiliency is broader than weather resiliency. The services must be able to quickly recover from energy disruptions from any cause, be it from natural disaster or a more malicious source. Over the several years, the services have been conducting energy gap analysis at their installations with a focus on the most critical missions. I am interested in hearing about what they have learned, and how they plan to address those gaps, particularly from threats coming from outside the fence line. I am also interested in hearing about the innovative approaches the services are using to resolve these gaps sustainably and by utilizing the knowledge and expertise of the private sector.

Questions about the Department's preparedness for energy disruptions are also tied to cyber-security. I am told that the services have faced considerable challenges in implementing cyber-security best practices in areas such as industrial control systems that monitor and control energy, water, and waste systems on our installations. I look forward to hearing about the progress they have made in implementing those best practices and in managing cyber risk generally at our installations worldwide.

The threats to installation resiliency are diverse and require a holistic approach to ensure that readiness is minimally impacted when foreseeable events occur. The Department must identify and seek to mitigate these threats enterprise-wide and in a systematic way. I expect our witnesses today will give us a greater understanding of how they are managing these threats now and into the future. With that, I would yield back the remainder of my time to Chairman Langevin.

Statement of Hon. Doug Lamborn
Ranking Member, Subcommittee on Readiness

"Resiliency of Military Installations to Emerging Threats"

October 16, 2019

Thank you Chairman Langevin, Chairman Garamendi, and Rep. Stefanik for scheduling this joint subcommittee hearing on such an important topic. Installation resilience has always been important to our national defense but given the dynamic and evolving nature of the threats we face, it is becoming even more critical.

Most of our installations rely at least in part on power generated in nearby communities. At the same time, the armed forces have invested significantly in renewable energy. I am very interested to hear from our witnesses today regarding their efforts to improve energy resilience and efficiency on our military installations, as well as protect it from capable and cunning adversaries.

Having recently visited all four bases damaged by storms and earthquakes that we are addressing in our FY20 National Defense Authorization Act, I am also concerned about getting our work done quickly to fund the $5 billion necessary for reconstruction. Without this funding, the critical missions will continue to be negative impacted, including:

- The Air Sovereignty and F22 training missions at Tyndall Air Force Base;
- One of kind Navy research testing missions at China Lake;
- Runway operations, tanker simulator, and critical missions of the 55th Wing at Offutt Air Force Base; and
- The Marines at Camp Lejeune, New River and Cherry Point continuing to operate after approximately 800 buildings were compromised with 500 severely damaged; and
- We also owe it to our military families to ensure that the privatized military family housing is fully restored. The damage in North Carolina and Florida continues to create a burden for these families.

I look forward to hearing from our witnesses about how they are ensuring that we plan effectively, build to appropriate building codes, incorporate lessons learned from recent disasters, and inspect work on new construction to ensure it met specifications.

Thank you for your testimony today. I yield back.

HOLD UNTIL RELEASED
BY THE COMMITTEE

Statement of

Honorable Robert McMahon

Assistant Secretary of Defense

(Sustainment)

Before the House Committee on Armed Services

Subcommittee on Intelligence and Emerging Threats and Capabilities and

Subcommittee on Readiness

Resiliency of Military Installations to Emerging Threats

October 16, 2019

Chairmen Langevin and Garamendi, Ranking Members Stefanik and Lamborn, and distinguished members of the Subcommittees: Thank you for the opportunity to discuss the Department's efforts to enhance installation resiliency.

Our installations are key platforms for our nation's defense. They are our power projection platforms and support every mission the DoD Components undertake to defend this nation. Therefore, we must work to ensure installations and infrastructure are resilient to a wide range of challenges—regardless of the source—to include weather, climate, natural events, disruptions to energy or water supplies, and direct physical or cyber attacks. We have been and will continue to be proactive in developing comprehensive policy, guidance, and tools to mitigate these impacts, with a focus on robust infrastructure, sound land management policies, and increased energy resilience.

Building Installation and Range Resiliency

To ensure that our installations are prepared to support the defense of this nation, the Department takes a broad, systemic approach that considers threats to both built and natural infrastructure. Not only must we ensure that facilities themselves are resilient in the face of a range of threats, but we must also ensure that the surrounding land, water, and airspace can support mission-essential activities.

Facilities

Regarding the built environment, the Department pursues resilience through application of its building codes in both installation planning, and design and construction of individual facilities. The Department updates these building codes, collectively known as Unified Facilities Criteria and Unified Facilities Guide Specifications, on a regular basis to reflect revised industry and federal standards. As building technologies improve and data from natural disasters increases over time, these standards become more stringent towards protecting life and property in these types of events. Examples of this include criteria for civil engineering related to flood mitigation and structural engineering related to earthquake resilience—both of which the Department has updated in the last year. In the case of earthquake codes, the Department's structural criteria actually surpass the national codes in several areas, and even exceed those of California in a couple of areas (hospital retrofits and long-span structures such as aircraft hangars).

Beyond the use of current industry standards, the Department is pursuing other initiatives to improve the resilience of its built environment. These include the following:

- The Department is incorporating analysis of climate-related risks specific to an installation into the master plan for that installation, to better guide development and facility design.
- As reported by the Government Accountability Office, the Department is moving towards incorporating forward-looking projections of climate-related data into its planning and design criteria, starting with projections of sea level change for coastal installations that will increase areas of inundation and expand floodplains at many locations. We are also

pursuing the development of a tool to identify additional sources of forward-looking climate-related data projections that will impact other aspects of installation planning and building design ranging from floodplain mapping to heating and cooling requirements.

- The Air Force recently completed a comprehensive analysis of severe weather events and their impact on built infrastructure that will further inform additional refinements in our criteria to improve resilience of future projects.
- The Army Corps of Engineers is testing a screening tool developed in-house to efficiently identify buildings at extremely-high risk in an earthquake event. This tool would sharply reduce the time and resources needed for such assessments compared with conventional methods.

Environmental Conservation and Compatible Development

The Department's lands and waters are vital to readiness. As training, testing, and operational requirements expand and new weapons systems are introduced, access and use of ranges becomes increasingly important. However, they also support a diverse array of fish and wildlife species, including nearly 500 that are federally protected under the Endangered Species Act, and over 550 that are at risk of needing listing protection. Managing for healthy and resilient natural landscapes, such as reducing fire risks, avoiding wildlife conflicts, removing invasive species, and improving range and training areas, provides the conditions necessary for mission-essential activities.

The Department continues to invest its Conservation funds to maximize our flexibility to use lands for military purposes and to address incompatible land uses beyond our fence lines. We are also developing policy providing governance within and across DoD, coordinating with other federal agencies, and interfacing with state and local governments and developers to counteract ever-increasing encroachment and promote compatible development to preserve mission capabilities.

To assist installations in developing plans to manage the evolving natural resources challenges, the DoD worked with the National Wildlife Federation to develop planning guidance – "Climate Adaptation for DoD Natural Resource Managers." The guide, published in June 2019, provides an overview of how a changing climate may affect military lands and other resources, and outlines a process to incorporate adaptation strategies into Integrated Natural Resource Management Plans (INRMP). The approach outlined in the guide can be used by installations to help improve land and natural resource resilience.

Two key programs that facilitate these sustainment efforts are the Readiness and Environmental Protection Integration Program (REPI) and the Military Aviation and Installation Assurance Siting Clearinghouse.

Readiness and Environmental Protection Integration Program (REPI) – The REPI program preserves test, training, and operational capabilities that enable readiness, strengthens strategic partnerships, and supports test, training, and operational capability. The REPI program stimulates innovative and diverse partnerships between local communities and military installations that increase collaboration and promote installation resilience. Partnership agreements provide installation commanders, trainers, testers, and operators with increased mission flexibility by preventing, mitigating, or removing restrictions that can result from nearby incompatible development. In the last 16 years, REPI partnerships have protected more than 586,000 acres of land around 106 installations in 33 states.

In FY 2019, the Department was provided expanded authority under 10 U.S.C. 2684a to specifically address military installation resilience as a key element of the REPI program. This authority further enhances the REPI program's ability to engage in collaborative land protection and natural resource management activities to help installations avoid, prepare for, minimize the effect of, adapt to, and recover from extreme weather events, or from anticipated or unanticipated changes in environmental conditions.

This includes opportunities to maintain and improve "natural infrastructure," implementing solutions outside installation boundaries to enhance the benefits provided by natural systems. Natural infrastructure solutions encompasses a wide range of possible actions that can help promote installation resilience and preserve access to critical installation and range assets and capabilities. For example: restoring historical hydrology (e.g., wetlands and coastal marshes) can help prevent flooding impacts on coastal infrastructure; reestablishing oyster reefs and restoring shoreline and dune vegetation can help minimize impacts of storm surge on low-lying installations; restoring high-value habitat can enhance wildlife corridors for threatened, endangered, or at-risk species and avoid or mitigate regulatory restrictions on training, testing, and operations; and removing vegetation and managing fuel loads can minimize wildfire risk to infrastructure, personnel, and operations.

Military Aviation and Installation Assurance Siting Clearinghouse – Energy and energy-related projects, such as wind farms and transmission lines, present a major encroachment concern for DoD. In January 2011, Congress directed establishment of the Clearinghouse, focusing DoD's official engagement within the Federal Aviation Administration (FAA) Obstruction Evaluation Airport and Airspace Analysis (OE/AAA) program and setting clear guidelines for DoD's review and response to energy project proposals. Recently, the Clearinghouse also assumed the role of coordinating offshore energy and energy-related programs, helping ensure consistency both within the Department and in DoD's engagements with external entities.

The Clearinghouse supports the Department's efforts to create resilient installations and ranges, protecting operating areas and missions that directly support National Defense Strategy objectives and efforts to build a more lethal force. Through the Clearinghouse the Department develops and articulates its position on proposed energy projects, determining whether or not they are compatible with training, testing and operations. In addition to coordinating with the FAA, the Clearinghouse responds to inquiries from federal agencies, state governments, tribal governments, energy developers and others seeking a DoD mission compatibility assessment. By working closely with the Military Departments, Joint Staff and other DoD components, the Clearinghouse has successfully avoided unacceptable risks to missions and national security. This builds upon the department's successes on land by ensuring all stakeholders are engaged in the process to preserve and enhance our offshore ranges and operating areas.

In FY 2019, the Clearinghouse coordinated reviews for over 5,000 energy projects, including over 750 wind farms. Wind energy development continues to be a concern for training, testing, and operations as wind turbines often exceed 500 feet in height and have the potential to adversely affect low-level training routes, air traffic control and weather radars, as well as military-unique radars across the country. In coordination with the Military Departments the Clearinghouse reviews each project to identify adverse impacts, and when necessary, engages with developers to seek mitigation strategies.

Because FAA determinations on energy projects are advisory in nature, developers may be able to construct projects even when DoD voices concern over risks to national security. As such, the Clearinghouse seeks state-level protections in areas with a large military footprint and high potential for wind energy development. Recently, Oklahoma enacted legislation that requires a mission compatibility review from the Clearinghouse for wind projects proposed within low-level military training routes. Oklahoma officials halted the construction of the wind energy project and protected the military training route for future use. While most wind energy developers are good partners and supportive of DoD missions, the Oklahoma example underscored the need for state-level support. The Clearinghouse will continue these outreach efforts to support and enhance resiliency.

Climate and Extreme Weather

The effects of a changing climate are a national security issue with potential impacts to the Department's built and natural infrastructure, as well as missions and operational plans. In January 2019, the Department submitted a Report to Congress on Effects of a Changing Climate to the Department of Defense. This report represented a high-level assessment of the vulnerability of DoD installations (based on operational roles) to five climate/weather impacts: recurrent flooding, drought, desertification, wildfires, and thawing permafrost. The report also provided an overview of efforts to increase installation resiliency.

The Department incorporates climate resilience as a cross-cutting consideration for our planning and decision-making processes, and not as a separate program or specific set of actions. Specifically, the Department considers resilience in the installation planning and basing processes. This includes consideration of environmental vulnerabilities in installation master planning, management of natural resources, design and construction standards, utility systems and service, as well as emergency management operations.

From a policy perspective, the Department has published several issuances to ensure the Services and Joint Staff integrate climate scenarios into planning. DoD Directive 4715.21, Climate Change Adaption and Resilience, assigns responsibilities to components to incorporate climate considerations into planning for infrastructure and operations. DoD Instruction 4715.03, Natural Resources Conservation Program, requires consideration of climate impacts during development of Installations Natural Resources Management Plans. In 2017, the Department updated DoDI 6055.17, DoD Emergency Management Program, to ensure the consideration of an all hazards approach to manage risks, including weather and climate related impacts on military installations.

It is important that our installations be resilient to a wide-range of vulnerabilities, including climate factors such as changing sea level, coastal and riverine flooding, drought, desertification, wildfires, thawing permafrost, select historic extreme weather events, and reduced aviation lift capacity due to air quality. The Department is deploying a number of tools to assist the DoD Components and installations in planning for these vulnerabilities:

- The Coastal Assessment Regional Scenario Database provides regionalized sea level scenarios for three future time horizons (2035, 2065, and 2100) for 1,774 DoD sites worldwide. The Database also contains extreme water levels statistics (storm surge without waves and wave run up) for annual exceedance probabilities (1, 2, 5 and 20 percent) based on historical tide gauge data. This information can be used to establish base flood elevation and potential future flood inundation areas of concern for installations in coastal and tidal areas.
- To provide assistance in conducting consistent analysis of risks based on prevailing scientific analysis, my office has funded U.S. Army Corps of Engineers (USACE) to build on the climate exposure tool originally developed for the Army to evaluate its installations. The DoD Climate Assessment Tool (Tool) will be expanded to include select historic extreme weather events and effects on aviation lift capacity. We have also funded USACE to apply the Tool to selected sites in the United States and overseas – 50 in the United States and 10 overseas for each Military Department. USACE will produce a summary report for each Military Department and a report for each site. The reports will include background information on the climate factors, the methods used in the assessment, preliminary results, and examples of resilience measures for consideration at specific installations. All work is scheduled to be completed by September 2020.

Research

DoD's Strategic Environmental Research and Develop Program (SERDP) and Environmental Security Technology Certification Program (ESTCP) invest in research focused on improving DoD understanding of environmental risks to installations and mission. SERDP and ESTCP investments support the development of the science, technologies, and methods needed to manage and enhance the resilience of DoD installation infrastructure with the goal of maximizing mission readiness. The following are a few examples of SERDP research efforts related to infrastructure and mission resiliency:

- In response to drought risk, SERDP initiated a study to understand and assess environmental vulnerabilities on installations in the desert southwest. This research seeks to detect and assess drought response of sensitive riparian forests to drought stress over recent decades and will be carried out within three DoD bases in the Southwest, with widely applicable results.
- In response to wildfire risk, SERDP developed a Fire Science Strategy in 2014 focused on the following: improved characterization, monitoring, modeling, and mapping of fuels to support enhanced smoke management and fire planning at DoD installations; enhanced smoke management using advanced monitoring and modeling approaches; and research to quantify, model, and monitor post-fire effects.

- SERDP and ESTCP investments seek to understand changes to the Arctic terrestrial environment relevant to DoD infrastructure. Permafrost degradation can impact soil, vegetation, buildings, roads, and airfields. SERDP and ESTCP investments are leading to tools for making Arctic infrastructure more "aware" of permafrost changes before costly failures occur. An example is Lawrence Berkeley National Laboratory's fiber-optic geophysical sensing package capable of providing real-time information on subsurface conditions relevant to infrastructure performance and failure in Arctic environments.

Water Vulnerability

The Department must take adequate measures to plan, prepare, and provided for an adequate water supply to meet mission needs. Increasing demand for water places stress on the same finite supplies of water that DoD installations depend on to fulfill their missions. In addition, the effects of a changing climate, along with near-term weather variability, may exacerbate water shortages and makes the management of water resources in the future more challenging. DoD must have a thorough understanding of its current and future water needs for each military installation. It is imperative that DoD plan and manage its water resources to ensure the sustainment of our mission and enhance our water security.

It is the policy of the DoD that each installation and range:

- Preserve its water rights under Federal and State law as is necessary to support the mission requirements; and
- Identify, as needed, additional water quantities required to meet reasonably foreseeable mission requirements and water resources that may be available to fulfill the requirements.

To be prepared for water vulnerabilities, including water shortages, the Military Departments must ensure that installations have programs and procedures to document access to water/water sources, to resolve conflicts, and to prioritize water usage during periods of scarcity.

Department of Defense Energy Programs

Energy is an essential enabler of military capability and the Department depends on energy-resilient forces and installations to achieve its mission. In FY 2018, the Department spent $3.4 billion on energy to power over 585,000 facilities and 160,000 non-tactical vehicles at over 500 worldwide military installations. Additionally, the Department consumed over 85 million barrels of fuel to power ships, aircraft, combat vehicles, and contingency bases at a cost of nearly $9.2 billion.

As described in the National Defense Strategy, the Nation's critical infrastructure, particularly energy assets, is being targeted by a range of adversaries. Recent events at Tyndall AFB, Offutt AFB, and Camp Lejeune also are sober reminders of the catastrophic effects that weather can have on the Department's missions. To address all hazards, both man-made and climate related, my office has worked proactively to lay the policy groundwork needed to ensure that energy resilience and cybersecurity are integrated across our full portfolio of appropriated and third-party financed programs.

These efforts described below are part of a broader "energy resilience roadmap" to ensure that our forces remain ready both now and in the future. These initiatives are supported by our Components and bolstered by key legislative requirements passed by Congress over the past several years. The Department appreciates the support received from this committee, and recognizes that your contributions have been invaluable in helping the Department strengthen its energy posture in support of mission readiness.

Energy Resilience Policies, Programs, and Tools

As defined in Section 101 of Title 10, energy resilience is the "ability to avoid, prepare for, minimize, adapt to, and recover from anticipated and unanticipated energy disruptions in order to ensure energy availability and reliability sufficient to provide for mission assurance and readiness, including mission essential operations related to readiness, and to execute or rapidly reestablish mission essential requirements."

The Department utilizes a portfolio of appropriated and third party financed programs to pursue energy resilience. These programs are governed by key instructions and policies to ensure warfighter requirements are addressed holistically and in a prioritized and cost effective manner.

Policies and Programs

Department of Defense Instruction 4170.11, Installation Energy Management – This formal policy provides guidance, assigns responsibilities, and prescribes procedures for all DoD installation energy management activities to include energy resilience requirements. It is currently being rewritten to further strengthen the role of installation energy plans and the inclusion of energy resilience and cybersecurity provisions.

Installation Energy Plans – Through the Installation Energy Planning (IEP) process, military installations are tasked with identifying mission critical loads, assessing energy resilience and cybersecurity gaps, and developing scalable and cost effective solutions to close those gaps. The Services have begun to submit IEPs for priority mission installations and will submit plans for top energy consuming installations by the end of FY20. All remaining installations will be required to complete IEPs by the end of FY21. To guide the IEPs, the Military Services have developed portfolio-level tools such as the Air Force's Mission Thread Analysis and the Navy's Energy Security Assessment tool to identify and prioritize gaps and investments. The Army also is leveraging OSD-provided tools to help prioritize investments.

Energy Resilience and Conservation Investment Program (ERCIP) – ERCIP is a subset of the Defense-Wide Military Construction Program, specifically intended to fund projects that improve energy resilience, contribute to mission assurance, save energy, and reduce DoD's energy costs. ERCIP accomplishes these goals through construction of new, high-efficiency energy systems or through modernizing existing energy systems. For example, at Beale AFB, ERCIP funding will construct an electrical substation to provide a secondary source of power to the Global Hawk mission. At Anniston Army Depot, ERCIP funding will establish on-site generation and grid controls to assure critical production and maintenance of combat vehicles during extended grid outages.

Energy Savings Performance Contracts (ESPC)/Utility Energy Savings Contracts (UESC) – ESPCs and UESCs continue to be important tools for financing resilient and efficient energy solutions. In November 2018, the Department updated ESPC/UESC policy to include resilience and cybersecurity requirements, better align these programs with the IEP process, and add post-award management requirements to maximize the full operational value from each project. For example, an ESPC at MCRD Parris Island enhances readiness through the installation of a 3.5 megawatt combined heat and power plant, 6.7 megawatts of solar photovoltaic panels with integrated energy storage, and a microgrid control system. These and other equipment upgrades will reduce energy consumption by 88% and water consumption by 25%. The Air Force is implementing a $262 million ESPC at Tinker AFB to modernize 50 buildings with energy conservation measures expected to increase energy efficiency, reliability, and resiliency, and support critical industrial processes at the depot.

Other Alternative Financing Authorities – The Department continues to leverage other alternative financing authorities to implement energy resilience and cybersecurity. These include power purchase agreements, enhanced use leases, and utilities privatization, when supported by the business case and/or IEP. For example, at Schofield Barracks in Hawaii, the Department is utilizing an enhanced use lease to gain access to a 50MW multi-fuel power generation plant that provides black-start capability for three critical Army installations during disruptions to the grid. Utilities privatization at Hill AFB also is improving the reliability of the energy distribution infrastructure needed to support critical missions at the Ogden Air Logistics Center and the 388th Fighter Wing (F-35). To accelerate the use of alternative financing mechanisms for energy resilience, DoD recently completed a review of best practices from the commercial finance industry and lenders. Based on stakeholder input across government and industry, the recommendations from the *Defense Energy Resilience Bank* study will inform how the Department achieves energy resilience through alternative finance.

Micro-reactor Demonstration – As directed in the FY 2019 National Defense Authorization Act, the Department of Defense will demonstrate a commercially developed, Nuclear Regulatory Commission (NRC) licensed, very Small Modular Reactor (vSMR) to power critical loads at a permanent domestic military installation by December 2027. Industry is making steady progress in developing advanced micro-reactors with the potential to enhance installation resilience through assured access to power in support of critical missions and remote operations. The Department will use the proposed demonstration to assess the energy resilience capability and the cost effectiveness of vSMR technology.

Exercises and Tools

To facilitate the implementation of energy resilience policy, the Department is utilizing exercises and analysis tools to continually improve our approach.

Energy Resilience Readiness Exercises (ERRE) – In accordance with U.S. Code Title 10 Section 2911 and DoD instruction 4170.11, the Department is performing ERREs to evaluate energy resilience risks to readiness while completely separated from the commercial electric grid. ERREs identify critical energy vulnerabilities and interdependencies that could degrade critical missions, assess latent risks in an installations energy resilience posture, and inform the development of appropriate mitigations. The Department has facilitated the planning and execution of exercises at Fort Stewart, Fort Greely and Fort Bragg. Looking ahead, the Department will complete three more ERREs at Hanscom AFB, Vandenberg AFB, and MCAS Miramar in FY20, and the Services are planning and budgeting to conduct future ERREs at priority installations. Based on best practices and lessons learned, my office will issue policy and guidance in the near future with the goal of enabling the Services to independently and routinely perform their own ERREs.

Energy Resilience Analysis Tool (ERAT) – To enable the identification and development of critical energy requirements, models, and metrics, my office commissioned the Massachusetts Institute of Technology Lincoln Laboratory (MIT-LL) to create the Energy Resilience Analysis Tool (ERAT). Fielded in the latter part of 2018, ERAT helps Military Components develop scalable and cost effective energy projects by providing a range of resilient alternatives based on technical and cost factors to address critical loads. Due in part to the transparency of this analysis, the use of ERAT is now required for ERCIP project submissions starting in FY22.

Cyber Secure Facilities

Given the importance of energy resilient facilities as nodes for projecting and sustaining power, the Department is reducing the cyber risks to facility related control systems (FRCS). Building on the July 2018 Deputy Secretary of Defense memorandum, *Enhancing Cybersecurity Risk Management for Control Systems (CS) Supporting DoD Owned Defense Critical Infrastructure*, my office has integrated the cyber security of industrial control systems into energy policies and guidance.

FRCS Cyber Security Plans – To build a FRCS defense posture, Components are refining cybersecurity plans to account for the capabilities and resources required to implement controls on highest priority assets, systems, and supporting systems. As a complement to overall installation energy plans, Components will update FRCS cybersecurity plans by April 2020.

Aligning Resources to Requirements – My office also is developing the framework for identifying the required resources for inventorying, assessing, mitigating, and sustaining FRCS Programs, and then arraying these requirements against component resources. Including staff training and the funding for "cyber hygiene," the FRCS budget exhibit will not only confirm what is needed to ensure the cyber security of control systems, but also enable appropriate oversight and governance during program and budget reviews.

Cybersecurity in ESPCs, UESCs, and Utilities Privatization – My office is taking the lead in issuing internal policy and governance for DoD Services and Components as well as requiring a cybersecure posture from partners. The Department is developing internal requirements for 'inside the fence' as well as requirements for external partners 'outside the fence' to be cybersecure and cyber-resilient. For example, military installations are including cyber security considerations in the development of their installation energy plans, and FRCS considerations are now required for utility privatization agreements, ESPCs, and UESCs.

We will continue to work with the Department's Chief Information Officer and Principal Cyber Advisor toward solutions and resources ensuring FRCS are defensible, survivable, and resilient to operate and sustain critical functions in a cyber-contested environment.

Conclusion

Thank you for the opportunity to testify on the Department's efforts to build resilient installations. Your continued support of Department of Defense's mission and for our military members and their families is appreciated.

The Honorable Robert H. McMahon
Assistant Sccretary of Defense for Sustainment

Mr. McMahon is the Assistant Secretary of Defense for Sustainment. He serves as the principal staff assistant and advisor to the Under Secrctary of Defense for Acquisition and Sustainment, Deputy Secretary of Defense, and Secretary of Defense on sustainment in the Department of Defense, and is the principal logistics official within the senior management. Mr. McMahon provides oversight of logistics policies, practices, and efficiencies to enable readiness across the Department of Defense and manages over $170 billion in logistics operations. Mr. McMahon provides budgetary, policy and management oversight of the Department of Defense's real property portfolio that consists of 28 million acres, over 500 installations, and more than 500,000 buildings and structures valued at $1 trillion dollars. He is rcsponsible for the Department's planning, programs, and capacity to provide mission assurance through military construction, facilities investment, environmental restoration and compliance, installation and operational energy resilience, and occupational safety programs. Mr. McMahon previously served as the Assistant Secretary of Defense for Logistics and Materiel Readiness from November 2017 to August 2018.

From 2015 to 2017, Mr. McMahon served as President of Fickling Management Services in Macon, Georgia. He led a team of commercial real estate professionals whose portfolio spanned cight states. Previously, hc served as thc Director of Field Operations and Site Lead (Warner Robins Air Force Base, Georgia) of the Bocing C-17 Globemaster III Integrated Sustainment Program (GISP), and as the CEO of the 21st Century Partnership in Warner Robins, Georgia.

Mr. McMahon retired from the Air Force as a Major General in 2012, after more than 34 years of service. Born in Toledo, Ohio, he entered active duty in the United States Air Force after graduation from the U.S. Air Force Academy in 1978. His command experience includes a maintenance wing, a logistics group and two maintenancc squadrons. He has served as the Director of Maintenance for the Ogden Air Logistics Center, and as the Director of Propulsion for the San Antonio ALC. General McMahon was also the military assistant to the Assistant Secretary of the Air Force for Installations, Environment and Logistics, Headquarters U.S. Air Force. He has also served as the Director of Logistics, Deputy Chief of Staff for Logistics, Installations and Mission Support, Headquarters U.S. Air Force.

Immediately prior to retirement, General McMahon served as Commander of the Warner Robins Air Logistics Center, Robins Air Force Base, Georgia. He was responsible for worldwide logistics support for C-130 and C-5 transport aircraft, F-15 fighter aircraft, U-2 reconnaissance aircraft as well as support for remotely piloted vehicles, Air Force helicopters, air-to-air missiles, surface motor vehicles and high-technology airborne electronics, avionics and electronic warfare requirements. The center was one of three Air Force air logistics centers and the largest single-site industrial complex in the state of Georgia.

Mr. McMahon holds a Bachelor of Science degree from the United States Air Force Academy and a Master of Science degree in Maintenance Management from the Air Force Institute of Technology.

DEPARTMENT OF THE AIR FORCE

STATEMENT BY

HONORABLE JOHN W. HENDERSON
ASSISTANT SECRETARY OF THE AIR FORCE
(INSTALLATIONS, ENVIRONMENT, AND ENERGY)

BEFORE THE

SUBCOMMITTEE ON READINESS

AND

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

COMMITTEE ON ARMED SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

SUBJECT: RESILIENCY OF MILITARY INSTALLATIONS TO EMERGING THREATS

OCTOBER 16, 2019

NOT FOR PUBLICATION UNTIL RELEASED BY
THE COMMITTEE ON ARMED SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

Introduction

The Air Force fights from our bases. We project power, generate readiness, test new platforms, train to support joint operations, and provide safe and healthy communities for our families at our bases. A global network of interdependent air bases enables the Air Force to deliver air, space, and cyberspace capabilities for joint warfighting operations. Therefore, the readiness and resiliency of our installations is a matter of strategic importance to our Nation and a necessity to meet the National Defense Strategy's call for a more lethal force.

The Air Force views installation resilience as the capability of a base to sustain the projection of combat power by protecting against, responding to, and recovering from deliberate, accidental, or naturally occurring events that impede air, space, or cyberspace operations. To meet mission requirements the Air Force must continually adapt to meet current and future threats, including severe weather, climate, energy and water disruption, and direct physical or cyber-attacks.

Through a holistic, deliberate, and proactive planning process, the Air Force incorporates resiliency measures in the development of the policy, guidance, and tools necessary to ensure our installations remain resilient in the face of threats. Leveraging our long-term Infrastructure Investment Strategy (I2S), the Air Force enhances resiliency by proactively upgrading facilities through targeted facility investments informed by powerful analytics, increased funding, evolving building codes, and improved processes.

Maintaining a resilient posture is a continual process of assessing threats and prioritizing available resources to mitigate the evolving risks to our missions created by these threats. The Air Force is taking the necessary steps to build resilient installations that are ready to withstand and quickly recover from man-made and natural events which could potentially impact our missions.

Installation Energy and Water Resilience

Energy and water are finite resources that often require long, complex, interdependent, and vulnerable logistics tails. The Air Force requires reliable power and water to accomplish both operational and training missions. The overarching vision for the Air Force's installation energy and water program is "Mission Assurance through Energy Assurance." This vision is focused on securing the ability to perform the warfighting mission, in the face of disruptions to traditional sources, while simultaneously optimizing energy and water productivity through technology and process improvements.

When assessing energy and water infrastructure requirements, the Air Force carefully considers resilience and cost, with emphasis placed on resilience, or the ability to plan for and respond to a denial of service. From the Air Force perspective, all energy and water projects must improve resilience in some capacity. Cost, the second factor, focuses on meeting requirements in the most cost effective manner. Finally, in recognition of the supply chain value associated with renewable energy, the third factor considered in evaluating energy sources is whether the source is clean or renewable

Installation Energy Resilience

Energy enables Air Force missions; without it, our ability to project power would be halted or severely hindered. Thus, the Air Force Installation Energy program focuses on ensuring Air Force installations have the energy required to fight from our bases, at any time and in the face of any circumstance. One key focus area addresses the growing threat associated with natural or nefarious events or activities that result in a denial of service, such as missions being separated from access to the national electrical grid and the increasing potential for long duration power outages. Using mission thread analyses, the Air Force is working to identify key nodes on and off installations, pinpointing critical vulnerabilities through denial of service scenarios that begin with a comprehensive understanding of mission requirements and current system operations.

One aspect of this approach involves detailed insight into historical data associated with past power outages. In FY18, Air Force installations reported 239 notable outage incidents to their basic energy commodities (i.e. electricity, water, steam, natural gas, and waste water), with notable outages defined as greater than or equal to 8 hours. This represents a 33 percent decrease from FY17. This decrease can be partly attributed to increased investment in, and improved maintenance of energy systems on Air Force installations as well as better situational awareness, and more accurate reporting of outages.

In addition, the Air Force has partnered with the Office of the Assistant Secretary of Defense for Sustainment and the Massachusetts Institute of Technology Lincoln Laboratory in the development of a comprehensive "pull-the-plug" exercise framework to baseline our installation power resilience capabilities and to validate vulnerabilities, requirements and system enhancements. To date the Air Force has completed one table top and one "pull-the-plug" exercise using the aforementioned framework with one more "pull-the-plug" exercise scheduled this calendar year and three proposed for next year.

Water Resource Management

Recognizing the dynamic threat environment, the Air Force is placing a renewed emphasis on water resilience. Threats to water availability range from aging water infrastructure, vulnerable utilities, or malicious attacks to water scarcity or consequential impacts from changes in precipitation patterns, water quality issues, or encroachment. The Air Force is in the nascent stages of establishing a water resources management program that moves away from managing water based primarily on conservation and condition assessments toward a risk-based approach, which more directly supports mission assurance. This shift will be in concert with an increased focus on the Air Force's installation development and activity management planning processes. It will help provide greater transparency at the enterprise level while aiding efforts to strategically direct infrastructure investments based on mission requirements.

In addition, the Air Force recently began conducting enterprise-level threat reviews, regional analyses on water stress, and installation-level water needs assessments, as well as increased engagement with external stakeholders, such as water utilities and regional water management agencies. These efforts will drive dialogue between mission owners, installation planners, and water suppliers in anticipation of a self-assessment and data collection phase of program development. Sophisticated water stress forecasting models from the public and private sectors will provide the technical basis for the analysis.

Installation Energy and Water Planning

As the Air Force shifts its thinking away from single point solutions with fixed time horizons to more dynamic solutions for variable time lines, we are committed to reducing installation vulnerability through the incorporation of holistic resiliency measures in installation master plans. The Air Force utilizes five key resilience attributes, the 5Rs, to prioritize energy projects and ensure targeted enabling system investments are effective in supporting mission needs. The 5Rs help describe how a system plans for crises (preventative attributes) and how the system performs in event of crises; dependent on risk, events, and time (performance attributes); the 5Rs are:

- Preventative Attributes:
  - Robustness: incorporates concept of reliability and the ability to withstand disturbances
  - Redundancy: having excess capacity and back-up systems, which enable the maintenance of core functionality in the event of disturbances
  - Resourcefulness: ability to adapt to crises, respond flexibly, and neutralize negative impacts
- Performance Attributes:
  - Response: ability to mobilize quickly in the face of crises
  - Recovery: ability to regain a degree of normality after event, including ability of a system to be flexible and to evolve to deal with new circumstances

The Air Force is developing a standardized framework for all Air Force installations to identify, track, and adjust requirements to advance the energy and water resilience goals of the installation. The Air Force intends to complete installation energy plans at seven installations by the end of Calendar Year 2019, with a target of finalizing plans for 70 major Air Force installations by the end of FY22.

In 2017, the Air Force established the Office of Energy Assurance (OEA) to balance the objectives of an installation's energy initiatives while optimizing cost and providing resilient energy solutions in support of the Air Force mission. In its role as the Energy Storefront for all Air Force energy resilience initiatives, OEA serves as the single point of entry for all installation energy requirements, and integrates energy assurance into the Air Force installation energy project portfolio by leveraging public, private, and community partnerships.

Industrial Control Systems Cyber Resilience

Industrial control systems are essential to Air Force core missions as they support critical infrastructure which enables mission capabilities across Air Force installations. Technological advancements have created more efficient control systems but have also opened up additional avenues for adversaries to attack. Increasing threats to control systems have the potential to degrade Air Force missions. They can physically damage critical infrastructure and serve as a new attack vector to target the broader Air Force network.

In compliance with the National Defense Authorization Act (FY) 2017, Section 1650, we are conducting assessments of critical infrastructure to identify vulnerabilities. These assessments are exposing risks to missions that the Air Force was unknowingly accepting while also validating the mitigation measures we were already pursuing to increase control systems' cybersecurity and resiliency. One such mitigation is installing enclaves for network segmentation that logically isolate the infrastructure network traffic.

In effort to address some of the cross-functional challenges inherent to improving infrastructure cyber resilience, the Air Force is developing a strategy which synthesizes the technical expertise and authorities of several functional communities to enhance existing processes and develop comprehensive, integrated solutions. This strategy will complement defensive cyber operations focused on critical infrastructure. Our facility experts have been actively assisting our cyber partners as they develop Mission Defense Teams to focus on defending our infrastructure in cyberspace.

The Air Force is actively changing its culture to emphasize cyber resilience. Next year we will institute a workforce development program that, in supplement to existing general awareness training required for all Airmen, will provide tailored training and education to all Civil Engineer Airmen who are responsible for the sustainment of our facilities and infrastructure systems.

Natural Disasters and Severe Weather

The Air Force recognizes that our installations and infrastructure are vulnerable to a wide variety of threats, including those from weather, climate, and natural events. Changing climate and severe weather effects have the potential to catastrophically damage or degrade the Air Force's warfighting readiness. To ensure the Air Force is prepared to effectively combat the significant mission and readiness impacts incurred from recent severe weather events around the globe, the Secretary and Chief of Staff of the Air Force directed the stand-up of an Air Force Severe Weather Readiness Assessment (SWRA) Team.

The SWRA Team was tasked to conduct a full-spectrum assessment of recent and relevant Air Force severe weather event response readiness and identify optimized ways and means for combating risk to mission caused by future severe weather events. The SWRA Team presented their findings in spring 2019. In response, our headquarters created a Severe Weather Assessment Tiger Team who continue to work diligently to implement the SWRA's recommendations and conduct cost benefit analysis of the more complex action items. A large number of the more than 100 recommendations from the SWRA will be implemented, many of which drive new facility standards to be implemented as facilities are recapitalized.

To mitigate risk and assure mission accomplishment, the Air Force incorporates resiliency attributes into our facility projects when constructing new facilities with Military Construction (MILCON) funds and through Facility Sustainment, Restoration and Modernization (FSRM) funded repair projects. The Unified Facility Criteria, which provide design and construction standards for all Department of Defense facility projects, are routinely reviewed and updated, some as often as yearly, to ensure the latest design standards, industry practices, and lessons learned are incorporated.

For example, the Air Force is applying lessons learned from past severe weather events in the Tyndall Air Force Base (AFB) rebuild effort by leveraging adaptation opportunities which will increase installation resiliency after the impacts of Hurricane Michael. Informed by historic and projected flood elevations, we developed design flood criteria for new construction at Tyndall AFB. Additionally, we are incorporating best practices used in Florida's High Velocity Hurricane Zone, which is applicable to Miami-Dade County. These and other resiliency measures ensure Tyndall AFB is rebuilt with agile, flexible, smart facilities that are resilient to future severe weather events.

On the policy front, the Air Force continues to update relevant policies as they evolve to enhance our risk management framework, most recently by including consideration of climate and severe weather as potential hazards within our mission sustainment, integrated installation planning, and environmental management portfolios. Generally, the Air Force takes a base-by-base approach to building resilience to climate and severe weather impacts, as every installation location is affected by different local weather and geography.

The Air Force is collaborating with OSD and other Component Services to conduct a more robust exposure analysis of selected installations via a tool currently under development. Future site-specific studies may build on the exposure results to estimate overall vulnerability and risk and help assess where best to apply resources to improve adaptation and resiliency and maintain mission capability.

Climate adaptation and resilience is critical to Air Force mission assurance and the sustainability of our installations as our power projection platforms. It is essential the Air Force continues to integrate climate adaptation and resiliency into our processes and decisions and to invest, as necessary, to minimize risk and ensure we retain the ability to operate. Continued cross-feed of lessons learned and success stories, as well as partnering with communities and host nations, enhances our abilities to meet common climate threats while delivering capabilities.

Infrastructure Investment Strategy

Building readiness and resiliency into our Air Force installations requires a long-term vision, understanding of the foundational components which support our missions, proactive investment practices, and a well-resourced strategy with predictable funding levels. Foundational to the success of Air Force resilience efforts is the Infrastructure Investment Strategy (I2S). Signed into policy in January 2019, the Air Force I2S is a proactive, long-term plan to restore our infrastructure readiness, improve resiliency for mission critical nodes, and reduce the backlog of deferred maintenance at the lowest life cycle cost.

Deteriorating components of our infrastructure introduce vulnerabilities that increase the risk of damage during routine or severe weather events. For example, the separation of roofing materials on a facility can render its interior vulnerable to environmental conditions that could accelerate deterioration. A strong wind storm could easily lead the weakened roof to collapse, undermining the facility's structural integrity and causing catastrophic failure.

Notably, I2S strives to cost-effectively modernize our infrastructure, implement innovations in installation management, and stabilize funding levels to reduce the risk we have assumed due to decades of challenging fiscal conditions. In order to maximize impact in a short period of time, we will assess mission thread vulnerabilities and prioritize infrastructure repair requirements that directly affect the primary mission of an installation.

Ultimately, I2S provides a feasible remedy to preserve the health of our facilities and infrastructure. By embracing a cost-effective infrastructure investment approach, the Air Force intends to save billions of dollars over the next 30 years through targeted infrastructure investments, and reinvest these savings back into our bases to buy-down our maintenance backlog and improve installation resilience.

Emergency Management and Disaster Response

Equally vital to resiliency as proactive planning and investments, is our emergency management and disaster response capabilities. Using the National Incident Management System as its foundation, the Air Force Incident Management System unifies Air Force programs with interagency, state, and local communities across the emergency management mission areas of prevention, protection, mitigation, response, and recovery. The Air Force mandates every installation worldwide to have an Installation Emergency Management Plan. Each Air Force installation has an all-hazards response planning team that identifies the greatest threats to that installation and ensures they are addressed in the Installation Emergency Management Plan. An emergency management "all-hazards" assessment includes any incident, natural or manmade, that warrants action to protect life, property, health, and safety.

Through annual exercises of the Installation Emergency Management Plans, our installations are ready to face any disaster. Two days before Hurricane Michael hit Tyndall AFB it went from a Category 2 with no sights on the installation to a Category 4 with direct line of sight on the installation. Due to emergency management preparedness, emergency management exercises, and installation emergency management plans, Tyndall AFB evacuated all mission capable aircraft, military members, and families in less than 48 hours. The result: *no loss of life or aircraft*.

Additionally, smart investments in infrastructure after each disaster result in future cost avoidance, increased mission effectiveness (requiring less time to open the installation and airfield), and safety for Airmen, civilians, and families. In 2003, Hurricane Isabel hit Joint Base Langley-Eustis (Langley AFB) with a 7.9-foot storm surge and 62 mph winds causing $146 million in damage. Fast-forward to 2011, Hurricane Irene struck Joint Base Langley-Eustis with a 7.5-foot storm surge and 85 mph winds. Post-Isabel investment decisions and updated preparation procedures contributed to personnel reopening the airfield and installation in less than 24 hours. Additionally, the storm only caused $1.5M in damage versus the $146M in 2003. The Air Force will continue to learn from past events in preparing for future disasters, with a focus on ensuring the safety of our military personnel and their families while mitigating threats to effective mission generation capabilities.

Conclusion

The Air Force We Need requires sustainment of ready and resilient Air Force installations. Prudent planning, underpinned by the Infrastructure Investment Strategy, ensures the resilience of our installations as power projection platforms and maintains strategic alignment with the National Defense Strategy to enhance combat capability. The strategic importance of our Air Force installations requires us to focus on infrastructure investments to ensure bases provide the resilient capability and capacity that we need for both today and tomorrow's fight.

John W. Henderson
Assistant Secretary of the Air Force for Installations, Environment and Energy

The Honorable John W. Henderson is the Assistant Secretary of the Air Force for Installations, Environment and Energy. He is responsible for the formulation, review and execution of plans, policies, programs and budgets to meet Air Force installations, energy, environment, safety and occupational health objectives. Mr. Henderson was commissioned in the U.S. Army Corps of Engineers in May 1994, upon graduation from the South Dakota School of Mines, and retired in the grade of colonel in 2017 after a 23-year career. Mr. Henderson commanded an engineer battalion during operation Enduring Freedom and deployed with the 25th Infantry Division and U.S. Army Corps of Engineers during two tours supporting operation Iraqi Freedom. He held multiple command and staff positions throughout his career, to include five assignments with the U.S. Army Corps of Engineers, culminating as the Omaha District Commander. Mr. Henderson is registered as a licensed professional engineer in the state of South Dakota.

EDUCATION
1994 Bachelor of Science, Civil Engineering, South Dakota School of Mines and Technology, Rapid City
2002 Master of Science, Civil Engineering, South Dakota School of Mines and Technology, Rapid City
2006 U.S. Army Command and General Staff College, Fort Leavenworth, Kansas
2015 National Security Fellowship, Massachusetts Institute of Technology, Cambridge

CAREER CHRONOLOGY
1995-1996, Platoon Leader, 44th Engineer Battalion, 2d Infantry Division, Camp Howze, Republic of Korea
1996-1997, Executive Officer, 82d Engineer Company, 2d Infantry Division, Camp Edwards, Republic of Korea
1997-1998, Company Commander, Engineer Brigade, 2d Infantry Division, Camp Howze, Republic of Korea
1999-2000, Company Commander, Charlie Company, 864th Engineer Battalion, Fort Wainwright, Alaska
2000-2001, Aide-De-Camp to U.S. Army Alaska Commanding General, Fort Richardson, Alaska
2001-2002, student, South Dakota School of Mines and Technology, Rapid City
2003-2004, Hydraulics/Hydrological Engineer, U.S. Army Corps of Engineers, Vicksburg, Miss.
2004-2004, Operations Officer, U.S. Army Corps of Engineers, Multi-National Forces – Iraq, Baghdad, Iraq
2004-2005, Resident Engineer, U.S. Army Corps of Engineers, Vicksburg, Miss.
2005-2005, Deputy District Commander, U.S. Army Corps of Engineers, Vicksburg, Miss.
2006-2007, Operations Officer, 25th Infantry Division, Tikrit, Iraq
2007-2008, Battalion Executive Offieer, 25th Infantry Division, Multi-National Division-North, Tikrit, Iraq
2008-2010, Honolulu District Deputy Commander, U.S. Army Corps of Engineers, Schofield Barracks, Hawaii
2010-2011, Pacific Ocean Division Chief of Staff, U.S. Army Corps of Engineers, Fort Shafter, Hawaii
2011-2013, Battalion Commander (OEF), 864th Engineer Battalion, Joint Base Lewis-McChord, Wash.
2013-2014, Corps Executive Officer, I Corps, Joint Base Lewis-McChord, Wash.
2015-2017, Omaha District Commander, U.S. Army Corps of Engineers, Omaha, Neb.

AWARDS AND HONORS
Legion of Merit Bronze Star Medal with two oak leaf clusters
Meritorious Service Medal with silver and bronze oak leaf cluster
Humanitarian Service Medal
Combat Action Badge

PROFESSIONAL MEMBERSHIPS AND ASSOCIATIONS
Society of American Military Engineers
American Society of Civil Engineers
National Society of Professional Engineers

(Current as of March 2018)

RECORD VERSION

STATEMENT BY
MR. ALEX BEEHLER
ASSISTANT SECRETARY OF THE ARMY
(INSTALLATIONS, ENERGY & ENVIRONMENT)

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES
AND THE
SUBCOMMITTEE ON READINESS
COMMITTEE ON ARMED SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

FIRST SESSION, 116TH CONGRESS

RESILIENCY OF MILITARY INSTALLATIONS TO EMERGING THREATS

OCTOBER 16, 2019

NOT FOR PUBLICATION UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES

Introduction

Chairman Langevin, Chairman Garamendi, Ranking Member Stefanik, Ranking Member Lamborn, and distinguished members of the Committees, thank you for this opportunity to testify on "Resiliency of Military Installations to Emerging Threats" and answer any questions you may have. I begin by thanking the committees for the continued support and commitment to our Soldiers, Families, and Civilians. Your leadership and guidance are instrumental to our successful ability to defend our nation and its interests, and I look forward to working with the Committees to achieve our mutual goals of ensuring resiliency at military installations, while supporting readiness, modernization, and reform. The Army seeks to enhance readiness by strengthening our installation resilience, which is vital to accomplish our mission of protecting U.S. national security interests at home and abroad; to modernize our installations to build a more lethal force; and to reform our installation management business processes to maintain effective warfighting operations.

Emerging Threats to Army Installation Readiness and Modernization

The Army Vision states that, "*the Army of 2028 will be ready to deploy, fight and win decisively, against any adversary, in a joint, multi-domain, high-intensity conflict. Army will maintain its ability to conduct irregular warfare while simultaneously deterring adversaries anytime, anywhere*." The Army's concept of Multi-Domain Operations includes the Strategic Support Area, which is the home of Army installations. The Strategic Support Area includes cross-communications and coordination between warfighting commanders and numerous supporting agencies. Forces operating in the Strategic Support Area are never out of contact, and constantly subjected to the possibility of both lethal and non-lethal attacks. The Strategic Support Area is the home to many essential warfighting components, such as cyber, space, command and control, and sustainment capabilities. The battlefield framework has changed, and the Strategic Support Area must have installations that are ready, modern, and able to project lethal power wherever and whenever called upon.

As our installations evolve and rise in their importance to operations, emerging threats have simultaneously presented additional challenges to our installations and national infrastructure that need to be addressed. We generally categorize these threats to our installations under three broad headings: cyber, physical, and natural. As the 2018 U.S. National Defense Strategy states, "[i]t is now undeniable that the homeland is no longer a sanctuary....During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated." While our installations have for decades prepared for the possibility of physical attacks, our surrounding and supporting private and public infrastructure are likely far less prepared to prevent or mitigate against that possibility. While we remain vigilant in protecting assets within the Army fence line, we are reliant upon other parties to protect the support infrastructure we rely on for many of our installations. Not just roads and buildings, but water sources and related infrastructure, energy infrastructure, and other supply chains that keep our installations ready to support operations.

There is also the rapidly expanding concern for cybersecurity for our systems and networked infrastructure, both on-and-off installations. In the Worldwide Threat Assessment of the U.S. Intelligence Community, submitted to the Senate Select Committee on Intelligence on 29 January 2019, it was stated that, "*China has the ability to launch cyber-attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States*," and further stated that, "*Russia has the ability to execute cyber-attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016.*" The assessment went further to state that, "*Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage*."

Meanwhile, I am greatly concerned about the potential consequences of the increased frequency and severity of extreme weather events. The same Worldwide Threat Assessment states that, "*[e]xtreme weather events, many worsened by accelerating sea* *level rise, will particularly affect urban coastal areas in South Asia, Southeast Asia, and the Western Hemisphere. Damage to communication, energy, and transportation infrastructure could affect low-lying military bases, inflict economic costs, and cause human displacement and loss of life*." Meanwhile, it is also highly likely that the Army will be called upon to assist in a greater number of humanitarian and disaster response events while we are simultaneously impacted.

Army Actions Being Taken to Address Emerging Threats to Installations

A multitude of actions and policies have been put into motion by the Army to address the aforementioned threats to installation resilience. However, I want to be clear that we know we have great challenges ahead of us, to include defining the expanding scope and magnitude of the problems which these threats present. I will now highlight three areas where we have placed particular focus for our installations: cybersecurity of facility-related control systems (FRCSs), resilience of installations energy, and planning for extreme weather.

Cybersecurity of Facility-Related Control Systems

Army facilities can serve as critical nodes for projecting and sustaining power from our installations. Accordingly, the Army is improving the cybersecurity of FRCS to ensure reliable power for critical missions. This effort will enhance the Army's ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from utility disruptions that critically impact operations on military installations. In addition, this increased security will improve the sustainability of critical Army missions, provide installation support to operational warfighters, and ensure Army readiness.

To improve FRCS defense posture, Army installations are developing cybersecurity plans to account for the capabilities and resources required to implement controls on their highest prioritized assets and systems. The Army is in the process of integrating cybersecurity into its overall installation management plans and guidance. For example, our installations now include cybersecurity considerations in the planning, design, construction, operation and maintenance of Army-owned installation FRCS, as well as FRCS associated with infrastructure obtained with alternative finance authorities that may be owned or operated by private parties but in service to Army installations. Specifically, FRCS considerations are now integral to utility privatization agreements, energy savings performance contracts, and utility energy service contracts.

The Army installation enterprise is working closely with LTG Crawford, the Army's Chief Information Officer, LTG Fogarty the Army's Cyber Commander, and GEN Funk, the Army's Chief of Operations, Plans and Training, toward developing solutions and resources ensuring that our FRCS are defensible, survivable, and resilient to operate and sustain critical functions in a cyber-contested environment. A key accomplishment of this collaboration has been establishment of standard benchmarks for assessing cybersecurity risk of control systems and identifying vulnerabilities. The results of these assessments are being used to inform mitigation prioritization efforts and help ensure that infrastructure, facilities, and related services are available when needed.

In addition, the Army is working with interagency partners as well as private sector transportation providers to maintain and improve security—to include cybersecurity—of commercial transportation assets when being use by the military. Further, to ensure that we remain synchronized with local law enforcement and commercial transportation providers we periodically conduct exercises and reviews to identify and reduce friction points to achieve and maintain the required force flow.

Installations Energy Resilience

Energy resilience, or secure, uninterrupted access to energy, is essential for the Army to accomplish its mission. Supplying energy to Army installations has become increasingly challenging as vulnerabilities in interdependent electric power grids, natural gas pipelines, and water resources potentially jeopardize mission capabilities and security. Data shows that Army installations reported approximately 22,000 combined hours of utility outages in FY 2018 (including Puerto Rico outages). This is a two-fold increase since FY 2017 and an eight-fold increase since FY 2016.

To drive energy resilience more proactively, the Army has refined the processes for assessing energy and water risks and opportunities by utilizing Installation Energy and Water Plans to identify the needs of critical missions and address vulnerabilities. These comprehensive plans are being developed across Army installations in a prioritized fashion, with the first set being completed in the coming months. Installations and commands will use these plans to identify critical requirements for energy, identify energy resilience gaps, develop potential courses of action to fill these gaps, and identify and recommend solutions that are most viable for the installations. Additionally, the Army has undertaken large-scale installation energy disruption exercises in conjunction with the Office of the Secretary of Defense and Massachusetts Institute of Technology's Lincoln Laboratory. The Army has conducted large-scale exercises at four Army installations: Fort Greeley, Alaska; Fort Stewart, Georgia; Fort Knox, Kentucky; and Fort Bragg, North Carolina. These exercises disconnect Army installations from the local power grid to evaluate installations' energy posture, identify capability gaps, and prioritize mission-critical projects. These exercises have revealed capability gaps related to infrastructure, operations and maintenance; the requirement for the identification of critical loads ensuring configuration to appropriate backup generation; and better communications with the wide variety of mission, garrison, and support staff owners. Further, the exercises highlighted that "table top" exercises do not sufficiently identify all energy resilience capability gaps. The Army anticipates doing several more such exercises over the coming year.

The Army is the largest consumer of electricity and installation energy in the Federal government, and spends more than $1.1B annually. Congressional appropriations, third-party financing, and direct private investments enable the Army to undertake energy infrastructure projects to modernize and diversify on-site generation sources, and repair aging infrastructure to reduce impacts of grid outages and enhance energy resilience. The Army seeks to develop energy resilience projects with on-site energy generation, energy storage, and energy controls to create "islandable" capabilities to provide the energy necessary to sustain critical missions in the event of a major disruption in supply.

Congressional Appropriations

The Army utilizes the Energy Resilience and Conservation Investment Program (ERCIP), DoD's only direct-funded program targeted for energy resilience. The Army has been focusing on ERCIP projects to incorporate resilience attributes, conserve energy and water, reduce reliance on the grid, and construct on-site power generation and associated infrastructure. In FY 2019, the Army competed for, and received, approximately $40.5M out of $193M for eight projects that included some energy resilience capability. While many Army ERCIP projects enhance an installation's energy security, projects must strictly meet the language in the FY 2017 National Defense Authorization Act to compete in the energy resilience category: "*enhance mission assurance, support mission critical functions, and address known vulnerabilities*." We look forward to continued congressional support of the ERCIP program in FY 2020.

Third-Party Financing

Energy Savings Performance Contracts (ESPC) and Utility Energy Service Contracts (UESC) utilize third-party financing to fund energy resilience approaches. The Army leverages private sector expertise through ESPCs and UESCs to enhance resilience, and improve efficiency. ESPCs and UESCs allow companies and utilities to provide the initial capital investment to design, implement, and maintain energy and water conservation measures, the cost of which is paid back over the course of the contract. These projects address maintenance backlogs and repair or replace aged and failing equipment using private sector capital repaid from savings realized over the contract term. The Army has the largest ESPC program in the Federal government and the second largest UESC program. Across the board, the Army has awarded more than $2.9B in ESPCs and UESCs to leverage third-party financing, increase resilience, modernize Army infrastructure, and reduce operating costs. Funding from these sources are instrumental in building energy-resilient solutions at Army installations. One example project is the battery energy storage system at Fort Carson, Colorado. This battery energy storage system is the DoD's largest peak-shaving battery storage project, with 8.5 megawatt hours of storage capacity, which will save Fort Carson approximately $500,000 annually on its electric bill. This ESPC project, funded by energy cost savings, reduces peak electric demand and increases the resilience of Fort Carson's grid.

Direct Private Investments

The Army's Office of Energy Initiatives (OEI), within my office, specializes in attracting direct private investment for projects that are privately funded, constructed, owned and operated, and typically sited on land leased from the Army that can also provide an energy resilience benefit back to the Army. The OEI serves as the Army's central program management office for the development, implementation, and oversight of privately financed, large-scale energy projects focused on enhancing energy resilience on Army installations. The OEI portfolio includes 11 already operational projects that deliver 325 megawatts of onsite generation capacity. Further, for the total current projects portfolio, 17 of 21 projects bring some "islandable" capability for critical missions for a minimum of 14 days. This office's efforts have attracted an estimated $627M in direct private capital investment for installations in Georgia, Texas, Alabama, Oklahoma, New York, California, Maryland, and Louisiana among others, to the benefit of the private investors and the Army.

One example of a direct private investment project is located on Schofield Barracks, on the Hawaiian island of Oahu. This energy resilience project is a utility funded, owned

and operated 50 megawatt Multi-Fuel Power Generation Plant, located above the tsunami inundation zone, which provides peaking power capability to the Oahu power grid, to the benefit of the utility's power consumers. In the event of a long-term grid power outage or emergency, the plant is capable of providing the Army's Schofield Barracks, Field Station Kunia, and Wheeler Army Airfield with secure, resilient energy generation for weeks, if necessary. It has been operational since May 2018.
In addition, the Army continues to collaborate with the Department of Defense and the other military services, industry, utility partners, and other Federal agencies, working along with the Department of Energy (DOE) to strengthen our Nation's energy resilience and build a stronger America. In particular, the Army has collaborated with the DOE in evaluating Army energy resilience and to reduce energy costs. The critical topics of the evaluation include: increasing resilience, adopting energy management system standards, and utilization of combined heat and power technologies.

As part of this evaluation, DOE completed a review of Army energy resilience efforts for lessons learned that could be deployed among additional Army installations as well as other Federal agencies. DOE identified energy best practices, key objectives, policy drivers, and ways to improve the alignment between policy drivers and mission-critical capacity metrics. In addition to making recommendations for Army consideration, these inputs were used in development of a DOE comprehensive framework for energy resilience planning and implementation across the Federal government. The evaluation will identify opportunities for energy performance contracting to better include resilience measures. The evaluation began in July of 2018 and will conclude in early 2020.

In addition, DOE and Army worked together to screen 92 Army installations for potential application of combined heat and power systems, and used the results to help inform energy project priorities.

Finally, in collaboration with DOE, Army is piloting the International Organization for Standardization's 50001 energy management system standard, to standardize energy management procedures potentially across 156 Army installations. The benefits of standardization include: persistent energy & cost reductions, improved strategic energy security/resilience planning, and improved preventative maintenance for continuity of operations and readiness.

Planning for Extreme Weather

The 2018 National Defense Authorization Act, Section 335 requires the Department of Defense to conduct specific vulnerability assessments and develop mitigation plans to address the national security threat posed to installations by climate-related threats, including extreme weather events. In response, the Army worked with the U.S. Army Corps of Engineers (USACE) to develop an interactive climate vulnerability assessment tool to evaluate the near-term vulnerability of Army installations, located in the U.S., to six climate-related threats: coastal and riverine flooding, drought, desertification, wildfire, and permafrost thaw. This tool is based on validated climate data from government agencies and will be available to Army installations in early 2020. The intention is to provide installation managers with a method to identify critical climate hazards and incorporate climate resilience measures into their installation master plans.

The Army accounts for potential natural disaster impacts in the site selection stage of project planning and in applying seismic and hurricane criteria during the design phase of each construction project. A good example of such effort is a major modernization project for the Army's Powertrain Facility at Corpus Christi Army Depot in Texas where the project site was changed to an elevation of 25 feet above sea level to protect it from a Category 3 level hurricane storm surge.

Conclusion

Readiness is, and must continue to be, the Army's number one priority. While our attention is on the increasing threats to Army installations and supporting infrastructure, we remain aligned with the Secretary of Defense and the Secretary of the Army's efforts to build, sustain, and ensure warfighting capabilities. As outlined in the National Defense Strategy, Army modernization efforts support our readiness priority, in order to meet current and future threats. Army installations are readiness platforms where our Soldiers live, train, and work. Attaining desired readiness levels requires both a system-wide assessment of current conditions and a modernization effort that seeks to mitigate risk, while setting conditions to meet all threats. The Army's 156 installations must be ready, secure, and capable of deploying and sustaining forces in contested environments, anytime and anywhere the Army may be called upon to fight and win our Nation's wars.

We greatly appreciate the flexible authorities and funding provided by the Congress in FY 2019, and commit to continue being responsible stewards of the resources and responsibilities entrusted to us. On behalf of the Soldiers, Civilians, and Families, I am proud to serve, appreciate the opportunity to present this testimony, and thank you for your continued support of the United States Army.

Mr. Alex A. Beehler
Assistant Secretary of the United States Army (Installations, Energy and Environment)

Mr. Alex A. Beehler was confirmed by the U.S. Senate on Jan. 2, 2019, and sworn in as the 16th assistant secretary of the U.S. Army for Installations, Energy and Environment (ASA(IE&E)) on Jan. 10, 2019.

As ASA (IE&E), he is the primary advisor to the Secretary of the Army and Chief of Staff of the Army for all matters related to Army installation policy and oversight, and coordination of energy security and management. In addition, he is responsible for policy and oversight of sustainability and environmental initiatives; resource management, including design, military construction, operations and maintenance; Base Realignment and Closure (BRAC); privatization of the Army real estate portfolio and installations' Safety and Occupational Health programs.

Mr. Beehler previously served from 2004 to 2009, in the Office of Under Secretary of Defense for Installations and Environment, first as the Assistant Deputy for Environment, Safety and Occupational Health (ESOH), then Principal Deputy, and Acting Deputy Under Secretary. In those capacities, Mr. Beehler served as the principal assistant and advisor for all environmental, safety and occupational health policies and programs in the Department of Defense (DoD). Those programs included cleanup at active and closing bases, compliance with environmental laws, conservation of natural and cultural resources, pollution prevention, environmental technology, fire protection, safety and explosive safety, and pest management and disease control for defense activities worldwide. He also was the first Chief Sustainability Officer (CSO) of the Department of Defense.

Mr. Beehler also has extensive experience in private industry, where he served as a director of environmental and regulatory affairs. Mr. Beehler has maintained a strong background in federal environmental policy, having served in the Department of Justice as a senior trial attorney for environmental enforcement and at the Environmental Protection Agency as a special assistant for legal and enforcement counsel. He also served as staff counsel on the U.S. Senate Judiciary Committee.

Mr. Beehler is a member of the bar of Maryland, Virginia and the District of Columbia. He received a bachelor's degree from Princeton University in public and international affairs and a law degree from University of Virginia.

Mr. Beehler and his wife Stephanie have two adult children.

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

Lucian Niemeyer
Acting Assistant Secretary of the Navy
(Energy, Installations and Environment)
6/26/2019 - Present

On 26 June 2019, the Honorable Lucian Niemeyer assumed duty as the Acting Assistant Secretary of the Navy Energy, Installations and Environment (EI&E). His responsibilities include oversight and policy for Navy and Marine Corps facilities sustainment, restoration and modernization; military construction; acquisition, utilization and disposal of real property and facilities; environmental protection, planning, restoration and natural resources conservation; and safety and occupational health.

In August 2017, he was appointed by the President and confirmed by Congress as the Assistant Secretary of Defense for Energy, Installations, and Environment. In this role, he provided budgetary, policy and management oversight of the Department of Defense's real property portfolio, which encompasses 28 million acres, over 500 installations with over 500,000 buildings and structures valued at a trillion dollars. Upon successful integration of the EI&E portfolio into the newly created Sustainment portfolio, Secretary Niemeyer served the Under Secretary of Defense for Acquisition and Sustainment as a Strategic Advisor. His specific focus was on Defense energy resilience and cybersecurity programs responsible for enhancing the Department's planning, programs, and military capabilities to provide mission assurance through installation and operational energy and cybersecurity resilience policy development, and execution of initiatives for domestic and overseas installations.

Prior to his appointment, Secretary Niemeyer worked in the private sector from 2014 to 2017 as the founder of The Niemeyer Group, LLC. From 2003 to 2014 he served on the professional staff of the United States Senate Committee on Armed Services where he was responsible for a wide portfolio of national security programs, including military installations, ranges, world-wide basing, energy programs, facility privatization initiatives, military budgets, unit readiness, industrial base, and environmental issues. He also provided oversight for military logistics and sustainment programs as well as Air Force and Navy acquisition programs.

Secretary Niemeyer is an Air Force veteran, retiring in 2008 at the rank of Lieutenant Colonel with 15 years of active and five years of Virginia Air National Guard service working within the installation engineering and military plans community. He holds a Bachelor of Architecture, from the University of Notre Dame, a Master of Business Administration from The George Washington University, and a Master of National Security and Strategic Studies from the Naval War College.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

October 16, 2019

QUESTIONS SUBMITTED BY MS. STEFANIK

Ms. STEFANIK. Who is responsible for defending ICS/SCADA systems? How much (if any) of this is a contractor work force?

Secretary MCMAHON. The Deputy Secretary of Defense designated the DOD CIO as the official responsible for the cybersecurity of industrial control systems for the DOD. Subsequently, in a December 2018 memo, the DOD CIO delineated responsibilities to the DOD Components to implement cybersecurity requirements for control systems. The policy memo also clarifies that DOD cybersecurity requirements are applicable to all DOD control systems. In addition, the Department is developing enhanced cybersecurity implementation guidance for control systems. Operationally, U.S. Cyber Command and JFHQ–DODIN have a critical role in defending all DOD systems including ICS/SCADA systems, however it is the system owners and operators that are ultimately responsible for the safety and security of their systems. The contractor workforce is not differentiated from the overall cyber workforce comprised of government civilians, military personnel, and contractors. Currently, ICS/SCADA systems owners and operators are not included in the cyber workforce requirements. Integrating ICS/SCADA competencies in the forthcoming update to the DOD cyber workforce policy (DOD Issuance 8140) will enable those distinctions.

Ms. STEFANIK. What coordination takes place with cyber defensive teams? Are your service cyber forces familiar enough with local ICS/SCADA to assist?

Secretary MCMAHON. The DOD CIO ensures Cyber Mission Forces and cyber protection teams are establishing the processes to work collaboratively with local facilities managers and other stakeholders to provide assessments and mitigations of mission relevant ICS/SCADA systems and networks. Steady progress is being tracked by the Components with a focus on the most critical mission relevant systems being assessed through FY20. As the expertise of these teams grows and the processes are optimized, DOD is confident the proper coordination and collaboration will occur at the installation-level.

Ms. STEFANIK. Are ICS/SCADA systems subject to the same security and accreditation standards as DOD networks are? Or are there differences with these so-called "operational systems"?

Secretary MCMAHON. Yes, the DOD requires all DOD systems and technology, including ICS/SCADA systems, must have cybersecurity applied IAW existing policy as described in DODI 8500.01, Cybersecurity and follow authorization processes as described in the DODI 8510.01, Risk Management Framework for DOD IT. The DOD does not differentiate cybersecurity policy requirements by system type, rather, the policies apply to all and are inclusive of varied cybersecurity implementation risk-based approaches to different system and technology types.

Ms. STEFANIK. Similar to our supply chain concerns with Huawei components being in critical defense systems, do we have any concerns with foreign components being used within ICS/SCADA hardware? Is this something you have surveyed or considered? How are you mitigating this concern?

Secretary MCMAHON. Yes, the DOD is concerned about the supply chain associated with ICS/SCADA hardware. Compared to information technology, ICS supply chains are challenged by the inherent lack of security, limited monitoring, and constrained vendor support (often the original equipment manufacturer) for these products. To address these concerns, the OUSD (Acquisition) Chief Information Security Officer has taken a number of steps to reduce the vulnerabilities and impacts of compromised devices and components. The DOD has adopted the NIST SP 800–161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations and is working with the Defense Industrial Base, suppliers, vendors, and other organizations such as the International Society of Automation to ensure that supply chain risk management processes are implemented. In addition, the U.S. Army Combat Capabilities Development Command—Aviation & Missile Center (DEVCOM) is developing a Tested Products List for Control Systems certification process for the DOD. This process will allow vendors/products to go through cybersecurity testing and enable Type Authorization (test once and use many times) at lower cost in less time.

Ms. STEFANIK. One of the other focus areas for the IETC subcommittee is science and technology, which is a community that for decades has leveraged advances in modeling and simulation and other technologies to understand complex and unpredictable problems. With respect to climate change and extreme weather events—how are you working with the DOD S&T community and academia to understand and prepare for extreme weather events, to include modeling and simulation and other technologies that could help and develop and enhance resiliency for installations and infrastructure?

Secretary MCMAHON. OASD(S) works closely with OUSD(R&E) as well as the Military Departments, academia, and the broader research and engineering community through communication and coordination, technology development and implementation, and research. Communication and coordination is evidenced in many ways. OASD(S) supports OUSD(R&E) as DOD's principal agency representative to the U.S. Global Climate Change Research Program (USGCRP), Subcommittee on Global Change Research (SGCR) and their leadership of DOD's work within the Earth System Prediction Capability interagency coordination activity. OASD(S) supports technology development and implementation with a focus of understanding and preparing for extreme weather events. For example, we are supporting the development of a web-based assessment tool to provide better insight into DOD's exposure to extreme weather and climate impacts. This tool is a text book example of how critically important modeling and simulation technologies developed by other agencies, academia, and the DOD S&T community is used to prepare for extreme weather events and climate change. DOD's Strategic Environmental Research and Development Program (SERDP) and Environmental Security Technology Certification Program (ESTCP) programs harness the latest science and technology to improve DOD's environmental performance, reduce costs, and enhance and sustain mission capabilities. SERDP and ESTCP support research collaboration in academia, industry, the Military Departments, and other Federal agencies. For example, SERDP leadership, in conjunction with the National Oceanic and Atmospheric Administration (NOAA), the U.S. Army Corps of Engineers (USACE), U.S. Geological Survey (USGS), numerous universities and others, resulted in the development of DOD's Regional Sea Level (DRSL) database for projected sea level rise at all coastal installations, a key tool for understanding coastal sea level rise.

Ms. STEFANIK. How are you preparing for emerging technologies such as 5G and what will be an exponential increase in IOT devices? In 2017 we saw some 8.4 billion devices connected to the internet—but by 2020 it is estimated that we may see up to 75 billion connected devices, depending on what estimate you use. This presents tremendous opportunity but also significant challenges. Can you outline how you are thinking about 5G and this massive increase of IOT?

Secretary MCMAHON. The DOD CIO continuously assesses new technology types against existing policies to identify areas where additional policy or implementation guidance may be required. The DOD reviewed and assessed existing cybersecurity, operations security, physical security, and information security policies for guidance on Internet Of Things (IOT) devices. While IOT is not directly mentioned, the Department has found existing policies to be sufficient to address IOT security requirements. From a cybersecurity perspective, all IOT must have DOD cybersecurity applied IAW existing policy as described in DODI 8500.01, Cybersecurity.

Ms. STEFANIK. If there was a crippling cyber-attack on one of our major installations that took down critical infrastructure such as power, or disabled ICS/SCADA systems, can you walk us through how a military installation would handle such an incident? What responsibilities are within your portfolios, as compared to and coordinated with CYBER COMMAND, and those that are providing Service Mission Defense Teams, for example?

Secretary MCMAHON. As ASD(S), I oversee the cyber security of DOD facility-related control systems and the resilience of enduring installations to energy disruptions. My office established the requirement for the Services to develop installation energy plans and supporting cyber security plans to identify critical energy requirements, assess vulnerabilities, take action to mitigate risks, and conduct sustained maintenance and testing of these systems over time. OASD(S) provides policy and governance to enable energy resilience at enduring installations, ensures that cyber security and energy resilience are integrated into third party financed energy improvements, and funds military construction projects that improve energy resilience and contribute to mission assurance through the Energy Resilience and Conservation Investment Program. Likewise, the Department is implementing a series of Energy Resilience and Readiness exercises that use "black start" scenarios to test and evaluate energy systems at our installations. Each of these efforts supports the capability of the Services to carry out critical missions in spite of energy disruptions or cyber-attacks. Cyber defense best practices includes two methods of defending control systems. First, there is a logical separation of networks that limit communications between information technology and operational technology networks with very few exceptions. Secondly, asset owners maintain a manual method of operation that does not require the use of a network to maintain operation. Should an attack occur, the on-site maintenance and operational personnel would take the respective system off line and manually operate the system. In the event of a power outage, mission owners would immediately turn to backup power options (e.g., on-site generator, on-site distributed energy resources, and uninterruptible power sources) to sustain critical missions over the short-term. Based on assigned mission assurance responsibilities, Combatant Command and OUSD(Policy) would begin coordinating with any non-DOD power providers regarding the timely restoration of power to the installations. Depending on the duration of the energy disruption, Services and Combatant Commands also would consider transitioning to continuity of operations posture and/or transitioning affected missions to other locations. Cyber Command activities are outside the purview of this office. As such, any questions referring to Cyber Command responsibilities should be redirected to that office.

Ms. STEFANIK. What if—instead of an attack on ICS/SCADA or electricity—we had an attack on the entire Military Electronic Health Records System that prevented our military health care installations and systems from functioning—similar to the WannaCry attack that crippled the U.K.'s National Health Service? Do we have incident response plans in effect to deal with these types of cyber incidents that could impact our installations?

Secretary MCMAHON. The Defense Health Agency (DHA) has implemented significant cyber protections both at an enterprise level and at the local unit level that mitigates the risks from WannaCry and any other cyber exploit. In fact, DHA's military electronic health record system program vendor, Cerner Corporation, was responsible for providing the first copy of the WannaCry software code in America to both the Federal Bureau of Investigation and the Department of Defense (DOD). As part of standard DOD policies and procedures established for security accreditation, incident response plans are required for Authority To Operate (ATO) certification and are independently evaluated by the accreditation authority. MHS GENESIS, the new electronic health record for the Military Health System, was implemented with a defense-in-depth strategy. The first layer of defense is the protected network called the Medical Community of Interest (MEDCOI). At the enterprise-level, MEDCOI separates health- related network traffic from all DOD network and internet traffic that is also monitored by Cyber Security Service Provider. MHS GENESIS has a full suite of active and passive cyber measures to predict, identify, and isolate threats. Furthermore, MHS GENESIS is building a continuity-of-operations and disaster recovery (COOP&DR) solution that will restore mission critical capabilities to end users within 4 hours of a declared disaster event. This solution will be in place September 2020. This multi-tiered defense-in-depth strategy provides MHS GENESIS with state-of-the-art protection measures ensuring the delivery of capability to the Defense Health Community and the Veterans Administration even in the face of a catastrophic event. Each Military Treatment Facility is also architected with a suite of cyber defenses customized to the unique requirements of that facility. In the current state, each facility operates under their service specific legacy downtime procedures moving to paper when the electronic systems are not available. DHA's Health Informatics Division is developing a standardized enterprise wide downtime procedure to include scheduled downtime, unscheduled downtime, and recovery.

Ms. STEFANIK. Who is responsible for defending ICS/SCADA systems? How much (if any) of this is a contractor work force?

Secretary BEEHLER. The Army has multiple stakeholders responsible for defending ICS/SCADA systems. Army Chief Information Officer/G–6 is responsible for establishing cybersecurity policies. Those policies are implemented by mission and asset owners and enforced by authorizing officials that approve and allow the use of the systems, and are required to align the systems to a Cybersecurity Service Provider (CSSP). Army Cyber Command (ARCYBER) is responsible for CSSP services, to include defensive cyber operations—internal defensive measures (DCO–IDM). ARCYBER has delegated some CSSP authority to certain commands, such as U.S. Army Corps of Engineers (USACE) and United States Army Space and Missile Defense Command (USASMDC) to provide CSSP for their portion of the Army network under the purview of ARCYBER. On 4 October 2019, the Director of the Army Staff designated U.S. Army Chief of Engineers to develop a program managed structure that covers procurement, configuration, cybersecurity, testing, and lifecycle for ICS. The Army has not conducted a full inventory of ICS/SCADA hardware, hence it is not possible to determine how much of the Army ICS/SCADA systems are defended by contractors. Based on the completed NDAA § 1650 assessments, the Army does not have the internal resources (trained manpower/equipment/money) to properly defend existing ICS/SCADA systems.

Ms. STEFANIK. What coordination takes place with cyber defensive teams? Are your service cyber forces familiar enough with local ICS/SCADA to assist?

Secretary BEEHLER. Coordination to defend resources between elements of the Army cyber defense community is an on-going activity. The proliferation of types of devices and wide range in age of devices supporting Army infrastructure makes developing expertise in all areas challenging. The Army is developing a greater familiarity with local ICS/SCADA systems. For ICS/SCADA systems currently connected to networks, the Army has expertise in assessments.

Ms. STEFANIK. Are ICS/SCADA systems subject to the same security and accreditation standards as DOD networks are? Or are there differences with these so-called "operational systems"?

Secretary BEEHLER. Yes, ICS/SCADA control systems must follow the same Department of Defense (DOD) security and accreditation standards as DOD networks.

Ms. STEFANIK. Similar to our supply chain concerns with Huawei components being in critical defense systems, do we have any concerns with foreign components being used within ICS/SCADA hardware? Is this something you have surveyed or considered? How are you mitigating this concern?

Secretary BEEHLER. The Army shares concerns about supply chain security across all our data systems. These concerns are larger than any single supplier (such as Huawei) or even solely suppliers with foreign origins. We must ensure that our systems, regardless of origin, are effective for their purpose, including being cyber secure. The Army has entered into an enterprise-wide effort to survey/inventory and assess the installations to better bound what control systems we have on our installations, how they are connected, and how they are constructed/serviced so that we can assess risk. The Army is already implementing measures to mitigate risk; from implementing Unified Facility Criteria and Specifications used to incorporate cybersecurity measures across the infrastructure lifecycle, ensuring that control systems are assessed and authorized using the DOD Risk Management Framework (RMF), and ensuring a continuous cybersecurity monitoring strategy is in place to ensure vulnerabilities are identified and remediated.

Ms. STEFANIK. One of the other focus areas for the IETC subcommittee is science and technology, which is a community that for decades has leveraged advances in modeling and simulation and other technologies to understand complex and unpredictable problems. With respect to climate change and extreme weather events—how are you working with the DOD S&T community and academia to understand and prepare for extreme weather events, to include modeling and simulation and other technologies that could help and develop and enhance resiliency for installations and infrastructure?

Secretary BEEHLER. The Army Climate Assessment Tool, developed with the U.S. Army Corps of Engineers, incorporates the latest actionable science data and model results from the scientific community regarding climate change and extreme weather. The sources of this data include the U.S. Geological Survey (USGS), National Atmospheric and Oceanic Administration (NOAA), Federal Emergency Management Agency (FEMA), the Fourth National Climate Assessment volumes released by the U.S. Global Change Research Program, and the DOD's Strategic Environmental Research and Development Program (SERDP), which itself includes interagency and academic experts. Additional information derives from peer-reviewed scientific literature, including work sponsored in part by the U.S. Army Corps of Engineers. The tool uses this data to indicate exposure of select locations to coastal and riverine flooding, drought, desertification, wildfire, and thawing permafrost. Observed historical data regarding hurricane and tornado intensity and location is also incorporated into the tool. This information provides a screening-level assessment of the exposure of Army locations to extreme weather and changing climate, allowing prioritization of more detailed studies to reduce vulnerability and enhance resilience to these impacts. Installation managers will use the information provided by this tool inform master planning and to identify ways to improve the resilience of their installations to extreme weather events and other climate-related threats.

Ms. STEFANIK. How are you preparing for emerging technologies such as 5G and what will be an exponential increase in IOT devices? In 2017 we saw some 8.4 billion devices connected to the internet—but by 2020 it is estimated that we may see up to 75 billion connected devices, depending on what estimate you use. This presents tremendous opportunity but also significant challenges. Can you outline how you are thinking about 5G and this massive increase of IOT?

Secretary BEEHLER. There are three steps the Army is taking to prepare for the integration of emerging technologies: assessing the current state of installation information technology (IT), developing a cyber supply chain risk management governance structure to mitigate cybersecurity risks to ensure warfighter and installation security and readiness, and leveraging new technologies to increase readiness. As part of the Army's holistic modernization efforts, the Army is working with DOD to conduct 5G experiments at DOD facilities. Each Service nominated, and DOD approved one location, each as the first experimentation site in FY20. The Army recommended Joint Base Lewis-McChord (JBLM), WA. JBLM was nominated asthe first site based on the potential to prove out technology in multiple-use case areas, alignment to Army modernization priorities as well as JBLM being the site for the Army's existing Multi-Domain Task Force, a National Guard and Reserve force generation site, a future synthetic training environment location and a Joint Base. DOD secured $52M in FY19 to support initial 5G efforts and intends to release an initial Request for Proposal (RFP) in November 2019 and allow industry to provide feedback and then release the final RFP in early December. The additional selection of sites and broader experimentation are subject to funding and continuing resolution. As part of DOD's established Scoping and Mitigation program to scrutinize Supply Chain vendors using the U.S. Code § 2339A review process (FY19 NDAA, Section 889), the Army is developing a Supply Chain Risk Management governance structure. The Army is also conducting supply chain analysis leveraging public data research combined with advanced analytics to address national-level requirements in support of FY16 NDAA, Section 1647, and FY17 NDAA, Section 1650. As the number of IT devices increases, the scrutiny of the cyber supply chain will assist in securing our warfighters and installations. To prepare for future conflicts, the Army is also ensuring Soldiers are ready and armed with the latest technology. The driving force behind this modernization effort is U.S. Army Futures Command (AFC) in conjunction with Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)), created to streamline modernization efforts and field new equipment and capabilities more quickly to Soldiers. Additionally, the Army is leveraging previously granted authorities like Other Transactional Authority agreements (OTA's) to tap into innovation from nontraditional suppliers of commercial technology for research and prototyping.

Ms. STEFANIK. If there was a crippling cyber-attack on one of our major installations that took down critical infrastructure such as power, or disabled ICS/SCADA systems, can you walk us through how a military installation would handle such an incident? What responsibilities are within your portfolios, as compared to and coordinated with CYBER COMMAND, and those that are providing Service Mission Defense Teams, for example?

Secretary BEEHLER. Regardless of the cause of an outage event, cyber, or other, Army installations have robust planning in place to ensure continuity of critical operations. Each installation has a specific emergency response plan and all critical missions have continuity of operations plans to ensure mission effectiveness throughout the duration of an event and for priority restoration of services to recover from an event. From an energy and water perspective, Army Directive 2017–07 sets the requirement for Army installations to secure critical missions by being capable of withstanding an extended utility outage of 14 days. This includes timeframes to accomplish, curtail, or relocate the critical mission(s), as needed. The Army is also taking proactive measures to test our ability to withstand a long-duration outage. Through the Army protection program, installations regularly conduct integrated protection exercises related to Defense and Army critical infrastructure. Army installations are also required to complete full-scale and routine testing of emergency and standby energy generation systems that support their critical energy requirements. Select installations have further tested their systems by completing Energy Resilience Readiness Exercises that simultaneously disconnect the entire installation (or a subset) from utility power in a controlled environment to test system backups and validate installation backup and restoration procedures. Installation Department of Public Works (DPW) personnel work closely with Army Cyber Command personnel to respond and recover from cyber-attacks. A critical part of this team effort is the use of the Advanced Cyber Industrial Control Systems (ICS) Tactics, Techniques, and Procedures (TTP) to guide Army response. The ACI TTP provides procedures that enable ICS managers and network managers to detect cyber-attacks, mitigate the effects of those attacks, and recover their networks following an attack. The primary goal during a cyber-attack is to retain operations of the critical infrastructure priorities (e.g., electric, water, etc.).

Ms. STEFANIK. What if—instead of an attack on ICS/SCADA or electricity—we had an attack on the entire Military Electronic Health Records System that prevented our military health care installations and systems from functioning—similar to the WannaCry attack that crippled the U.K.'s National Health Service? Do we have incident response plans in effect to deal with these types of cyber incidents that could impact our installations?

Secretary BEEHLER. Incident response plans and Continuity of Operations (COOP) plans are in place and practiced throughout the Medical Treatment Facilities (MTF) and these are inspected by the Services and Joint Commission (JC). The WannaCry virus exploited unpatched systems, and is a reason why DOD is focused on making sure computers are all patched with the latest software from vendors today. The Military Electronic Health Records enterprise is currently comprised of multiple systems that include but are not limited to Armed Forces Health Longitudinal Technology Application, Composite Health Care System, and Essentris and is actively migrating to Military Health System GENESIS, the new DOD Electronic Health Record. Each of these systems are architected in a different fashion and has internal security built into the systems; they also sit in a Defense in Depth posture (isolated Virtual Local Area Networks (VLANS)) as well as perimeter security. With the incident response and COOP plans in place, the MTFs are still able to provide health care. They would document the care on paper versus in the electronic health record. The concern is depending on the length of "down time" that may affect access to previous data to facilitate the care.

Ms. STEFANIK. Who is responsible for defending ICS/SCADA systems? How much (if any) of this is a contractor work force?

Secretary HENDERSON. Sixteenth Air Force (16 AF) is responsible for defending all Air Force Information Networks (AFIN), of which ICS/SCADA is a portion. The 16 AF defense work force is primarily comprised of government personnel (military & civilian), with a few contractors in various units.

Ms. STEFANIK. What coordination takes place with cyber defensive teams? Are your service cyber forces familiar enough with local ICS/SCADA to assist?

Secretary HENDERSON. Should an ICS/SCADA-impacting cyber attack occur, the Air Force has seven service-reallocated Cyber Protection Teams which it can direct to respond. Those teams can leverage greater USCYBERCOM resources if warranted. Air Force defensive teams are trained and equipped to respond to a broad range of cyber activity, and will apply that training to any area of need. Additionally, they are expected to be familiar with any cyber terrain on which their supported missions rely, including AF-owned and civilian ICS/SCADA.

Ms. STEFANIK. Are ICS/SCADA systems subject to the same security and accreditation standards as DOD networks are? Or are there differences with these so-called "operational systems"?

Secretary HENDERSON. The "security and accreditation" is accomplished in accordance with DODI 8510.10 and implemented by AFI 17–101 RISK MANAGEMENT FRAMEWORK (RMF) FOR AIR FORCE INFORMATION TECHNOLOGY (IT) to address both traditional IT and control systems using tailored security protocols based on their applicability to the system.

Ms. STEFANIK. Similar to our supply chain concerns with Huawei components being in critical defense systems, do we have any concerns with foreign components being used within ICS/SCADA hardware? Is this something you have surveyed or considered? How are you mitigating this concern?

Secretary HENDERSON. The integrity and supply chain risk of foreign components in ICS/SCADA systems is of concern, especially where these systems directly support Defense Critical Infrastructure and Defense Critical Missions. Supply chain risk management is a consideration in the Air Force control systems cybersecurity strategy that is in development. An element of the strategy is to evolve our acquisition processes to reduce the risk of cyber vulnerabilities in ICS/SCADA systems. To mitigate the concern in currently-fielded hardware, we are working towards more advanced network hardening, monitoring and defensive cyber operations.

Ms. STEFANIK. One of the other focus areas for the IETC subcommittee is science and technology, which is a community that for decades has leveraged advances in modeling and simulation and other technologies to understand complex and unpredictable problems. With respect to climate change and extreme weather events—how are you working with the DOD S&T community and academia to understand and prepare for extreme weather events, to include modeling and simulation and other technologies that could help and develop and enhance resiliency for installations and infrastructure?

Secretary HENDERSON. We work with DOD, federal, and academic entities to understand and enhance installation resilience and share the following examples. The DOD's Strategic Environmental Research and Development Program (SERDP) led the development of the Regionalized Sea Level Change Scenarios and Extreme Water Level Statistics database, a valuable resource for localized sea level rise scenarios and historical storm surge statistics. As noted in the Report on Effects of a Changing Climate to the Department of Defense (Jan 2019), SERDP and DOD's Environmental Security Technology Certification Program (ESTCP) investments support the development of the science, technology, and methods needed to manage and enhance resilience. The Report outlines efforts by SERDP, ESTCP, and the Lawrence Berkeley National Laboratory on understanding sea level rise, drought, wildfire risk, and permafrost degradation. We are working with the Colorado State University Center for Environmental Management of Military Lands to improve floodplain delineation and explore the potential sea level rise, storm surge, and changes in temperature and precipitation patterns on 60+ Air Force sites across the world. The intent is identification of potential vulnerabilities and possible adaptation strategies to feed into our installation Integrated Natural Resource Management Plans. In the future, we hope to use this information to inform siting and planning applications. Working with the University of Alaska—Anchorage we are pursuing more accurate Alaska shoreline erosion prediction models that take into account warming water near the shore, increasing air temperatures, longer periods when sea ice is gone, increasing spatial extent of open water, increasing wind speeds, storm surges, wave height, and thawing of permafrost. We rely on the USACE Cold Regions Research and Engineering Laboratory (CCREL) expertise for its work on construction techniques in permafrost regions. We are also partnering with ASD(S) and the Massachusetts Institute of Technology Lincoln Lab to develop a "pull-the-plug" exercise framework to baseline capabilities and identify vulnerabilities. We will continue to collaborate across the DOD, federal, and academic S&T communities to enhance our installation and mission resilience.

Ms. STEFANIK. How are you preparing for emerging technologies such as 5G and what will be an exponential increase in IOT devices? In 2017 we saw some 8.4 billion devices connected to the internet—but by 2020 it is estimated that we may see up to 75 billion connected devices, depending on what estimate you use. This presents tremendous opportunity but also significant challenges. Can you outline how you are thinking about 5G and this massive increase of IOT?

Secretary HENDERSON. The Air Force is aware of the potential and promise of 5G and is pursuing opportunities to address gaps in coverage. The Air Force will continue to pursue ways to leverage 5G to drive a resilient warfighting communications architecture to promote our multi-domain command and control capabilities to preserve the Joint Force's and the Air Force's competitive advantage in today's strategic environment. The Air Force streamlined the process to grant leases for commercial broadband. Currently, ten bases in the Southeast have leases pending that will enable small node, whole-base commercial broadband coverage. The next leasing opportunity will be for 17 bases in the Northwest region later this calendar year. In addition to this, the AF is participating in DOD's 5G experiments to evaluate various 5G capabilities such as smart depots, shared spectrum and mission planning that will assess various 5G configurations for optimal mission usage.

Ms. STEFANIK. If there was a crippling cyber-attack on one of our major installations that took down critical infrastructure such as power, or disabled ICS/SCADA systems, can you walk us through how a military installation would handle such an incident? What responsibilities are within your portfolios, as compared to and coordinated with CYBER COMMAND, and those that are providing Service Mission Defense Teams, for example?

Secretary HENDERSON. During their initial response, Civil Engineering Squadron (CES) operators or support contractors could identify malicious cyber activity and trigger the appropriate response in partnership with a local Mission Defense Team (MDT), if applicable. That response would include notifying the 624th Operations Center at 16th Air Force, which would coordinate further response actions with CYBERCOM, including the deployment of a service-reallocated Cyber Protection Team (CPT) if warranted. The CPT would partner with the MDT to optimally understand the affected terrain and respond to the malicious activity.

Ms. STEFANIK. What if—instead of an attack on ICS/SCADA or electricity—we had an attack on the entire Military Electronic Health Records System that prevented our military health care installations and systems from functioning—similar to the WannaCry attack that crippled the U.K.'s National Health Service? Do we have incident response plans in effect to deal with these types of cyber incidents that could impact our installations?

Secretary HENDERSON. Any questions specific to enterprise system recovery or redundancy would have to be answered by the Defense Health Agency or Program Executive Office Defense Health Modernization System. The answer below pertains to the local military treatment center actions. Each military treatment facility has contingency response plans for how to operate should the electronic health record be unavailable. These plans typically include paper-based processes for documenting care. There is often a reliance on civilian pharmacy networks to fill routine non-urgent medications during an outage, should a patient not be able to wait until the system is restored. For a prolonged outage, elective care may be delayed or deferred. Much of the Military Health System's clinical data is shared with the Department of Veterans Affairs (Joint Legacy Viewer) through health information exchanges, or replicated in various data warehouses (Carepoint, Medical Data Repository, etc). In a prolonged outage these data sources may become alternative means to access clinical information to support continued operations. Most routine acute care can continue simply by collecting background information from the patient at the time of care (normal clinical practice). Local recovery operations will require care documented on paper or other means to be entered into the electronic health record once it becomes available. This is commonly accomplished via scanning of paper documentation into the record. In a small number of cases, specific data elements may have to be transcribed into the record as part of the recovery.

Ms. STEFANIK. Who is responsible for defending ICS/SCADA systems? How much (if any) of this is a contractor work force?

Mr. NIEMEYER. The responsibility for cyber defense of Navy ICS/SCADA resides with the local system owners at the installations. System owners work closely with Naval Facilities Engineering Command (NAVFAC) who is the cybersecurity technical authority for these systems. Leveraging a workforce of about 40% contractor and 60% Government (military and civilian) worldwide.

Answer (MCICOM): The responsibility for defensive cyber operations of ICS/ SCADA systems is Marine Corps Forces Cyberspace Command (MARFORCYBER) and its subordinate command, the Marine Corps Cyber Operations Group (MCCOG). MARFORCYBER is responsible for the overall security, operations, and defense of the Marine Corps Enterprise Network. MCCOG performs those duties as the Cyber Security Service Provider (CSSP) for the Marine Corps.

Ms. STEFANIK. What coordination takes place with cyber defensive teams? Are your service cyber forces familiar enough with local ICS/SCADA to assist?

Mr. NIEMEYER. Within the Navy, Naval Facilities Engineering Command (NAVFAC) regularly coordinates with Navy Cyber Defense Operations Command (NCDOC) and their higher headquarters, Navy Fleet Cyber Command (FCC). The Navy's Service Defense Teams are aware of U.S. Cyber Command tactics, techniques, and procedures (TTP) for ICS/SCADA cybersecurity. They regularly receive updates of the latest control systems cybersecurity including the development of technological advances and procedures.

Answer (MCICOM): Within the Marine Corps coordination between cyber defensive teams, the local IT and the local ICS/SCADA operators currently occurs on an ad-hoc basis. This is absent the adoption of an Enterprise Architecture which can provide visibility of the local FRCS networks to a dedicated Cyber Security Service Provider (CSSP) network operations center, similar to those that exist for the Marine Corps Enterprise Network (MCEN). Cyber forces are engaged at the stakeholder level in the developing of this Enterprise Architecture and aware of the need to standup expertise for ICS/SCADA. The service cyber forces have a very limited familiarity with ICS/SCADA systems, and training for cyber forces on ICS/SCADA is not formalized. Marine Corps Forces Cyberspace Command (MARFORCYBER) as the responsible party for cybersecurity and Marine Corps Installations Command (MCICOM) as the responsible party for the operation of ICS/SCADA are aware of this gap and are actively working to address it.

Ms. STEFANIK. Are ICS/SCADA systems subject to the same security and accreditation standards as DOD networks are? Or are there differences with these so-called "operational systems"?

Mr. NIEMEYER. Yes, DON ICS/SCADA systems are subject to the same DOD Risk Management Framework and security and accreditation standards used for information technology systems and networks. Differences for ICS and SCADA are addressed in NIST Special Publication 800–82 Revision 2: Guide to Industrial Control Systems (ICS) Security.

Ms. STEFANIK. Similar to our supply chain concerns with Huawei components being in critical defense systems, do we have any concerns with foreign components being used within ICS/SCADA hardware? Is this something you have surveyed or considered? How are you mitigating this concern?

Mr. NIEMEYER. The Department of Navy shares concerns about supply chain security across our industrial control systems. Foreign components being used within ICS/SCADA pose a significant concern to mission critical and essential operational facilities worldwide. To survey and mitigate this risk, the DON leverages our Navy and Marine Corps Mission Assurance Assessment programs to assess the function and resilience of ICS/SCADA systems critical to the performance of DOD Mission Essential Functions across the supply chain. To mitigate risk in acquisitions, we utilize Defense Federal Acquisition Regulations (DFAR) clauses in our contracts. When assessments and monitoring determine an elevated risk, we use immediate remediation techniques and technical solutions such as disconnecting those systems from the internet. To improve our understanding of the issue and maintain continuous awareness of the cyber battle space, we are developing infrastructure and governance processes to continuously monitor our critical ICS/SCADA systems worldwide.

Ms. STEFANIK. One of the other focus areas for the IETC subcommittee is science and technology, which is a community that for decades has leveraged advances in modeling and simulation and other technologies to understand complex and unpredictable problems. With respect to climate change and extreme weather events—how are you working with the DOD S&T community and academia to understand and prepare for extreme weather events, to include modeling and simulation and other technologies that could help and develop and enhance resiliency for installations and infrastructure?

Mr. NIEMEYER. The DON actively participates with in the DOD's Strategic Environmental Research Development Program (SERDP) and Environmental Security Technology Certification Program (ESTCP) in partnership with DOE, EPA, and academia in the development of research and resulting projects focused on "Resource Conservation and Resiliency" which includes evaluating climate and weather. The DON incorporates climate resilience as a crosscutting consideration for our planning and decisions making process. As an example the DON is closely working with DOD to leverage the U.S. Army Corps of Engineers climate exposure tool to analyze climate impacts and natural hazards at 60 DON locations (50 sites CONUS and 10 OCONUS), which is planned to be complete by September 2020.

Ms. STEFANIK. How are you preparing for emerging technologies such as 5G and what will be an exponential increase in IOT devices? In 2017 we saw some 8.4 billion devices connected to the internet—but by 2020 it is estimated that we may see up to 75 billion connected devices, depending on what estimate you use. This presents tremendous opportunity but also significant challenges. Can you outline how you are thinking about 5G and this massive increase of IOT?

Mr. NIEMEYER. DON and DOD are collaborating as part of a U.S. "Whole of Government" approach to foster 5G innovations and mitigate security risks. We are working with universities and commercial vendors (5G infrastructure and handsets) on efforts related to 5G. Additionally, the Department of Navy is participating in the 5G study with OUSD R&E to test 5G applications on our installations. These pilots will enable the evaluation of 5G cyber security risks in addition to new attack surfaces that 5G may expose given the wider network connectivity (e.g., Internet of Things). Navy continues to make significant progress and investments in "trusted" HW/SW/networking for C2 and combat systems and these solutions are applicable to 5G. One example is Network Slicing technology used by the DON to create multiple logical networks with different performance characteristics overlaid on a single physical network enabling data segregations and slice specific security solutions. Slicing is not unique to 5G networks but will be an enabler in increasing the security of 5G. If DOD employs IOT devices on our installations to create a smart port or smart depot, we can use slicing to create partitioned networks for isolating the IOT devices from the main enterprise network. Additionally, OUSD (R&E) is pursuing measures to add greater protection and resiliency to a network that is using slices. We are directly taking on the security risks posed by installed equipment manufactured from untrusted companies, by publishing guidance by January 2020 for use by installation commanders when considering the development of 5G infrastructure on bases and ranges. We are also working with States and local communities on the establishment of security requirements through state legislation within permitting processes to ensure 5G networks around bases and ranges do not pose a security risk to critical DON missions. Our goal is to ensure the military value of bases in the future are rewarded by the development of a secure 5G network.

Ms. STEFANIK. If there was a crippling cyber-attack on one of our major installations that took down critical infrastructure such as power, or disabled ICS/SCADA systems, can you walk us through how a military installation would handle such an incident? What responsibilities are within your portfolios, as compared to and coordinated with CYBER COMMAND, and those that are providing Service Mission Defense Teams, for example?

Mr. NIEMEYER. When personnel with DOD information network (DODIN) security responsibilities detect compromise of cyberspace security measures, they transition, in accordance with standing authorities delegated by the commander, to the cyberspace defense actions of Defensive Cyberspace Operations-Internal Defensive Measures to restore security to their assigned portion of the DODIN. Their effectiveness in making this transition depends upon their level of training and resources to detect and respond to threats. If discovery and mitigation of malicious cyberspace activity requires expertise beyond that available to the network operator and/or the ISP, the cyberspace protection teams (CPTs) may respond to provide support conducting cyberspace defense actions, either remotely or by deploying to the affected location. CPTs perform other tasks to support network operators, including penetration testing, security surveys, and assessment. National-level CPT support can be extended to defend non-DOD mission partner or critical infrastructure networks when ordered by Secretary of Defense.

Ms. STEFANIK. What if—instead of an attack on ICS/SCADA or electricity—we had an attack on the entire Military Electronic Health Records System that prevented our military health care installations and systems from functioning—similar to the WannaCry attack that crippled the U.K.'s National Health Service? Do we have incident response plans in effect to deal with these types of cyber incidents that could impact our installations?

Mr. NIEMEYER. To ensure warfighters and decision makers have access to information systems and data after a disruption, DOD Instruction 8500.01 requires that DOD Component heads develop Information Systems Contingency Plans (ISCPs) and conduct testing to recover information system services following an emergency or other disruption. An ISCP is the coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. In the Department of Navy, System Owners/Program Managers are responsible for having an operational ISCP as a part of their accreditation approval by the Navy or Marine Corps Authorizing Official.

QUESTIONS SUBMITTED BY MR. BROOKS

Mr. BROOKS. In July of 2015, the Government Accountability Office issued a report (GAO–15–749) that stated, "as of February 2015, none of the military services had a complete inventory of existing Industrial Control Systems." It's been four years since that report was issued. Does the Office of the Assistant Secretary of Defense for Sustainment (OASD(S)) have a complete inventory of existing Industrial Control Systems on all DOD installations managed through the Office of Facilities Management? Who has responsibility of the Industrial Control Systems on an individual installation? Who operates Industrial Control Systems on installations—military personnel, Department of Defense civilians, or contractors? How has OASD(S) utilized Industrial Control System Subject Matter Experts during cyber vulnerability threat assessments? Is there a deadline set for all Industrial Control Systems on installations managed by the Office of Facilities Management to be cybersecure? What is the estimated cost to secure Industrial Control Systems across all installations managed by the Office of Facilities Management? What is the acquisition plan for software and/or hardware to cybersecure Industrial Control Systems? Who within the DOD is responsible for that acquisition effort?

Secretary MCMAHON. *Does the Office of the Assistant Secretary of Defense for Sustainment (OASD(S)) have a complete inventory of existing Industrial Control Systems on all DOD installations managed through the Office of Facilities Management?* The Components are developing installation-level cybersecurity plans that show their progress towards inventorying, assessing, mitigating, and monitoring their ICS. These plans address all elements of a control system, such as computer hardware, software, and associated sensors, and address the full range of infrastructure and facilities across the Department (e.g., installation electricity, water, wastewater, natural gas, lighting, building heating and air conditioning equipment, building control systems, etc.). The DOD Components are required to implement these plans and account for an inventory of facility-related control systems supporting Defense Critical Assets and Tier 1 Task Critical Assets (TCAs), as well as facility-related control systems that are connected to DOD networks, are internet-facing and/or standalone, and require Authorization to Operate (ATO).

Who has responsibility of the Industrial Control Systems on an individual installation? System asset owners have responsibility for the Industrial Control Systems on an individual installation.

Who operates Industrial Control Systems on installations—military personnel, Department of Defense civilians, or contractors? Depending on the asset and installation, military personnel, DOD civilians, and contractors may operate industrial control systems.

How has OASD(S) utilized Industrial Control System Subject Matter Experts during cyber vulnerability threat assessments? Subject matter experts are used throughout the Department's effort to secure Industrial Control Systems. For instance, subject matter experts from industry, the Services, and national laboratories are informing the development of a Tested Products List for ICS. The Tested Projects List will enable vendors/products to go through cybersecurity testing and enable Type Authorization (test once and use many times) in less time and at lower cost. DOD's Environmental Security Technology Certification Program also funded a number of cybersecurity projects associated with Smart Grids, Energy Storage, Heating, Ventilation and Air Conditioning, and Cloud/Mobile/Internet of Things that evaluate next generation devices and components capabilities and how vendor/suppliers can meet the new NIST ICS guidelines and standards. DOD also created Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) to enhance the detection, mitigation, and recovery of cyber-attacks on control systems and support the training of risk assessment teams across the Department.

Is there a deadline set for all Industrial Control Systems on installations managed by the Office of Facilities Management to be cybersecure? As required by the FY 2017 NDAA Sec. 1650, "Evaluation of cyber vulnerabilities of DOD critical infrastructure," Components are responsible for completing an inventory of ICS for defense critical and task critical assets by the end of CY2020.

What is the estimated cost to secure Industrial Control Systems across all installations managed by the Office of Facilities Management? Estimated costs to secure Facility-Related Control Systems across all DOD installations are being collected as part of the POM22 cycle and will be formalized as a standalone budget exhibit to improve the policy and governance of overall DOD investments in ICS security.

What is the acquisition plan for software and/or hardware to cybersecure Industrial Control Systems? Who within the DOD is responsible for that acquisition effort? The DOD has taken a number of steps to reduce the vulnerabilities and impacts of compromised devices and components. The DOD has adopted the NIST SP 800–161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations and is working with the Defense Industrial Base, suppliers and vendors, and other organizations such as the International Society of Automation to ensure the implementation of appropriate supply chain risk management processes. Additionally, cybersecurity has been integrated into installation policy and guidance. This guidance requires control systems to incorporate the cybersecurity requirements established in the Unified Facilities Criteria 4–01–16 and meet cybersecurity risk management framework requirements of DOD Instruction 8510.01 Risk Management Framework (RMF).

Mr. BROOKS. In July of 2015, the Government Accountability Office issued a report (GAO–15–749) that stated, "as of February 2015, none of the military services had a complete inventory of existing Industrial Control Systems." It's been four years since that report was issued. Does the Army currently have a complete inventory of existing Industrial Control Systems on all Army installations? Who has responsibility of the Industrial Control Systems on an individual installation? Who operates Industrial Control Systems on installations—military personnel, Department of Defense civilians, or contractors? How has your department utilized Industrial Control System Subject Matter Experts during cyber vulnerability threat assessments? Is there a deadline set for all Industrial Control Systems on Army installations to be cybersecure? What is the estimated cost to secure Industrial Control Systems across all Army installations? What is the acquisition plan for software and/or hardware to cybersecure Industrial Control Systems? Who within the Army is responsible for that acquisition effort?

Secretary BEEHLER. *a) Does the Army currently have a complete inventory of existing Industrial Control Systems on all Army installations?* For control systems installed as part new construction, renovation, or modernization efforts, as well as the identification of control systems discovered during cybersecurity assessments since 2017, the Army has a complete inventory. To address the installed base of control systems across its infrastructure, the Army has been systematically inventorying control systems using priorities as scaled in the Army's Cybersecurity Strategy for Facility-Related Control Systems. Army expects to have a complete inventory of all Facility-Related Control systems by 2025. The initial focus of this effort is centered on the Army defense critical assets and Tier 1 task critical assets as part of the requirements of the FY17 NDAA Section 1650. Army Cyber Command (ARCYBER) is the executing authority for the FY17 NDAA Section 1650 cyber assessments. The Army continues to make gains in the inventory of the installed base of control systems outside of the NDAA 1650 efforts. Army has identified over 365 control systems, and have completed cyber assessments on over 120 of them. Army plans to release a Fragmentation Order (FRAGO) to Execution Order (EXORD) 141–18 directing Army organization to increase efforts on the inventory and cyber assessment of FRCS.

b) Who has responsibility of the Industrial Control Systems on an individual installation? All control systems must have an appointed owner responsible for the overall procurement, development, integrations, modification, or operation and maintenance of the system. Primarily those owners are members of the local Installation or industrial activity staff.

c) Who operates Industrial Control Systems on installations—military personnel, Department of Defense civilians, or contractors? The Army control system workforce is a mixture of DOD civilians, military, and contractor support.

d) How has your department utilized Industrial Control System Subject Matter Experts during cyber vulnerability threat assessments? The Army has chosen to develop a training pipeline and equip teams to support FY 17–NDAA 1650 assessments for critical infrastructure. We are also developing an ICS Red Team capability under the Army Corps of Engineers, and have executed several missions with Cyber Protection Teams and USACE infrastructure. In most cases, the ICS/SCADA systems are connected to, controlled, and managed by more traditional IT systems, resulting in a training cross over from more traditional defensive cyber operations to ICS/SCADA networks.

e) Is there a deadline set for all Industrial Control Systems on Army installations to be cybersecure? Based on priorities as scaled in the Army's Cybersecurity Strategy for Facility-Related Control Systems. Army's expects to complete the assessment of all Facility-Related Control systems by 2025. The initial focus of this effort is centered on the Army defense critical assets and Tier 1 task critical assets as part of the requirements of the FY17 NDAA Section 1650. Army Cyber Command (ARCYBER) is the executing authority for the FY17 NDAA Section 1650 cyber assessments. To date ARCYBER has completed 11 of 26 cyber assessments IAW the NDAA 1650, and expects to complete all assessments by the December 2020 deadline.

f) What is the estimated cost to secure Industrial Control Systems across all Army installations? The completed cyber assessments are providing critical insight to the challenges of securing control systems and will inform mitigation prioritization effort. While the total cost for expected modernization and changes is difficult to determine at this point, based on existing assessments, hardware replacement and software upgrades will be required.

g) What is the acquisition plan for software and/or hardware to cybersecure Industrial Control Systems? Since 2017, Army has integrated cybersecurity into its Installation policy and guidance. This guidance requires control systems to incorporate the cybersecurity requirements established in the Unified Facilities Criteria 4–010–16 and meet cybersecurity risk management framework requirements of DOD Instruction 8510.01 Risk Management Framework (RMF).

h) Who within the Army is responsible for that acquisition effort? Acquisition is largely decentralized. Control systems are generally locally budgeted, acquired, maintained, and operated at each Installation. However, Army guidance requires control systems to incorporate the cybersecurity requirements established in the Unified Facilities Criteria 4–010–16 and meet cybersecurity risk management framework requirements of DOD Instruction 8510.01 Risk Management Framework (RMF).

Mr. BROOKS. In July of 2015, the Government Accountability Office issued a report (GAO–15–749) that stated, "as of February 2015, none of the military services had a complete inventory of existing Industrial Control Systems." It's been four years since that report was issued. Does the Air Force currently have a complete inventory of existing Industrial Control Systems on all Army installations? Who has responsibility of the Industrial Control Systems on an individual installation? Who operates Industrial Control Systems on installations—military personnel, Department of Defense civilians, or contractors? How has your department utilized Industrial Control System Subject Matter Experts during cyber vulnerability threat assessments? Is there a deadline set for all Industrial Control Systems on Air Force installations to be cybersecure? What is the estimated cost to secure Industrial Control Systems across all Air Force installations? What is the acquisition plan for software and/or hardware to cybersecure Industrial Control Systems? Who within the Air Force is responsible for that acquisition effort?

Secretary HENDERSON. The Army is developing its own inventory of their installation's control systems. The Air Force has conducted a front-end inventory of Civil Engineer systems across Active Duty bases and the Air National Guard has started a similar effort. The scope of the inventory does not include end-devices but focuses on the number of different control system types at an AF base (e.g. the Energy Management Control System is counted as one—the count is not every facility's HVAC, etc.). The installation commander has authority over all control systems on an Air Force installation, and the operation and maintenance of Civil Engineer-owned Facility Related Control Systems is conducted by the Civil Engineer Squadron. The operation of control systems is specific to each base, but includes all three categories (military personnel, Department of Defense civilians, and contractors). The Air Force Civil Engineer community has established partnerships with Idaho National Labs through their fellowship program, National Security Agency through assessment expertise, and Sandia National Labs through a Joint Capability Technology Demonstration. The Air Force is using a continual process improvement approach as cybersecurity is a constantly evolving issue. Total security is unattainable. The Air Force is using a risk-based approach to focus resources on cybersecurity that enable Department of Defense and Air Force core missions. The approach is to identify and mitigate the cyber vulnerabilities of the Air Force's highest-priority critical assets and supporting infrastructure that enable Combatant Command warfighting capabilities. Acquisition of control systems requires a partnership with industry who designs the system architecture. Our plan is to collaborate with industry and to produce standards for requirements development and contract language in order to mature the resiliency of Industrial Control Systems. Acquisition authority resides with SAF/AQ, but each system owner develops the requirements for every contract. A team approach will be needed to ensure we obtain cyber resilient systems and some clauses exist while striving to improve.

Mr. BROOKS. In July of 2015, the Government Accountability Office issued a report (GAO–15–749) that stated, "as of February 2015, none of the military services had a complete inventory of existing Industrial Control Systems." It's been four years since that report was issued. Does the Navy and Marine Corps currently have a complete inventory of existing Industrial Control Systems on all Army installations? Who has responsibility of the Industrial Control Systems on an individual installation? Who operates Industrial Control Systems on installations—military personnel, Department of Defense civilians, or contractors? How has your department utilized Industrial Control System Subject Matter Experts during cyber vulnerability threat assessments? Is there a deadline set for all Industrial Control Systems on Navy and Marine Corps installations to be cybersecure? What is the estimated cost to secure Industrial Control Systems across all Navy and Marine Corps installations? What is the acquisition plan for software and/or hardware to cybersecure Industrial Control Systems? Who within the Navy and the Marine Corps is responsible for that acquisition effort?

Mr. NIEMEYER. 1) The DON has developed and is maintaining a comprehensive inventory of its Industrial Control Systems through several ongoing efforts including: Mission Assurance Assessments, Cyber Hygiene Assessments, Building and Utility Control System Implementation Plan Assessments, and ICS authorization and accreditation.

2) On an individual U.S. Navy installation, responsibility of ICS/SCADA falls to the system owner, who also has the responsibility for managing its operations. Within the Marine Corps. MCICOM is responsible for the secure operation of ICS/SCADA.

3) Navy ICS/SCADA systems are operated by leveraging a workforce about 40% contractor and 60% Government (military and civilian) worldwide. The Marine Corps is still developing its workforce capability but expects to use a mix of military, civilian and contractor resources.

4) Navy and Marine Corps ICS/SCADA Subject Matter Experts are an integral members of the Cyber Vulnerability Threat Assessment Team providing architectural knowledge and validating recommendations and mitigations.

5) Both Navy and Marine Corps have taken a deliberate phased approach to securing ICS/SCADA worldwide. The Navy is currently on track with securing the most critical infrastructure first and plan to be complete with this first phase by the end of FY21. The Marine Corps plan all of its ICS/SCADA cyber secure by the end of FY25.

6) The Navy and Marine Corps have taken a deliberate phased approach to securing ICS/SCADA worldwide. The Navy is currently on track with securing the most critical infrastructure first and plan to be complete with this first phase by the end of FY21. The Marine Corps plan all of its ICS/SCADA cyber secure by the end of FY25.

7) The DON does not have a final cost estimate to secure all ICS across all Navy and Marine Corps installation, but instead is focusing its resources on mitigation of its most critical risks as outlined in DON facility related control system plans.

8) DON is pursuing policies for standardizing control systems at the installation level as way to reduce cybersecurity and lifecycle control system modernization costs.

9) NAVFAC is leading the acquisition efforts in their role as the ICS/SCADA acquisition and technical authority. Marine Corps intends to purchase necessary hardware and software through Navy and Marine Corps acquisition avenues based on best value.

QUESTIONS SUBMITTED BY MR. KIM

Mr. KIM. Please describe the top lessons you learned from the black-start exercises.

Secretary MCMAHON. As indicated in the National Defense Strategy, resilient forces and facilities are a critical component of deterring and defeating adversaries. The Energy Resilience Readiness Exercises, also referred to as black-start exercises, executed by the DOD in collaboration with its Components are designed to ensure military installations are energy resilient and have the power they need to operate their critical missions in the event of a disruption. The four exercises completed to date have provided invaluable lessons learned that fall within four key areas. First, we've learned that unknown interdependences exist between the energy systems and other systems on our installations, such as communications and life, health, and safety systems. Second, full operational testing and exercises ensure that all critical building loads (e.g., elevators, emergency signs/lights, SIPR doors, etc.) are on the backup system when power is disrupted. Third, military installations lack the appropriate resourcing strategy for interior electrical systems contributing to energy resilience, such as purchases of transfer switches and uninterruptable power systems as well as insufficient resources needed for facility engineers to maintain these systems. Last, the exercises provided information to prioritize energy resilience gaps to remediate risks and vulnerabilities that would prevent mission degradation or failure. The DOD is addressing these gaps through our Installation Energy Plans process to identify the most cost-effective solutions that provide the maximum benefit towards improving energy resilience and mission readiness.

Mr. KIM. What have you done to implement lessons learned from black-start exercises?

Secretary MCMAHON. The DOD has taken the lessons learned from the Energy Resilience Readiness Exercises (ERRE) and developed several solutions for closing gaps, reducing risk, and enhancing our energy resilience posture across the Department. The Department works with each of its Components to develop solutions to addressing these gaps. This is accomplished by coordinating with the Services to document gaps and necessary mitigations in each installation's Installation Energy Plan and ensure that solutions are implemented a timely and effective manner. The DOD has also developed ERRE framework guidance which provides the Components the necessary policy statement to resource and to continue to routinely perform exercises and to monitor the effectiveness of implemented energy resilience solutions. Lastly, the Department plans to enhance the ERRE framework and augment future exercises with additional elements, such as simulated cyber-attacks. These efforts promote specific actions that all installations can take to identify and mitigate mission-related risks and enhance energy resilience.

Mr. KIM. In 2012 when Hurricane Sandy ravaged my district, Joint Base McGuire-Dix-Lakehurst's resiliency allowed it to rebound and serve as a staging area for FEMA. In the event of future natural disasters or cyber-attacks, the destruction will not be limited to just bases; what are you doing to work with FEMA and other organizations to prepare? Are there any tabletop/real world exercises planned?

Secretary MCMAHON. DLA is synched with FEMA, USNORTHCOM, NGB, etc. on disaster preparedness plans. We participate in FEMA's yearly exercises such as the 2019 Hurricane Preparedness Exercise conducted in July 2019 based on the 2017 Hurricane Maria that devastated Puerto Rico. FEMA has begun the initial planning for a Utah Wasatch earthquake exercise in May 2020 and FEMA's Binary Blackout Exercise as part of Eagle Horizon. DLA will participate in both exercises. DLA also participates in FEMA's annual Senior Leader Seminar along with U.S. Army Corps of Engineers. We utilize disaster lessons learned and planned exercises to develop and refine our Pre-scripted Mission Assignments so they are current for quick menu use during hurricane season and any natural disasters. The exercises revolve around preparedness and DLA's ability to support through commodities such as food, water, cots, generators, and fuel to name a few. We also execute quarterly USNORTHCOM DSCA Executive Seminars. Although Eagle Horizon and Binary Blackout will address cyber issues, exercises previously executed have not specifically addressed cyber issues or the resiliency of military organizations.

Mr. KIM. Please describe the top lessons you learned from the black-start exercises.

Secretary BEEHLER. Energy Resilience Readiness Exercises (ERREs) have enabled installations to uncover hidden dependencies among critical systems. Backup energy infrastructure often exists in configurations that are either unknown or not documented. The ERREs provide verification of backup energy system configurations including: identification of critical facilities that do not have backup generation, confirmation that all critical loads are connected to backup generation circuits, and evaluation of outage recovery processes. Planning for an ERRE forces discussions to happen amongst various internal and external stakeholders. The planning supports clear determination of critical load requirements, and documentation of back start procedures and emergency response plans.

Mr. KIM. What have you done to implement lessons learned from black-start exercises?

Secretary BEEHLER. Energy Resilience Readiness Exercises (ERREs) have helped installations identify deficiencies in backup power capabilities in the event of a wide spread grid outage. The scope and scale of deficiencies varies and installations are working to address both near-term and longer-term mitigation actions. In the weeks and months following the ERREs, installations have taken immediate action to address deficiencies like re-assigning backup generators to better align with critical facilities; purchasing new uninterruptible power supply (UPS) systems for mission-essential equipment; and updating maintenance and emergency response procedures with privatized utility providers. Additional deficiencies identified during the ERREs require more significant technical solution development (engineering design) or larger capital investment. These projects are being included for action in the Installation Energy and Water Plans (IEWPs). The IEWPs provide an installation-wide prioritized list of actions to address energy and water resilience gaps and will guide both appropriated and third-party funding project investment.

Mr. KIM. In 2012 when Hurricane Sandy ravaged my district, Joint Base McGuire-Dix-Lakehurst's resiliency allowed it to rebound and serve as a staging area for FEMA. In the event of future natural disasters or cyber-attacks, the destruction will not be limited to just bases; what are you doing to work with FEMA and other organizations to prepare? Are there any tabletop/real world exercises planned?

Secretary BEEHLER. In December 2006, the Joint Requirements Oversight Council Memorandum (JROCM) 263–06 established requirements for the National Guard Bureau (NGB) and USNORTHCOM to establish a National Guard (NG) joint interagency training program that included four regional NG command post exercises annually. As a result of this requirement, the NGB and USNORTHCOM developed the Vigilant Guard (VG) Joint Exercise Program. VIGILANT GUARD is a USNORTHCOM Joint Exercise Program conducted in conjunction with NGB. The VG program provides an opportunity for State National Guard Headquarters, State Joint Task Forces and Field Units to improve command and control and operational relationships with Federal, Regional, State, and Local civilian and military partners. Routine participants in VG exercises include:

- State Joint Force Headquarters (JFHQs) and Joint Task Forces (JTFs) per DOD Directive 5105.83
- State emergency management agencies and City/County emergency operations centers
- National Guard Reaction Forces (NGRFs), Civil Support Teams (CSTs), CBRNE Enhanced Response Force Packages (CERFPs), and Homeland Response Forces (HRFs)
- Various Federal civilian partners (e.g., DHS, FEMA) and Federal military partners (e.g. USNORTHCOM, ARNORTH) as dictated by the scenario.

The NGB also establish the Special Focus Joint Exercise (SFE) Program. The SFE is a NGB full scale exercise that enables Joint NG and interagency operations at the local, state and regional level, emphasizing how the participants establish liaison relationships within the Incident Command Structure. Routine participants in the SFE exercises include:

- State Agencies
- Federal Civilian Partners (e.g., DOE, DHS,FEMA, USCG)
- Federal Military Partners (e.g., ARNORTH)
- State emergency management agencies and City/County emergency operations centers, and Incident Management Teams
- Local/State Civilian Partners (e.g., Police, Fire)
- Regional Response Partners (e.g., SAR teams)
- Volunteer Organizations in Disasters
- Non-Governmental Organizations
- Private Sector Partners
- Faith Based Groups

Additionally, in an effort to meet the requirements outlined in JROCM 263–06, the NG, in conjunction with USNORTHCOM, participates in the National Exercise Program (NEP). NEP is a two-year cycle of exercises across the nation that examine and validate capabilities in all preparedness mission areas. Within the program, FEMA facilitates National Level Exercises (NLE) built upon real-world incidents to make sure that our nation is better prepared when the next disaster strikes. These exercises are whole of community engagements.

Mr. KIM. Please describe the top lessons you learned from the black-start exercises.

Secretary HENDERSON. The Air Force recently completed two planned Energy Resilience Readiness Exercises (ERREs) at Hanscom Air Force Base (AFB) and Vandenberg AFB. Both exercises went very well, and the final reports on these are due to OSD in March of 2020. At this time, the findings are preliminary and general, but the Air Force would appreciate the opportunity to provide a more-detailed briefing on our lessons learned after we have had the opportunity to fully assess the outcomes from these exercises. In general, it is clear that these ERREs identified asset interdependencies that will enable the installation to better-prepare for and recover from energy disruptions in the future.

Mr. KIM. What have you done to implement lessons learned from black-start exercises?

Secretary HENDERSON. The Air Force is still awaiting the full analysis and report from the Hanscom AFB ERRE. Upon receipt of that report and the results of the Vandenberg ERRE later this fall, SAF/IEE will look for patterns and lessons learned to implement across installations. The results of these lessons learned may be incorporated into Installation Energy Plans (IEPs) or specific project recommendations on Hanscom or Vandenberg AFBs. Currently USAF policies or procedures have not changed as a result of the Hanscom AFB ERRE. The ERREs help baseline readiness posture installation by installation, and the Air Force will need to complete more exercises across the enterprise before changes to policy are enacted.

Mr. KIM. In 2012 when Hurricane Sandy ravaged my district, Joint Base McGuire-Dix-Lakehurst's resiliency allowed it to rebound and serve as a staging area for FEMA. In the event of future natural disasters or cyber-attacks, the destruction will not be limited to just bases; what are you doing to work with FEMA and other organizations to prepare? Are there any tabletop/real world exercises planned?

Secretary HENDERSON. The Department of Defense actively supports and participates in FEMA's National Level Exercise program, which promotes preparedness and response to catastrophic events across the federal agencies.. For example, Ardent Sentry is an annual North American Aerospace Defense Command and U.S. Northern Command exercise that is part of the Federal Emergency Management Agency's national level exercise. Each year a different event type is exercised using a mock catastrophic event (such as Atlantic Hurricane, Southern California Earthquake, Cascadia Subduction Zone Earthquake, New Madrid Seismic Zone Earthquake, 10kt Nuclear Detonation, and Alaska Earthquake). The Air Force and other military departments participate in a supporting role to Federal Emergency Management Agency in these exercises. In addition, Air Force forces may be provided to a combatant commander for directed exercises designed to improve force readiness to accomplish Defense Support of Civil Authorities related operations. Finally, Air Force Emergency Preparedness Liaison Officers participate in local, state, and regional exercises.

Mr. KIM. Please describe the top lessons you learned from the black-start exercises.

Mr. NIEMEYER. The DON has taken a deliberate approach to black starts, investing in tabletop exercises and comprehensive mission assurance assessments as a precursor. DON has partnered with OASD(Energy) and the Massachusetts Institute of Technology-Lincoln Labs to conduct dozens of tabletop energy resilience assessments at multiple installations in California, Washington State, Pennsylvania, Virginia as well as overseas in Guam and Italy. Theses tabletop exercises simulate a multi-state outage of the electrical grid for 30-days while the installation maintains a state of constant readiness. From these exercises, we learned that installations often do not have a perfect understanding of the energy requirements, generation and distribution needed to sustain operations over many weeks. Installations also currently operate with unknown risks and interdependencies to systems and missions, and more work is necessary to ensure installations have a comprehensive site picture of the energy system capabilities during a real outage. Moving forward, the DON is planning a large and several smaller scale exercises in 2020 at MCAS Miramar, MCB Butler and Camp Lejeune.

Mr. KIM. What have you done to implement lessons learned from black-start exercises?

Mr. NIEMEYER. The DON is implementing the lessons learned from our tabletop exercises through our established Mission Assurance Program. DON's Mission Assurance Program provides an integrative framework and a process to protect or ensure the continued function and resilience of capabilities and assets critical to the performance of Department of Defense mission-essential functions in any operating environment or condition.

Mr. KIM. In 2012 when Hurricane Sandy ravaged my district, Joint Base McGuire-Dix-Lakehurst's resiliency allowed it to rebound and serve as a staging area for FEMA. In the event of future natural disasters or cyber-attacks, the destruction will not be limited to just bases; what are you doing to work with FEMA and other organizations to prepare? Are there any tabletop/real world exercises planned?

Mr. NIEMEYER. The DON is implementing the lessons learned from our tabletop exercises through our established Mission Assurance Program. DON's Mission Assurance Program provides an integrative framework and a process to protect or ensure the continued function and resilience of capabilities and assets critical to the performance of Department of Defense mission-essential functions in any operating environment or condition.

QUESTIONS SUBMITTED BY MS. TORRES SMALL

Ms. TORRES SMALL. During the hearing Congresswoman Torres Small discussed the aging infrastructure at White Sands Missile Range. In particular, she discussed an information systems facility built in 1962. The facility serves as the gateway for all communications and data to the outside world, and houses critical equipment providing support for administrative command and control and testing and evaluation users. The facility is relied upon to provide critical support for modern missile testing ranging from the Standard Missile-2 and Patriot Missile System-3 to next generation weapon systems. Can you please speak to how conducting operations in a 57-year-old facility could stunt the efforts for maximizing installation resiliency? How does this impact our cyber security?

Secretary BEEHLER. Currently, the Information System Facility (ISF) operates out of ten separate buildings located at WSMR. Each assigned building has undergone varying levels of retrofit to accommodate the current ISF mission. Current geographically separated space is suboptimal and in regard to facilitating the operational synergy required for 24-hour information management and the necessary workforce fusion required for network defense and security. The Army assesses risks and needs in determining where to allocate funds for military construction (MILCON) and facility sustainment, restoration and modernization. At this time, the ISF project will compete for funding in FY21.

○