

UNDER SECRETARY OF DEFENSE

4000 DEFENSE PENTAGON WASHINGTON, D.C. 20301-4000

The Honorable Mike Gallagher U.S. House of Representatives Washington, DC 20515

NOV 2 0 2020

Dear Representative Gallagher:

Thank you for your October 30, 2020 letter to the Secretary of Defense expressing your support of the proposed Federal Acquisition Regulation: Protecting Life in Global Health Assistance, RIN: 9000-AN62, FAR Case 2018-002.

The public comment period for this proposed regulation closed on November 13, 2020. The Department of Defense will work with the Federal Acquisition Regulation Council, which is comprised of the Office of Management and Budget, General Services Administration, and National Aeronautics and Space Administration. The Council will adjudicate the comments that are received and then continue the established regulatory process to publish this regulation.

Thank you for your continued strong support for the health and well-being of our Service members, civilian employees, and families.

Sincerely,

Matthew P. Donovan

Congress of the United States Washington, DC 20515

October 30, 2020

Honorable Mark Esper Secretary Department of Defense 100 Pentagon Defense Washington, DC 20301 Honorable Emily W. Murphy Administrator General Services Administration 1800 F Street, N.W. Washington, D.C. 20405 Honorable James F. Bridenstine Administrator National Aeronautics and Space Administration 300 E Street, S.W. Washington, D.C. 20546

Re: Federal Acquisition Regulation: Protecting Life in Global Health Assistance, RIN: 9000-AN62, FAR Case 2018-002

Dear Secretary Esper, Administrator Murphy, and Administrator Bridenstine:

We write to express our strong support and gratitude for the September 14, 2020 proposed rule on Protecting Life in Global Health Assistance (PLGHA). The proposed extension of PLGHA to contracts and sub-contracts will close a significant loophole and further protect U.S. taxpayer dollars from flowing to the international abortion industry.

First implemented under President Reagan 36 years ago, the Mexico City Policy ensured that foreign non-governmental organizations (NGOs) receiving U.S. foreign aid through the USAID Family Planning Assistance program would not be allowed to perform or actively promote abortion as a method of family planning in foreign countries. President Trump reinstated and expanded this policy in 2017 to include all "global health assistance furnished by all departments or agencies". President Trump's expansion of the Mexico City Policy, PLGHA, ensured that \$9 billion in taxpayer funding was protected from supporting abortion, compared to \$600 million under previous administrations.²

On August 17, 2020, the Trump Administration released a report reviewing the implementation of PLGHA. It found that, out of 1,340 prime partners, only eight prime grantees declined to comply with the PLGHA terms; forty-seven subgrantees also declined to comply.³ The report noted that, when a subrecipient declined, in most cases the prime grantee was able to transition the activities to another organization. Overall, the report found that the vast majority of grantees chose to comply with the PLGHA terms and implementation caused minimal disruption to health care delivery.

Under the proposed rule issued on September 14th we will see even stronger protections. Currently, PLGHA only applies to global health assistance provided through grants and cooperative agreements.⁴ Under the proposed rule, PLGHA will be extended to include contracts as well. Additionally, the proposed rule states that all foreign contractors must comply with the PLGHA terms, and clarifies that, while U.S. contractors and subcontractors are not subject to PLGHA themselves, they are responsible for ensuring the compliance of any foreign subcontractors. We applied this much-needed clarification.

⁴ "Protecting Life in Global Health Assistance Frequently Asked Questions and Answers." Pg. 6. https://www.state.gov/wp-content/uploads/2019/10/PLGHA-FAQs-September-2019/pdf on RECYCLED PAPER



¹⁸² FR 8495

² https://www.state.gov/background-briefing-senior-administration-officials-on-protecting-life-in-global-health-assistance/

³ Department of State. "Review of the Implementation of the Protecting Life in Global Health Assistance Policy." August 17,2020. https://www.state.gov/wp-content/uploads/2020/08/PLGHA-2019-Review-Final-8.17.2020-508.pdf

Abortion is not healthcare, and more than 76 percent of Americans oppose using taxpayer dollars to support abortions in other countries.5 This proposed rule's extension of PLGHA to contracts will redirect additional U.S. foreign assistance away from funding the global abortion industry and toward legitimate, life-affirming global health initiatives.

This proposed rule is a critical step forward to strengthen and support the PLGHA. We thank you for you work to close this loophole and ask that you finalize the September 14th rule.

Sincerely,

CC: The Honorable Mike Pompeo Secretary U.S. Department of State 2201 C St. NW Washington, D.C. 20520

The Honorable John Barsa Acting Administrator U.S. Agency for International Development Ronald Reagan Building Washington D.C. 20523

Ron Estes Virginia Fox much

Ron Estes U.S. Representative Virginia Foxx U.S. Representative Michael, S. Lee U.S. Senator

Mike Kelly U.S. Representative Vicky Hartzler U.S. Representative Steve Daines U.S. Senator

- Chenez And

Liz Cheney U.S. Representative Andy Biggs U.S. Representative Kevin Cramer U.S. Senator

⁵Marist Poll. "Americans' Opinions on Abortion." January 2020. http://www.kofc.org/un/en/resources/news-room/polls/americansopinions-abortion.pdf

Matt Gaetz U.S. Representative

Jeff Duncan U.S. Representative fam M. She hape

James M. Inhofe U.S. Senator

Foto Oh

Pete Olson U.S. Representative John Joyce, M.D. U.S. Representative John Barrasso, M.D. U.S. Senator

N- Tillia

2 L Mg

Doug LaMalfa U.S. Representative W. Gregory Steube **U.S. Representative**

Thom Tillis U.S. Senator

Jody Hice **U.S. Representative** Kolur & Som

Robert E. Latta U.S. Representative Kelly Loeffler U.S. Senator

Dang Lambon alex & Morney

Doug Lamborn U.S. Representative

Alex X. Mooney U.S. Representative

Pat Roberts U.S. Senator

Ted Sylo

Ted S. Yoho, D.V.M. U.S. Representative William R Timmona D

William R. Timmons, IV U.S. Representative

Mike Braun

Mike Braun U.S. Senator

Scott Perry U.S. Representative Jim Banks U.S. Representative

Cindy Hyde-Smith U.S. Senator

Steven M. Palazzo Bill Flores U.S. Representative U.S. Representative U.S. Senator John Bozman **Guy Reschenthaler** David Rouzer John Boozman U.S. Representative U.S. Representative U.S. Senator Luy Busha derry Moran Larry Bucshon, M.D. Ted Budd Jerry Moran U.S. Representative U.S. Representative U.S. Senator M. K Kafel Norman Dain P. Ree Ralph Norman David P. Roe, M.D. Marco Rubio U.S. Representative U.S. Representative U.S. Senator Bill Cassida, M.D. David B. McKinley P.E. Jim Jordan Bill Cassidy, M.D. U.S. Representative U.S. Representative U.S. Senator get Feinuis Doug Collins Tom Cotton Roger Williams U.S. Representative U.S. Representative U.S. Senator

Brogg I huplow

Gregory F. Murphy, M.D. **Greg Gianforte** U.S. Representative U.S. Representative

John Thune U.S. Senator Slesko

Bloken

Harsha Hackburn

Debbie Lesko
U.S. Representative

Bradley Byrne U.S. Representative

Marsha Blackburn U.S. Senator

Austin Scott

Ranky K. Webu

John Journ

Austin Scott U.S. Representative

Randy K. Weber U.S. Representative

John Hoeven U.S. Senator

steve King

ZW. Mall

Thethay

Steve King U.S. Representative

Roger Marshall, M.D. U.S. Representative

Josh Hawley U.S. Senator

Dem Stottmu

Glenn Grothman U.S. Representative Steve and

Steve Chabot Ted
U.S. Representative U.S.

748

Ted Cruz U.S. Senator

MIRS Bern

Mike Johnson
U.S. Representative

David Kustoff

Roud Paul

David Kustoff U.S. Representative Rand Paul, M.D. U.S. Senator

Je Ho commend

John H. Rutherford U.S. Representative

carre V. Miller

Carol D. Miller U.S. Representative

Kevin Hern U.S. Representative

Jashen.

John Shimkus U.S. Representative James Lankford U.S. Senator

TZob Dontonan

Rob Portman U.S. Senator

Neal P. Dunn, M.D. U.S. Representative Daniel Webster U.S. Representative

Cathy McMorris Rodgers

U.S. Representative

Rick Scott U.S. Senator

Louie Gohmert U.S. Representative Out the Lodger

1/1 Mehter

Ben Sasse U.S. Senator

Michael Guest U.S. Representative

Ross Spano U.S. Representative Roger F. Wicker U.S. Senator

Jeff Fortenberry U.S. Representative milsolin

- Shall

Brian Babin, D.D.S. U.S. Representative

Michael B. Eng Michael B. Enzi

Bu Sacce

U.S. Senator

Lance Hooben

Rick Crawford U.S. Representative

Mike Gallagher U.S. Representative Joe Wilson U.S. Representative

Tim Burchett U.S. Representative **Garret Graves** U.S. Representative Lance Gooden U.S. Representative

Hen Buck

Brad R. Wenstrup, D.P.M.

U.S. Representative

Frank? Uto

Ken Buck

Glenn 'GT' Thompson U.S. Representative

U.S. Representative

AM_

Jadie Walorsky

BI Mill

Ralph Abraham, M.D. U.S. Representative Jackie Walorski U.S. Representative

Bob Gibbs U.S. Representative

A B TO

When Wind

Rich Huis

Billy Long
U.S. Representative

Warren Davidson U.S. Representative

Bill Huizenga U.S. Representative

Steer 1.0.

REKN ALON

J: Hogedon

Andy Harris, M.D. U.S. Representative

Rick W. Allen U.S. Representative

Jim Hagedorn U.S. Representative

Ben Cline

- Fire Walberg

John Ow Rose

Ben Cline U.S. Representative Tim Walberg U.S. Representative

John Rose U.S. Representative

Duoty Jomson

Fred Keller

Minhad Claud

Dusty Johnson U.S. Representative

Fred Keller
U.S. Representative

Michael Cloud U.S. Representative

Russ Fulcher U.S. Representative

Bill Johnson
U.S. Representative

Fulcher Bill Jahnoon

Congress of the United States

Mashington, DC 20515

March 27, 2020

The Honorable Peter T. Gaynor Administrator Federal Emergency Management Agency 500 C Street S.W. Washington, D.C. 20472 The Honorable Mark T. Esper Secretary of Defense 1000 Defense Pentagon Washington, D.C. 20301

Dear Administrator Gaynor and Secretary Esper:

We write to express support for the State of Wisconsin's request for the Federal Emergency Management Agency to coordinate federal assistance for Wisconsin to respond to the current emergency. Additionally, we write to ask for support from the Department of Defense in providing the necessary authorities for the Wisconsin National Guard under Title 32(f) in support of the current federal emergency. Federal assistance at this time is critical to leverage the efforts the State of Wisconsin is undertaking at the state and local level to contain the spread of the virus and to address and mitigate the consequences of its continued spread.

Specifically, we request your support in allowing the Wisconsin National Guard to utilize Title 32 authority and resources to provide the following critical capabilities, as outlined in a recent letter from Governor Tony Evers which we have attached for you convenience:

Community based specimen collection and testing for the virus, including:

- Establishing and providing resources for testing sites, with the location and number to be determined by WEM;
- Providing site operations, including information and temperature collection, specimen collection, and transportation of specimen; and
- Providing additional support as needed to operate the sites and support personnel assigned to the collection assignment.

Medical surge capacity, including providing:

- A surge resource to medical facilities most severely affected by the intake of patients suffering from COVID-19;
- Training in use of Personal Protective Equipment (PPE); and
- Basic level care, assist with intake, and assist providers and nurse staff at medical facilities.

Logistics, warehousing and transportation support, including providing:

 point of distribution operations and management of essential commodities, to include PPE;



OSD003437-20/CMD004192-20

- Transportation operations for PPE released to the State of Wisconsin from the National Stockpile;
- Organizational control of support infrastructure developed to distribute PPE inventory;
- Support resupply and supply chain operations to critical supplies are distributed:
- Rotary and fixed wing capacity to assist with transportation support of essential resources; and
- Resources to ensure food, water, and critical supply distribution.

Isolation support centers, including providing:

- Medical personnel qualified to establish and maintain isolation sites for known COVID- 19 patients, trained to utilize PPE; and
- Personal capable of providing the administration and sustainment of isolation centers.

Public Safety, including providing:

- Security forces upon request to ensure public safety;
- State rapid response forces to ensure security;
- · Resources to support first responders and Department of Corrections facilities in support role due to illness;
- Additional planning support to State agencies to assist with COVID-19. resource response; and
- Engineering support to civilian authorities.

Authorizing Title 32 duty status will allow the Wisconsin National Guard to apply its resources and capabilities to support civil authorities. It is our hope that you will give the Governor's request due consideration and quickly approve the federal assistance outlined in his letter.

Sincerely.

United States Senator

Member of Congress

Mike Gallagher Member of Congress

United States Senator

F. James Sensenbrenner, Jr. Member of Congress

Byan Steil Member of Congress

Glenn Grothman Member of Congress

Ron Kind

Member of Congress

Gwen Moore

Member of Congress

Ce: The Honorable Ryan McCarthy

Secretary of the Army 101 Army Pentagon Washington, D.C. 20310

General Joseph L. Lengyel Chief, National Guard Bureau 1636 Defense Pentagon Suite, 1E169

Washington, D.C. 20301



THE UNDER SECRETARY OF DEFENSE 3010 DEFENSE PENTAGON

WASHINGTON, DC 20301-3010

JUN 0 9 2020

The Honorable Mike Gallagher U.S. House of Representatives Washington, DC 20515

Dear Representative Gallagher:

Thank you for your letter dated March 26, 2020. On behalf of the Secretary of Defense, and the Department of Defense (DoD), I apologize for the delay in this more detailed response. In addition to efforts highlighted in the Department's previous interim response dated April 15, 2020, the Department continues to support the Defense Industrial Base (DIB) by issuing guidance allowing companies to continue to work, providing liquidity to the industrial base, implementing legislation benefitting industry, and improving the speed of contracting activity, all while maintaining a continued dialogue with Congressional Defense Committee members, their staff, and the Department's Industry partners and small businesses.

As you note in your letter, oversight is important throughout this pandemic. We are committed to spending transparency and regularly analyze data on contracting actions in support of COVID 19, and we share that information with congressional staff and oversight organizations. In addition, the Department prioritizes continued oversight of measures taken supporting the DIB, such as increased progress payments to industry, to ensure they are conducted in the best interest of the entire defense enterprise. We were working closely with industry before the crisis began, but have increased our engagement to ensure we are aware of their concerns and they are aware of the Department's expectations regarding cash flow. To augment our own oversight efforts, the Department of Defense Inspector General (DoDIG) announced on May 27, 2020, the "Audit of DoD Implementation of Section 3610 Authorized by the Coronavirus Aid, Relief, and Economic Security Act (Project No. D2020-D000AH-0137.000)" which will assess DoD's implementation of section 3610, including the authorization and reimbursement of contractor costs as authorized by contracting officers. In addition to the DoDIG's audit, the Government Accountability Office is conducting an audit on a federal scale.

Additionally, my staff has worked closely with the professional staff of the Congressional Defense Committees to include weekly status calls. In advance of those engagements, we provide your staff the latest COVID-19 contracting policy guidance and obligation information, as well as responses to any inquiries they may present. Most recently, we provided them with details of actions taken to support the DIB, as well their demonstrated results (enclosed).

I look forward to continuing to communicate with you and your House colleagues on our shared goal of protecting and preserving the defense industrial base. Thank you for your continued support of our national security and the American people.

Sincerely,

Enclosure: As stated

150 665377 AC

Congress of the United States Washington, DC 20515

March 26, 2020

The Honorable Mark Esper
Secretary
Department of Defense
1000 Defense Pentagon Washington, DC 20301-1000

Re: Mitigating Impacts of COVID-19 on the Defense Industrial Base

Dear Secretary Esper,

We greatly appreciate the actions you and your colleagues in the Department have taken both to combat the spread and effects of COVID-19 as well as provide guidance for protecting the Defense Industrial Base. As Congress acts to bring relief to individual Americans and many of the industries hardest hit, we encourage you to continue taking additional action within your existing authority to mitigate damage to the only sector charged with protecting our national security. There is much you can do to avoid both short term and long term damage to the defense industrial base—an industry comprised of approximately 300,000 companies, the majority of which are small businesses.

First, we appreciate the memorandum Under Secretary Lord released on March 20, 2020, and thank all of you for getting this guidance out expeditiously. The designation of the Defense Industrial Base as Essential Critical Infrastructure will ensure vital parts, equipment, and services continue to flow to our warfighters even in the midst of the disruption caused by COVID-19. This, of course, comes with the understanding that the defense industry will do everything recommended by the CDC and federal and state governments to ensure the safety of our workforce and their families as we cope with the spread of this virus. As these measures continue, we encourage you to work closely with state and local authorities to ensure these workers maintain access to their facilities, installations, and work areas even as measures are taken to limit movement around the nation. It is particularly important for the small business in the supply chain to avoid ruinous work stoppages.

We were pleased to learn the Department has taken action to increase progress payment rates, and appreciate your acknowledgement of how vulnerable the defense-industrial base is to adversarial capital during this crisis. As Ms. Herrington's memo states, it is imperative that we "ensure companies stay in business without losing their technology." We applaud these efforts and proactive measures.



PRINTED ON RECYCLED PAPER

We were also pleased with the guidance from the Office of Management and Budget released on March 20, 2020 regarding the management of federal contract performance. In accordance with this guidance, we ask you to direct your contracting authorities to exercise both their judgment and what authorities they currently have to excuse delays, entitle vendors to an equitable adjustment of the contract price, and still make payments in a timely manner when vendors run into challenges to their contract fulfillment presented by COVID-19 and mitigation efforts by the federal, state, and local governments. These extraordinary circumstances have the potential to cripple our supply chain, which relies so heavily on specialized small businesses for parts and services. Allowing thousands of companies to shutter their doors and close down lines during this economic hardship will have devastating long-term implications for our entire national security enterprise.

Oversight will remain tremendously important throughout this disruptive pandemic, and we encourage you and your colleagues to maintain strict oversight of where these dollars are going. For our part, we will do the same, and ask the Department to provide an overview on how they plan to achieve this. As we move forward, oversight and accountability will remain very important.

Finally, we ask that you work closely with the Congressional Defense Committees to inform us of any gaps in your authority needed to adequately protect and preserve our defense industrial base. To this end, we request you provide recurring weekly updates on the impact to the defense industrial base. Included in this briefing should be a detailed list of companies with any impacts to their operations as well as the resulting impact to weapon system availability and readiness. Congress is moving forward quickly to provide the American people and companies relief from the second and third order effects of the COVID-19 pandemic. We urge you to let us know immediately if there is anything we as lawmakers can to do support the Department of Defense and the thousands of individuals, small business, and companies which make up the industrial base that supports it.

We thank you for your time and attention to these matters, and stand ready to assist however we are able. We intend to work closely with you on this and look forward to your reply.

Sincerely,

Doug Samborn

Signatories to this letter include:

Anthony G. Brown

Vicky Hartzler

Bill Foster

Paul Mitchell

Chris Pappas

Don Bacon

Robert J. Wittman

Marcy Kaptur

Bradley Byme

Mike Gallagher Seth Moulton

Michael R. Turner

James R. Langevin

Michael Waltz

C.A. Dutch Ruppersberger

Salud Carbajal

Joe Wilson

Congress of the United States

Mashington, DC 20515

March 23, 2020

The Honorable Mark T. Esper Secretary of Defense United States Department of Defense 1000 Defense Pentagon Washington, D.C. 20301

Dear Secretary Esper:

We write in support of the state of Wisconsin during this turbulent time. Although we strongly support the measures that the Department of Defense has taken thus far in order to safeguard service member health and readiness as well as to provide support to civil authorities, we want to ensure states like Wisconsin are receiving as much assistance as possible in order to counter this pandemic. As Wisconsin runs low on critical medical supplies, we are aware that the Department of Defense has unparalleled resources at its disposal that could help mitigate the severity of the crisis.

Given the extraordinary circumstances, including President Trump's declaration of a national emergency and invocation of the Defense Production Act, we respectfully request answers to the following questions about the Department of Defense's response and resources that might be available to Wisconsin:

- 1. Is the Department coordinating its response across the interagency, including with the Department of Health and Human Services (HHS) under the National Response Framework?
- 2. Can the Department provide a timeline on making major purchase orders under Defense Production Act authorities, either for direct distribution through HHS, or to backfill its own stockpiles?
- 3. Does the Department plan to federalize the National Guard in order to support its national response? If so, does the Department plan on doing so using Title 32 or Title 10 authorities? If the Department does plan on federalizing the National Guard, how will the Department ensure that states still maintain the capacity they need to coordinate their local responses?
- 4. In a White House press conference on March 18, you stated that the first of up to five million N95 respirator masks and other personal protective equipment the Department is transferring to HHS would be available immediately. Are you able to provide a timeline for when the four million additional masks and personal protective equipment will be



available? Is there anything Congress can do to assist the Department in promptly delivering this second tranche of equipment to HHS?

- 5. In the same press conference, you also noted that the Department was prepared to distribute to HHS up to 2,000 deployable ventilators as needed. Is the Department in the process of providing those ventilators to HHS? If not, at what point does the Department plan to release these ventilators to HHS? And what additional training will civilian health care providers will need in order to be able to utilize these ventilators?
- 6. What, if any, consideration has the Department given to releasing additional resources from the National Defense Stockpile beyond the items announced previously?
- 7. In light of the Department's success in providing field hospital beds during the Ebola response in West Africa, has the Department coordinated with states and local authorities either to determine whether bases have medical facilities that may be appropriately used to supplement the local response or whether the Department could assist states in building field hospitals or other medical facilities? What existing rapid contracting authorities could the Department leverage to construct these types of facilities, and are there additional authorities it would be useful for Congress to provide?
- 8. While we are grateful for your March 17 statement that 16 of the Department's laboratories would be made available to test non-DoD personnel, on March 19, Defense Health Agency Director Lt. General Ronald Place stated that the Department had not yet been asked to do so—despite possessing the capacity to conduct tens of thousands of tests per day. When can we expect these 16 labs to begin tests of non-DoD personnel, and is there any additional laboratory capacity the Department can spare to conduct additional tests?
- 9. What, if any, supply chain shortages are the Department facing in its COVID-19 response, particularly when it comes to critical medicines or medical devices manufactured in the People's Republic of China?
- 10. In addition to the \$8.3 billion identified by the administration in the March 17 letter from the Office of Management and Budget to Vice President Pence, what additional supplemental funding or reprogramming authorities specifically related to COVID-19 response efforts would better assist the Department in supporting its partners across the interagency, states, and local authorities?

In this time of unprecedented uncertainty and growing crisis, we cannot afford to leave potential resources untapped. We urge the Department to make use of all the tools at its disposal to assist civil authorities in their efforts to combat the COVID-19 pandemic. We are grateful for your continued leadership and partnership, and we stand ready to provide you and our service members with the resources you need to keep our nation secure.

Sincerely.

Ab

Mike Gallagher Member of Congress

Glenn Grothman

Member of Congress

Bryan Steil

Member of Congress

MAR

Mark Pocan Member of Congress

Ron Kind

Member of Congress



SECRETARY OF DEFENSE 1000 DEFENSE PENTAGON WASHINGTON, DC 20301-1000

3/19/2020

The Honorable Michael J. Gallagher U.S. House of Representatives Washington, DC 20515

Dear Representative Gallagher:

As a critical partner in building a strong, lethal Navy and Marine Corps, I believe it is important that I share with you the priorities and process I have instituted to better assess the alignment of Naval force structure with the National Defense Strategy (NDS). At the same time, I want to address your expectations regarding key budget and supporting documents, including the statutory requirement for the Secretary of Defense to submit a 30-year shipbuilding plan.

The Department of Defense (DoD) remains committed to building a Navy of at least 355 ships. I personally believe the force structure required is even larger. More urgently, though, the Department also remains focused on the readiness of our current fleet by allocating an additional \$3.4 billion into the Navy's operations and maintenance accounts relative to FY 2020. A Navy of 355 ships is a priority that DoD intends to achieve, but we must avoid doing so in a way that creates a hollow force unable to modernize, outfit, crew, operate, or maintain the ships the Navy has now. I want to ensure we have a fleet that is ready to deploy, fight, and win when duty calls.

While the 30-year shipbuilding plan requires certification that there is sufficient funding across the first five years, the remaining 25 years are both speculative and not budget-informed. You have the FY 2021 President's budget request, which fulfills the certification requirement. I am committed to building and providing you a plan that aligns force mix to the NDS, is based on an approved war plan, and considers resources throughout the 30-year period.

At the same time, the character of maritime warfare is changing rapidly. Technological advancements in space, cyber, and long-range missiles increase the potential for adversaries to track, target, and threaten our ships, as well as other joint platforms. Therefore, and to maintain our maritime superiority, we must explore a range of alternative "future fleet" designs that fully meet the demands of the NDS, while being compatible with future warfighting doctrine, threat developments, and budget constraints. The "future fleet" design will be based on the following:

- Modern warfighting concepts that prioritize joint operations and Navy and Marine Corps integration;
- Operational attributes that emphasize distributed awareness and lethality; survivability
 in a high-intensity conflict; adaptability in a complex world; ability to project power
 and demonstrate presence; and the capability to deliver precision effects at long ranges;



OSD002450-20/CMD003477-20

- Compositional attributes that result in fewer larger surface platforms; more smaller surface combatants; greater reliance on lightly- and optionally-manned ships: and an ample submarine force;
- Incorporation of other assets that are integral to the joint fight, such as strategic scalift;
- Emphasis on building a future fleet that will be ready and lethal over its lifetime by remaining affordable, sustainable, and adaptable in an ever-changing environment; and
- The importance of a robust and healthy industrial base, with modern shipyards and highly-skilled workers.

For the reasons outlined above, I assess that it is very prudent to take a fresh look at how we determine the composition of our future Naval forces. To this end, I have charged the Deputy Secretary of Defense with leading a comprehensive review and analysis of the Navy's proposed "future fleet" force structure. Working collaboratively with Navy and Marine Corps leadership, this team will conduct a number of war games, simulations, and detailed analyses over the coming months to assess a wider and bolder range of "future fleet" designs against key desired outcomes and parameters, including those listed above.

The results of this rigorous analysis are due back to me this summer and will drive future shipbuilding plans. It is my intention to be transparent with you regarding the methods, progress, and results of this assessment. This effort marks a unique opportunity to ensure that analysis on the fleet – the fleet that is needed to meet the NDS – better drives our shipbuilding plan into the future.

Acting Secretary Modly, Admiral Gilday, and General Berger have demonstrated a consistent commitment to ensuring the Navy and Marine Corps are integrated, not just coordinated. I look forward to working with you as we endeavor to ensure the U.S. Navy remains the most dominant maritime force and the best in the world for years to come.

Sincerely

Watt. Epa

Secretary Espor,

The Marian Control of Maria Carried Control of the State of and the second of made a second of the secon

-

Rep Gellegher—
Congrets on your survive !!

With you and open bride all

With you and open bride all

Me let. Gus I also went to

Mank you for your service on Fill

Exposite to an military Surpe Fill

Whank Efer

JUSER 19 2550019



OSD010205-19/CMD012589-19

Congress of the United States

Washington, DC 20510

September 11, 2019

The Honorable Mark Esper Secretary of Defense U.S. Department of Defense 1000 Defense Pentagon Washington, DC 20301-1000

Dear Secretary Esper,

During your Senate confirmation hearing in July, we were pleased to hear your endorsement of the 2018 National Defense Strategy, in particular your recognition of the growing threats posed by great-power competitors such as China. Long-term, peacetime competition with the Chinese Communist Party (CCP) is one of the defining challenges of our time.

The CCP has adopted a strategy of "Military-Civilian Fusion" to achieve its national objectives, enlisting Chinese corporations and universities to harness emerging civilian technologies for military purposes. If Beijing cannot develop technology on its own, it attempts to steal it from the United States using cyber espionage, intelligence assets operating in the United States, and state-directed companies that acquire American firms to transfer proprietary information. As Assistant Secretary for International Security and Nonproliferation Christopher Ford has stated, Military-Civilian Fusion is the "CCP's blueprint for China's global 'return' to military preeminence."

The Administration should reexamine all the statutory authorities at its disposal to confront the CCP's strategy of Military-Civilian Fusion, including powers that have lain dormant for years. One such statutory authority can be found in Public Law 105-261, the FY 1999 National Defense Authorization Act (NDAA), as amended. Section 1237 of this legislation states that:

"Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall make a determination of those persons operating directly or indirectly in the United States or any of its territories and possessions that are Communist Chinese military companies"

Section 1237, as amended in the FY 2001 NDAA, requires the Secretary of Defense to notify Congress, the Director of Central Intelligence, the Attorney General, and Secretaries of State, Treasury, Commerce, and Energy, of any determinations under this provision. The Secretary is also required to update this list on an ongoing basis in consultation with these officials. For the purposes of this legislation, a Communist Chinese military company includes any firm that is "owned or controlled by the People's Liberation Army" and is "engaged in providing commercial services, manufacturing, producing, or exporting."

We kindly request answers to the following questions about Section 1237, as amended:

- 1. When was this list of Communist Chinese military companies operating in the United States last updated by the Department of Defense?
- 2. As part of your commitment to achieving the goals set out in the 2018 National Defense Strategy, will you commit to updating and publicly releasing this list as soon as possible?

Thank you for your consideration of this important matter. We look forward to receiving your response and working with you to combat China's economic espionage in the United States.

Sincerely,

Tom Cotton

United States Senator

Charles E. Schumer

United States Senator

Mike Gallagher

United States Representative

Ruben Gallego

United States Representative

Congress of the United States

Washington, DC 20515

August 14, 2019

The Honorable Mark Esper Secretary of Defense 1300 Defense Pentagon Washington, DC 20301

Secretary Esper,

We are writing today to express our serious concerns regarding the recent Department of Defense (DOD) Inspector General (IG) audit that revealed DOD's pattern of purchasing vulnerable commercial-off-theshelf (COTS) technology equipment with known cybersecurity risks. We strongly encourage DOD to complete each of the IG's recommendations to ensure U.S. military personnel and facilities are protected from cyber espionage activities.

As you know, the audit discovered that in Fiscal Year 2018, the Air Force and Army purchased at least \$32.8 million of information technology products with known cybersecurity vulnerabilities. As Members of Congress who championed the language in last year's National Defense Authorization Act banning the federal government from purchasing Hikvision and Dahua video surveillance equipment, we are frustrated that it took an act of Congress to stop the military from purchasing equipment with known Chinese cyber espionage risks. It is alarming that this pattern is systemic across DOD and includes the habitual purchases of Chinese computers, printers, security cameras, and networking equipment. DOD should be a leader in assessing supply chain risks, especially when it comes to the purchase of information technology equipment for our nation's defense agency.

We understand that DOD is working to address the recommendations identified in the IG report, and we encourage DOD leaders to act swiftly to close each resolved and unresolved recommendation to ensure information technology equipment does not pose a risk to the U.S. military. Understanding the sensitive nature of this issue, we respectfully request a classified briefing to discuss each of the IG's recommendations and to learn how DOD is implementing procedures to assess and prohibit the purchase of high-risk COTS technology.

Thank you for your attention to this matter.

Wickey.

Sincerely,

Vicky Hartzler

Member of Congress

Mike Gallagher

Member of Congress

Cc: The Honorable Ellen Lord, Under Secretary of Defense for Acquisition and Sustainment

The Honorable Dana Deasy, DOD Chief Information Officer



350,09

14 Aug 19



THE UNDER SECRETARY OF DEFENSE

3030 DEFENSE PENTAGON WASHINGTON, DC 20301-3030

期1 03 261

The Honorable Mike Gallagher U.S. House of Representatives Washington, DC 20515

Dear Representative Gallagher:

Thank you for your letter, dated April 24, 2019, regarding the protection of Department of Defense (DoD)-funded research from foreign threats, particularly through cyber intrusions. This issue is very important to the Department and to this country's national security. Attempted cyber intrusions and successful cyber breaches have become increasingly common in recent years and we must be vigilant in the face of this ever-evolving threat. As your letter points out, the United States' system of open academic research and scientific inquiry is a strength of our Nation, but we must not allow adversary nations to exploit that openness to their own benefit.

The Department has a difficult balance to strike when it comes to protecting its research. Scientific research operates most efficiently when unfettered, but that openness makes it vulnerable to exploitation by foreign actors, which can provide critical knowledge and technical know-how gleaned from Department-funded research. The Department must provide the greatest protections to that work which is of a higher technical level of maturity while enabling collaboration and innovation in the academic community.

As you know, research in the Department is funded in different budget activities depending on its proximity to well-defined applications. Your letter specifically mentions the 6.1 and 6.2 budget activities; these are designated as basic and applied research, respectively, and are collectively referred to as "fundamental" research when conducted at universities. Fundamental research is the furthest away from application out of any work the Department funds. As such, the Department has traditionally given the university community fewer requirements on how such research is conducted or protected. At the same time, the Department works closely with the university community to recommend security best practices, such as the list of "Actions Taken by Universities to Address Science and Security Concerns" published by the Association of American Universities on April 22, 2019. The Department will continue to review the balance between openness and security to ensure that vital defense research is protected from our adversaries.

Given that your letter is addressed to both DoD and the Federal Bureau of Investigation (FBI), I have addressed those portions of the letter that are in the purview of the Department and have referred other inquiries to the agencies with the appropriate jurisdiction.

Question 1: What steps are the Department of Defense and the Federal Bureau of Investigations taking to protect those universities which receive funding through the Multidisciplinary University Research Initiative (MURI) and other DOD 6.1 and 6.2 category funding?

: DE 4445 19

In terms of foreign threats to university research, the Department works closely with the academic community to protect research including the MURI program and other research funded by 6.1 and 6.2 budget activities. The Department has taken a number of recent actions to protect against foreign actors seeking to exploit Department-funded research in the academic community. Foreign actors in this context would include those that seek to transfer intellectual property to adversary nations through affiliation with foreign talent programs, cyber intrusions, and other espionage activities.

To protect against foreign talent program members, the Department has strengthened its disclosure policy, which mandates that key personnel on research grants disclose all current and pending support that they are receiving which may be pertinent to Department research awards. The Department established the Protecting Critical Technology Task Force (PCTTF) to accelerate technology protection across all Department activities.

The Department has also engaged with the academic community and law enforcement on detecting and deterring foreign threats to its fundamental research; and will be expanding these engagements in the months to come. The Department has run three workshops in the past year with members of the academic community to raise awareness of the threats posed by foreign actors. The Department stood up a Deans' Roundtable this year to provide a forum for university deans to speak with high-level Department representatives in Research and Engineering and to discuss important issues including threats from foreign actors to research products. The Department also works closely with the American Security and Counter-Exploitation Working Group (ASCEWG) to develop recommendations on research security. ASCEWG has been recognized for excellence in industrial security practices by the Defense Security Services, and their meetings typically involve a chief security officer or export control officer from a university that deals with threats from foreign actors on a daily basis.

Question 2: Does the Department of Defense levy requirements on universities receiving DOD funding mandating the university institute cyber defenses, cyber monitoring, or to report suspected cyber intrusions?

Any contract to a university for the purpose of research that involves sensitive DoD information (covered defense information) must include Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting." This clause requires the university to both safeguard the covered defense information that resides on the university's internal information system and to report cyber incidents that affect covered defense information. Specifically, a university conducting such research must institute cybersecurity measures that comply with the cybersecurity standards laid out in the National Institute for Standards and Technology Special Publication 800-171 Revision 1, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

In addition to contractual requirements through DFARS Clause 252.204-7012, DoD maintains a voluntary cyber threat information sharing program with cleared defense contractors including universities. This public-private cybersecurity partnership enhances and supplements

Defense Industrial Base (DIB) participants' capabilities to safeguard DoD information that resides on, or transits, DIB unclassified information systems. Currently, 6 out of the 14 DoD University-Affiliated Research Center Laboratories (UARCs) participate in the cyber threat information sharing program.

Moreover, as a participant in the National Industrial Security Program, academic locations that maintain a facility security clearance are required to report to the FBI and DoD actual, probable, or possible espionage, sabotage, terrorism, or subversive activities, regardless of the domain (physical and virtual) in which the activity is discovered.

Question 3: What is the status of coordination between the DOD and FBI to protect research conducted at universities receiving Department of Defense funding for research? When is this coordination performed? At what level is it performed? Is this coordination performed at the National Cyber Investigative Joint Task Force (NCIJTF)? How is it documented by DOD and the FBI?

The Department, especially the Military Department Counterintelligence Organizations and Defense Criminal Investigative Organizations, maintain a close and continuous relationship with the FBI to analyze and address this threat, since the FBI is able to leverage authorities that DoD does not possess. DoD and FBI co-lead an interagency counterintelligence working group, focused on the mitigation of foreign intelligence threats to U.S. critical technologies, including taxpayer-funded research. DoD and FBI's relationship also extends to the field office level, where the Department works to provide information on DoD research to guide and facilitate FBI investigations.

Three examples of major activities that the Department has undertaken to further develop collaboration with the FBI are as follows: 1) the Department participated in the FBI Academia Summit with other Federal research funding agencies and the presidents of leading academic institutions to discuss the threat posed by foreign actors and foreign talent programs; 2) the Department hosted a briefing for FBI Counterintelligence to discuss the threat of foreign talent programs with DoD research program managers; and 3) the Department hosted an FBI representative at a meeting of the Defense Basic Research Advisory Group to discuss foreign talent programs and to help FBI establish points of contact at each of the services to speak with the program managers of individual research awards when FBI has relevant information about problematic activities. The Department has also participated in various other meetings over the past year where the FBI and State Department were present to discuss foreign talent programs.

In addition, the PCTTF is working with key subject matter experts within the Department to develop technology protection plans for critical technology areas designated by the Department, encompassing all areas of research from basic through developmental. In putting these plans together, the PCTTF is working closely with the Office of the Under Secretary of Defense for Intelligence and members of the intelligence community to better understand the threat posed by foreign actors and how best to create protection plans that address those threats.

Question 4: How is liaison work with colleges and universities on foreign cyber intrusions conducted by the FBI? What headquarters direction and support is provided to field

offices to conduct this activity? Is there an element of FBI which coordinates this engagement across field offices?

As this question is addressed to the FBI, I will defer to Director Wray for the response.

Question 5: Has the administration signaled to China that specific types of cyberattacks will be responded to with specific, proportionate yet costly, consequences?

Both the recent National Cyber Strategy and the DoD Cyber Strategy make clear that we are taking a more proactive approach to address various forms of malicious cyber activity, both by defending forward in cyberspace and taking other actions to shape adversary decision-making. DoD and State Department are closely collaborating in the Cyber Deterrence Initiative directed by the National Cyber Strategy. This effort, led by the State Department, includes the development of tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior.

I thank you for your continued leadership on this important issue. I look forward to working with your Committee to make sure that the products of Department-funded research are not lost to adversary nations due to cyber intrusions or other acts of espionage. An identical letter is being sent to Representative Speier.

Sincerely,

Michael D. Griffin

Congress of the United States Washington, DC 20515

April 24, 2019

The Honorable Patrick Shanahan Acting Secretary of Defense Department of Defense 1000 Defense Pentagon Washington, DC 20301 Christopher Wray
Director
Federal Bureau of Investigations
U.S. Department of Justice
935 Pennsylvania Avenue, NW,
Room 7240
Washington, DC 20535

Dear Secretary Shanahan and Director Wray:

We write to express our concerns stemming from recent news reports discussing offensive computer network operations conducted by the People's Republic of China against U.S. universities undertaking basic research. The reports indicated that the majority of targeted universities house research on undersea technology and the attacks began as far back as April 2017. The exploitation of vulnerabilities at these universities and the compromise of research with defense applications threatens our military advantage. We are concerned that coordination shortfalls between law enforcement, the Department of Defense, and universities as well as a paucity of security practices on the part of universities have allowed an adversary to once again exploit our openness to potentially gain an unearned advantage.

Though an open, innovative academic system remains a core strength of the U.S. research enterprise and an important advantage relative to China, we worry that the government has failed to take commonsense measures to protect its investments. Being open does not require being vulnerable. Universities must become savvier about identifying national security-related research and protecting it. The federal government can do far more to work with universities and research institutions to help in this endeavor.

Moreover, this is a national security problem affecting universities, not a university problem affecting national security. U.S. national security posture creates a permissive environment for these types of attacks from China and other adversaries. Having a more aggressive deterrent posture in public and in private wherein specific consequences are tied to specific Chinese cyber actions could help limit these intrusions in the first place.

To aid Congressional oversight of these issues, we are requesting information on the following:

1. What steps are the Department of Defense and the Federal Bureau of Investigations taking to protect those universities which receive funding through the Multidisciplinary University Research Initiative (MURI) and other DOD 6.1 and 6.2 category funding?



**OSD004445-19/CMD005462-19

PRINTED ON RECYCLED PAPER

- 2. Does the Department of Defense levy requirements on universities receiving DOD funding mandating the university institute cyber defenses, cyber monitoring, or to report suspected cyber intrusions?
- 3. What is the status of coordination between the DOD and FBI to protect research conducted at universities receiving Department of Defense funding for research? When is this coordination performed? At what level is it performed? Is this coordination performed at the National Cyber Investigative Joint Task Force (NCIJTF)? How is it documented by DOD and the FBI?
- 4. How is liaison work with colleges and universities on foreign cyber intrusions conducted by the FBI? What headquarters direction and support is provided to field offices to conduct this activity? Is there an element of FBI which coordinates this engagement across field offices?
- 5. Has the administration signaled to China that specific types of cyber attacks will be responded to with specific, proportionate yet costly, consequences?

Our military, our servicemembers, and our nation depend on the United States remaining the vanguard of technical advancements and scientific research. As you both well understand, these advantages are eradicated, and taxpayer dollars are wasted, if we are unable to preserve the integrity of the information obtained in the course of this research.

We request your response within 10 working days of receipt of this letter. Thank you for your attention to this matter and we look forward to your reply.

Sincerely,

Member of Congress

Member of Congress

ce Gallagher



THE UNDER SECRETARY OF DEFENSE

3030 DEFENSE PENTAGON WASHINGTON, DC 20301-3030 JUL 1 1 2019

The Honorable Mike Gallagher U.S. House of Representatives Washington, DC 20515-0605

Dear Representative Gallagher:

I am responding to your letter to the Acting Secretary of Defense and the Chairman of the Joint Chiefs of Staff, dated March 25, 2019, with questions on the potential threat to American national security and the information security of allies and partners of Chinese telecommunications firms building Fifth Generation (5G) networks.

The Department of Defense (DoD) is strengthening its approach to protecting information, and the systems on which this information resides, to address 5G security concerns. We are implementing the Executive Order on Securing the Information and Communications Technology and Services Supply Chain, supporting the recent Prague Proposals on 5G Security, participating in the Committee on Foreign Investment in the United States (CFIUS), and shaping the evolution of 5G design standards. We are undertaking these and other technology protection activities in coordination with interagency, commercial, and international partners, and will continue to examine a range of measures to increase security mechanisms built into the infrastructure.

Below are responses to your questions on the potential threat to American national security and the information security of allies and partners.

1. Can you articulate the espionage threat posed by the transfer of U.S. data and voice communications over a Chinese constructed 5G network?

Response: As the Acting Secretary Shanahan highlighted in his testimony to the House Armed Services Committee on March 26, 2019: "China aims to steal its way to a Chinacontrolled global technological infrastructure, including a 5G network." China's laws compel citizens and organizations to cooperate with intelligence and security services and to keep such cooperation secret. Chinese firms have a track record of undesirable cyber behavior, including intellectual property theft, intentional rerouting of data, and stealing personal information. Therefore, we are concerned that China could compel Chinese vendors to act against the interests of U.S. citizens, and citizens of other countries around the world. The scope and scale of data within 5G networks makes the threat of unauthorized access a serious concern for national security, requiring these networks be designed and operated with the highest security standards.

2. Will the United States be able to have confidence in allied or partner networks that rely on Chinese technology and which could be used for military or defense communications purposes?

13000 2915 M

Response: The United States, along with our partners and allies, must maintain robust, resilient, and reliable networks and supply chains to reduce the risk of unauthorized access and malicious cyber activity. The United States is urging countries, consistent with the Prague Proposals, to adopt a risk-based security framework for the construction of all elements of 5G networks, including a careful evaluation of potential hardware and software equipment vendors and the supply chain. The evaluation should consider the extent to which vendors are subject to control by a foreign government, and whether that government has meaningful checks and balances on its power to compel cooperation of said vendors with its intelligence and security agencies. As these networks are deployed by our close partners, we will continue to have frank and open conversations about evolving threats and the best ways to reduce risk.

3. Will our ability to share information with key allies change if a country like Germany or a Five Eyes ally were to adopt a 5G network with major systems or hardware sourced from Chinese state-directed companies?

Response: We are working closely with our Five Eyes and North Atlantic Treaty Organization (NATO) allies, and our European partners, to reinforce an informed and forward-leaning approach to dealing with Chinese-supplied information and communication technologies. Together, we intend to develop a shared understanding of the risks and cooperative approaches (technical, policy, and procedural) to mitigate the risk of unintended access.

4. What steps will DoD consider to mitigate these threats at home and at facilities abroad?

Response: We are working with interagency partners, industry, and academia to develop and promote secure design standards for 5G equipment and the ways in which that equipment is integrated and operated. Fifth Generation (5G) technology is evolving rapidly, and DoD is supporting a robust program of research and experimentation to promote 5G security. For example, we are looking to leverage the zero trust concept from cyber security and integrate that approach to 5G, ensuring that we can operate effectively even in untrusted network environments. By leading in 5G development, the United States will be better positioned to promote secure 5G technologies globally.

5. In light of these threats, do you find it concerning that American technology companies are selling critical enabling components to Chinese telecommunications firms like Huawei and ZTE?

Response: The recent Executive Order on Securing the Information and Communications Technology and Services Supply Chain is addressing this issue directly, along with the addition of Huawei to the Department of Commerce's Entity List. The 5G ecosystem is complex and American companies rely on the Chinese market to remain viable. We are working with our interagency partners to promote 5G technology control measures that both restrict our competitors' access to sensitive items while allowing U.S. companies to broadly market non-sensitive components. We want U.S. companies to do what they do best: innovate and collaborate to bring transformational products and services to the market, including the highest quality and most secure 5G components available.

I thank you for your strong support for the Department of Defense. An identical letter has been sent to Representative Ruben Gallego.

Sincerely

Michael D. Griffin



March 25, 2019

The Honorable Patrick M. Shanahan Acting Secretary of Defense 1000 Defense Pentagon Washington, DC 20301

General Joseph F. Dunford, Jr. Chairman, Joint Chiefs of Staff 9999 Joint Staff Pentagon, Room 2D920 Washington, DC 20319

Dear Secretary Shanahan and Chairman Dunford:

Congress has been briefed that Chinese telecommunications firms seeking to construct 5G networks around the world represent a potential threat to American national security and the information security of allies and partners.

China's own National Intelligence Law and concept of Military-Civil Fusion ensures that Chinese firms are not independent of the state. Rather, they must support the law enforcement, intelligence, and national security interests of the Chinese Communist Party. In light of this reality, the threat of a compromised 5G network and its negative effects on personal data, government secrets, military operations, and privacy, is high.

Accordingly, in advance of your testimony to the House Armed Services Committee this week, please consider the following questions:

- 1. Can you articulate the espionage threat posed by the transfer of U.S. data and voice communications over a Chinese constructed 5G network?
- 2. Will the United States be able to have confidence in allied or partner networks that rely on Chinese technology and which could be used for military or defense communications purposes?
- 3. Will our ability to share information with key allies change if a country like Germany or a Five Eyes ally were to adopt a 5G network with major systems or hardware sourced from Chinese state-directed companies?
- 4. What steps will DoD consider to mitigate these threats at home and at facilities abroad?
- 5. In light of these threats, do you find it concerning that American technology companies are selling critical enabling components to Chinese telecommunications firms like Huawer and ZTE?



OSD002915-19/CMD003586-19

Thank you for your attention to this matter as we continue this dialogue about our digital national security.

Mike Gallagher

Member of Congress

Ruben Gallego

Member of Congress



OFFICE OF THE UNDER SECRETARY OF DEFENSE

4000 DEFENSE PENTAGON WASHINGTON, D.C. 20301-4000

1 8 JAN 2019

The Honorable Mike Gallagher U.S. House of Representatives Washington, DC 20515

Dear Representative Gallagher:

The Department of Defense (DoD) appreciates the ongoing support from Congress and will continue to engage in strategic partnerships with teaching hospitals and professional medical organizations, as the DoD understands how critically important it is to advance trauma care for both military and civilian populations. The National Association of Emergency Medical Technicians (NAEMT) has a long standing relationship with DoD's Joint Trauma System's (JTS) Committee on Tactical Combat Casualty Care. This relationship has resulted in the NAEMT's adoption of the DoD's prehospital care guidelines, and the co-authorship and publication of the Prehospital Trauma Life Support manual. The National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2017 provided direction for several high level DoD initiatives. Section 708 of the NDAA for FY 2017 established the Joint Trauma Education and Training Directorate (JTETD). Additionally, section 707, "Joint Trauma System," of the NDAA for FY 2017 mandated the transfer of the JTS from the Secretary of the Army to the Defense Health Agency (DHA). Both NDAA sections provided additional direction to the Secretary of Defense for realignment that will drive goal-based criteria for entry into partnerships with all civilian organizations.

The Director, DHA, under the authority of the Assistant Secretary of Defense for Health Affairs (ASD(HA)), and in coordination with the Secretaries of the Military Departments, continues to standardize prehospital trauma care within the Armed Forces, as noted with the publication of DoD Instruction 1322.24, "Medical Readiness Training," March 16, 2018. The policy mandates that all Service members receive role-based, Tactical Combat Casualty Care training and certification. Simultaneously, the JTS successfully transitioned from the Department of the Army to the DHA on August 5, 2018. Immediately after the JTS transfer, the Director, DHA, in coordination with the Military Services and the Office of the ASD(HA), led a comprehensive organizational assessment that was completed October 15, 2018. The JTS organizational assessment provided numerous recommendations. One of the key recommendations was the establishment and placement of the JTETD within the JTS, which is currently scheduled for initial operating capability no later than March 2019.

The JTETD will serve as the DoD's primary facilitator of entry into partnerships contributing to the development of knowledge, skills, and abilities competencies required for the delivery of full spectrum trauma care. The JTETD and subsequent partnerships will include civilian academic and large metropolitan hospitals to share partnership lessons learned. In accordance with the section 708 of the NDAA for FY 2017 Report to Congress, the JTETD, in collaboration with the Military Departments, will use a systematic approach in the development

25DE1635218

and application of goal-based criteria for entry into partnerships with civilian academic and metropolitan teaching hospitals, and establish performance metrics for these partnerships. This design will promote consistent, high-quality training. The JTETD Division chief will develop a comprehensive strategy that will address both hospital and prehospital partnerships, consistent with all applicable procedures. The National Association of Emergency Medical Technicians will be one of the organizations that will be considered for a more formal partnership.

Thank you for your interest in the health and well-being of our Service members, veterans, and their families

Sincerely,

ames N. Stewart

Assistant Secretary of Defense for Manpower and Reserve Affairs, Performing the Duties of the Under Secretary of Defense for

Personnel and Readiness

Congress of the United States Washington, DC 20515

December 4, 2018

The Honorable James N. Mattis Secretary of Defense 1000 Defense Pentagon Washington, DC 20301-1000

Dear Secretary Mattis:

As Members of Congress concerned about our warfighters who serve in harm's way, we write to ensure the timely establishment of the Department of Defense (DoD's) new Joint Trauma Education & Training Directorate. The importance of implementing DoD Instruction (DoDI) 1322.24 regarding Medical Readiness Training (MRT) promptly, efficiently, and effectively cannot be overstated.

We believe that military-civilian collaboration is critically important to advance trauma care for both military and civilian populations. In its 2016 report A National Trauma Care System, the National Academies of Science, Engineering, and Medicine (NASEM) concluded, in part: "A national strategy and joint military and civilian approach for improving trauma care is lacking, placing lives unnecessarily at risk. A unified effort is needed to address this gap and ensure the delivery of optimal trauma care to save the lives of Americans injured within the United States and on the battlefield."

DoD has partially recognized this need; there is currently a strategic partnership between DoD and the American College of Surgeons (ACS) to promote advances in hospital-based care, but no such partnership exists for prehospital care. A large majority of combat casualty deaths occur in the prehospital phase of care, so we are extremely concerned at the lack of a specific military-civilian partnership targeting this critical need. We understand that Tactical Combat Casualty Care (TCCC) has achieved unprecedented success in decreasing preventable combat deaths in military units that have received accurate TCCC training, but we are disturbed by reports highlighting inadequate training. For example, in the cover letter accompanying the September 2015 Joint Trauma System (JTS) White Paper entitled Establishing a DoD Standard for Tactical Combat Casualty Care (TCCC) Training, then-Director of JTS, Col. Kirby Gross, stated:

[TCCC] training is not being satisfactorily accomplished. The two US CENTCOM/Joint Trauma System assessments of prehospital trauma care in Afghanistan documented inconsistent or absent TCCC training in combat forces deployed to CENTCOM. Secondly, the Joint Trauma System Performance Improvement process has noted adverse casualty care events associated with failure to perform standard TCCC measures. These events occurred even in units that had reportedly been trained in TCCC as a result of misinformation provided during that training. Finally, recent reports in the media have noted that US Service Members have been exposed to inappropriate and potentially dangerous training events during courses that were intended to provide battlefield trauma care training. One physician lost his medical license in Virginia as a result. These occurrences document a clear opportunity for the DoD to improve in its methods of conducting TCCC training.

PRINTED ON RECYCLED PAPER

We agree that there is a clear opportunity for DoD to improve TCCC training, particularly, as DoDI 1322.24 establishes TCCC as the US military standard for battlefield trauma care. This action recognizes the critical need to standardize prehospital trauma care training across the US military, and we encourage DoD to use this opportunity to establish a strategic partnership to promote prehospital care.

Specifically, we urge the DoD to consider formalizing its relationship with the National Association of Emergency Medical Technicians (NAEMT) to establish an official strategic partnership to promote prehospital care. We are aware that NAEMT has worked with DoD's Committee on TCCC for over two decades to improve prehospital trauma care for both military and civilian victims. NAEMT currently provides TCCC training coordination and quality assurance services to more than 50 U.S. military sites, including sites in our states. NAEMT TCCC courses are endorsed by the American College of Surgeons and recommended by the Joint Trauma System. NAEMT has an extensive quality assurance framework in place, ensuring that instructors are appropriately trained and credentialed, and that the military training facilities used for TCCC training meet or exceed the minimal training center requirements. In addition, NAEMT courses offer the most cost-effective option for TCCC training, a key consideration as DoD implements TCCC training more broadly.

We believe a strategic partnership like this presents a "win-win" scenario. We appreciate your consideration and we look forward to your response.

Sincerely,

Rep. Scott DesJarlais, M.D.

Member of Congress

Kep. Michael C. Burgess, M.D.

Member of Congress

Rep. Austin Scott

Member of Congress

Rep. Paul Cook

Member of Congress

Rep. Seth Moulton Member of Congress

`5~ (de

Rep. Tom Cole

Member of Congress

Rep. Mike Coffman

Member of Congress

Rep. Vicky Hartzler

Member of Congress



Rep. Scott Tipton Member of Congress

Rep. Don Bacon Member of Congress

Rep. Ron Kind Member of Congress

Rep. Will Hurd Member of Congress Rep. Mike Gallagher Member of Congress

Rep. Susan Brooks Member of Congress

Rep. F. Jim Sensenbrenner, . Member of Congress

Rep. Vicente Gonzalez Member of Congress



SECRETARY OF DEFENSE 1000 DEFENSE PENTAGON WASHINGTON DC 20301-1000

8/2/2018

The Honorable Mike Crallagher U.S. House of Representatives. Washington, DC 20515

Dear Representative Gallaghers

I want to express my sincere appreciation for your commitment to safeguarding our Nation's competitive advantage as a co-sponsor of the Foreign Investment Risk Review Modernization Act (FIRRMA), included in this year's National Defense Authorization Act (NDAA)

As you are aware, strengthening and protecting critical national security intrastructure, technologies, and functions are vital to safeguarding our freedoms for the next generation. The updates FIRRMA provides to the Committee on Foreign Investment in the United States will help provide that protection. This success would not have been possible without your securing FIRRMA's inclusion as an amendment to the House Rules committee NDAA package, and your sustained engagement with your fellow Representatives during floor consideration.

In the months ahead I look forward to continuing to work closely with you of Wisconsin's role in our defense and additional efforts to strengthen our Nation's security.

Semper Fi,



THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON WASHINGTON, DC 20301-3010

化机合物 电线线线

The Honorable Mike Gallagher U.S. House of Representatives Washington, DC 20515

Dear Representative Gallagher:

Thank you for your December 14, 2017, letter to the Secretary of Defense regarding your concerns with the Department of Commerce (hereinafter "Commerce") aluminum trade investigation pursuant to section 232(b)(1)(A) of the Trade Expansion Act of 1962. I am responding on the Secretary's behalf.

We appreciate your views and have conveyed similar concerns to Commerce with respect to the potential for unintended consequences from U.S. import restrictions, including increased prices for American consumers of aluminum products and possible retaliation by U.S. foreign trade partners. I assure you that the Department of Defense has been working closely with Commerce and the Administration in expressing our views.

Thank you for your interest in these important matters and for your service to the success of our Warfighters. We appreciate your support for U.S. national defense and the U.S. defense industrial base. An identical letter has been sent to the other signatories of your letter.

Sincerely,

Ellen M. Lord

Congress of the United States Washington, DC 20515

December 14, 2017

The Honorable James Mattis Secretary of Defense 1000 Defense Pentagon Washington, D.C. 20301-1000

Dear Secretary Mattis:

We are writing to you regarding our concerns about the Commerce Department's recent 232 investigation on aluminum.

In April, the President directed the Department of Commerce to begin a "232 investigation" into the aluminum industry. This investigation requires the Department of Commerce, in consultation with other agencies, to assess whether the United States' dependence on aluminum imports impacts national security. If the Commerce Department concludes that our national security is impacted, the President has wide latitude to implement import restrictions, such as tariffs or quotas, on foreign aluminum.

As you know, the Department of Defense, as experts on national security issues, regularly conducts materials assessments for both essential military and private sector requirements. Those assessments are reported back to Congress. We know of no assessment of aluminum that has taken place in recent history, presumably because the Department of Defense has concluded that both military and private sector demand are sufficiently met with the current domestic capacity as well as the capacity of our allies.

We are unaware of the extent the Department of Commerce is consulting with the Department of Defense, and if the Department of Commerce is aware of these annual assessments. We remain concerned that the 232 investigation will result in import restrictions on aluminum. These restrictions may have vast unintended consequences including increased prices for American consumers of aluminum, and retaliation from foreign countries in the form of higher tariffs on American-made goods.

It is our hope that the Department of Defense will increase its engagement with the Department of Commerce, and work with the White House in order to ensure that the final report reflects the input of the Department of Defense's expertise on national security issues. We look forward to working with you on this issue.

PENTED ON MICHOLOGIC PARE

Sincerely,

Mike Gallagher

Member of Congress

OSD015597-17/CMD020534-17

Chenez Liz Cheney Member of Congress Member of Congress Mike Coffman Member of Congress Member of Congress Member of Congress Member of Congress

Frank A. LoBiondo Member of Congress

Austin Scott Member of Congress

Michael R June

Michael R. Turner Member of Congress



OFFICE OF THE UNDER SECRETARY OF DEFENSE 3000 DEFENSE PENTAGON WASHINGTON, DC 20301-3000

ACQUISITION, TECHNOLOGY, AND LOGISTICS

JUL 1 7 2017

The Honorable Mike Gallagher U.S. House of Representatives Washington, DC 20515

Dear Representative Gallagher:

Thank you for your June 23, 2017, letter requesting to exempt certain aluminum materials and their applications (e.g., primary-aluminum and ingot milled into rolled can sheets for food packaging and related uses) from the ongoing Department of Commerce (DOC) aluminum trade investigation, pursuant to section 232(b)(1)(A) of the Trade Expansion Act of 1962. The Department of Defense is providing DOC with defense demand information for aluminum, but defers to DOC for consideration of exemptions to their investigation.

Your interest in safeguarding our national manufacturing industrial base is greatly appreciated. An identical response has been sent to all the signatories of your letter.

Sincerely,

James A. MacStravic

Performing the Duties of the Under Secretary of Defense for Acquisition, Technology, and Logistics

6512667972-17

Congress of the United States

Washington, DC 20515

June 22, 2017

The Honorable Wilbur Ross, Secretary, Department of Commerce 1401 Constitution Ave, NW Washington, DC 20230 The Honorable General James Mattis Secretary, Department of Defense 1400 Defense Pentagon Washington, DC 20301-1400

Dear Secretaries Ross and Mattis;

We are writing in regards to the *Presidential Memorandum for the Secretary of Commerce*, dated April 27, 2017, which directs an "investigation under section 232(b)(1)(A) of the Trade Expansion Act of 1962 (the "Act") (19 U.S.C. 1862(b)(1)(A)) to determine the effects on national security of aluminum imports."

We appreciate the President's commitment to America's security and his commitment to assuring a level playing field for American manufacturing. However, we are concerned that the scope of this investigation could include aluminum that has no national security application, such as rolled can sheet and the primary aluminum which is processed into food and beverage cans and bottles, lids, and closures. Primary aluminum used in can sheet is largely imported because U.S. aluminum smelters produce other alloys more profitably. The manufacturers of aluminum food and beverage cans and bottles use recycled aluminum, scrap aluminum and imported primary aluminum. Our dependence on the imports of primary aluminum is not recent. In fact, the U.S. has been in this deficit trade position with these products since the end of World War II.

Inclusion of rolled can sheet and primary aluminum and ingot for food and beverage containers, lids, and closures in this investigation could yield import restrictions or tariffs on these products – a result that would not increase their availability in the U.S., but would necessarily impose additional costs to American end-users, and American consumers. We understand that this consequence would be unintended. Not all aluminum is the same, and the distinction of rolled can sheet, and primary and ingot used for food and beverage containers, lids and closures versus other aluminum is very important. Specifically, we would like to see the following products excluded from 232 consideration:

- Aluminum cansheet bodystock 7606,12,3045;
- Aluminum can lid stock 7606.12,3055;
- Other aluminum cansheet 7606.12.3090;
- Aluminum used beverage container scrap 7602.00.0030
- Aluminum waste and scrap other than used beverage container scrap 7602,00,0090
- Aluminum slugs: 7616.99 and 7606.91; and
- Low purity (non-military) aluminum ingot 7601.10.6000.

We hope that your investigation under Section 232 will be limited in scope to only products that are used for national security applications and not include the products listed above. We look forward to working with you on this matter. Please have your staff contact Jeremy Lippert with Rep. Coffman at 202-225-7882, or Hana Greenberg with Rep. Kind at 202-225-5506 if we can be of any additional assistance.



PRINTED ON RECYCLED PAPER

Sincerely,

Mike Coffman

Patrick McHenry
Member of Congress

Scott Tipton Member of Congress

Member of Congress

David Scott Member of Congress

Jan Vargas Member of Congress

Luke Messer Member of Congress Ron Kind

Ron Kind Member of Congress

Steve Womack Member of Congress

olong fambom

Doug Lamborn Member of Congress

Bob Goodlatte Member of Congress

Walter B. Jones
Member of Congress

Ed Perimutter Member of Congress

Member of Congress Member of Congress John Rutherford Member of Congress Member of Congress Member of Congress Member of Congress Lit Cheney Member of Congress Member of Congress Paul Cook Member of Congress Member of Congress er of Congress Member of Congress Member of Congress Member of Congress

Member of Congress

Proce 3. Napolitano
Viember of Congress

Longerd Lance Membra in Compress

Michael R June

Michael Earner Member of Congress

M. moet of Congress

Robert E. Latta Member of Congress

Member of Congress

Member of Congress

ZKenny Marchant

Member of Congress

Member of Congress

TortRooney
Member of Congress

Austin Scott Member of Congress Doug Collins Member of Congress

Glenn Grothman Member of Congress



DEPUTY SECRETARY OF DEFENSE 1010 DEFENSE PENTAGON WASHINGTON, DC 20301-1010

APR 2 8 2017

The Honorable Mike Gallagher U.S. House of Representatives Washington, DC 20515

Dear Representative Gallagher:

On behalf of Secretary Mattis, thank you for your and your colleagues' April 10, 2017, letter to the Department of Defense expressing your support of the Department's approach to provide reliable, competitive, and cost-effective access to space.

The Air Force continues to work closely with its industry partners through public-private partnerships to protect the taxpayers' investment into the next generation of domestic launch systems. A draft Request for Proposal (RFP) was posted for review on March 14, 2017, and the Air Force is considering industry's feedback as they prepare for release of the final RFP. We anticipate the final RFP will be released in Summer 2017.

Thank you for your continued contributions to our Nation's defense and the bipartisan support of the Department of Defense and United States Air Force. An identical letter has been sent to the other signatories on your letter.

Lycotary)



Congress of the United States Washington, DC 20515

April 10, 2017

The Honorable James Mattis Secretary of Defense 1000 Defense Pentagon Washington, DC 20301-1000

Dear Secretary Mattis:

We write in support of the Department of Defense and the Air Force's approach to provide reliable, competitive, and cost-effective access to space. Allowing competition rather than directing government investment to only one technology or company will result in a better, more capable launch vehicle that will best serve national security, and ultimately yield better value and services for taxpayers' investment and save costs.

In its budget for Fiscal Year 2017, the Air Force requested \$1.2 billion across five years to invest in domestic launch systems. The end goal of these investments is two long-term domestic, commercially viable launch providers that meet national-security space requirements. This approach ensures the United States maintains its policy of assured access to space, enabling our ability to meet evolving space threats. We write to you in support of the Air Force's request and focus on the end-goal of complete, robust launch systems. Critical funding should not be restricted to specific components, such as a first-stage engine.

Congress' direction over the past several years has been clear: to end U.S. dependence on the Russian-made RD-180 and create a competitive environment that will continue the nation's policy of assured access to space while reducing the cost of launch. In the FY 2017 National Defense Authorization Act, Congress supported funding for both engine development and launch-system investment.

Investing in the entire launch system through government and industry cost-share partnerships – rather than a specific component – is the fastest, safest, and most affordable way for the taxpayer to achieve these objectives. Last year, then-Under Secretary of Defense for Acquisition, Technology, and Logistics Frank Kendall shared the same sentiment when he testified that, "Assured access to space requires end-to-end space launch service and not just a rocket engine. As many Department of Defense witnesses have testified to this and other congressional committees, simply replacing the RD-180 with a new engine will not deliver the performance of the current design." Under Secretary Kendall went on to note, "The Department would strongly prefer to not have to pay for the development of an RD-180 engine replacement that would benefit only one launch service provider."

The Air Force's investment into the next generation of launch vehicles will ensure the United States maintains a robust launch industry with at least two healthy providers and without pre-selecting a technology. Restricting funding only for a domestic engine will result in higher costs for the taxpayer and risks delays in ending use of the RD-180 engine.

Cost-effective investments by the government to ensure reliable access to space are all the more vital to national security in the face of growing threats. Evolving threats from countries such as China and Russia highlight the importance of space and the need for U.S. space superiority for our national security. In 2013 and 2014, Russia and China launched satellites demonstrating new capabilities to threaten U.S. or allied nations' satellites. These threats are real, they are rapidly evolving, and our



ability to launch new, more resilient assets into orbit requires reliable, capable and cost-effective systems.

We appreciate your attention to this matter, and hope you will continue promoting competition and maintaining our nation's assured access to space by supporting the Air Force request to invest in domestic launch systems.

Sincerely,

Member of Congress

Pete Sessions

PETE SESSIONS Member of Congress

tal chuto STEVE CHABOT

Member of Congress

ROB BISHOP Member of Congress

CATHY MCMORRIS RODGE'S

Member of Congress

DOUG L. LAMBORN

Member of Congress

Member of Congress

CHUCK FLEISCHMANN Member of Congress

ADAM SMITH Member of Congress

DIANA DEGETTE Member of Congress

HENRY C. "HANK" JOHNSON, JR.

Member of Congress

ED PERLMUTTER

Member of Congress

DENNY HECK

Member of Congr

DEKEK KILMER

Member of Congress

FILEMON VELA

SETH MOULTON Member of Congress David Webster
DANIEL WEBSTER
Member of Congress

Wen Buck

KEN BUCK

Member of Congress

Member of Congress

Member of Congress

And Andrews and Anthropological State of the Control of the Contro

CONTRACTORS OF A REGISSION SINGS VALUES:

Ci.S., Pous of Apri antalmy

@dashington, 79, 20515, 6005.

OCH BURANA CER ICCOLOS (SASSESS

January 23, 2017

The section of the management of the section of the hadan yan biri salah salah salah

and the contract of the contract of the

The Honorable James Mattis Secretary of Defense Washington, D.C. 20301

Dear Mr. Secretary:

Attached is the list of Members of the Committee on Armed Services who are authorized to travel within the United States and territories during the 115th Congress involving matters of concern to the committee and the Department of Defense.

The military departments are requested to publish travel orders for the period involved and to make such arrangements as may be required, individually or collectively, for such itinerary and for such travel as may be necessary.

As provided by title 31, United States Code, section 1108g, transportation and the payment for actual and necessary expenses is authorized. Such travel related expenses should be limited to the rates as published in the Per Diem Travel Allowance Committee regulations.

Sincerely,

William M. "Mac" Thornberry

Chairman

WMT:rar Enclosure 16 Aug 17



OSD010118-17/CMD013616-17

HOUSE ARMED SERVICES COMMITTEE MEMBERS OF CONGRESS AUTHORIZED BLANKET TRAVEL ORDERS DURING THE 115TH CONGRESS March 2017

William M. "Mac" Thomberry, Chairman (TX)

Walter B. Jones (NC)

Joe Wilson (SC)

Frank A. LoBiondo (NJ)

Rob Bishop (UT)

Michael R. Turner (OH)

Mike Rogers (AL)

Trent Franks (AZ)

Bill Sluster (PA)

K. Michael Conaway (TX)

Doug Lamborn (CO)

Robert J. Wittman (VA)

Duncan Hunter (CA)

Mike Coffman (CO)

Vicky Hartzler (MO)

Austin Scott (GA)

Mo Brooks (AL)

Paul Cook (CA)

Jim Bridenstine (OK)

Brad R. Wenstrup (OH)

Bradley Byrne (AL)

Sam Graves (MO)

Elise Stefanik (NY)

Martha McSally (AZ)

Steve Knight (CA)

Steve Russell (OK)

Scott DesJarlais (TN)

Ralph Lee Abraham (LA)

Trent Kelly (MS)

Mike Gallagher (WS)

Matt Gaetz (FL)

Don Bacon (NB)

Jim Banks (IN)

Liz Cheney (WY)

Adam Smith, Ranking Member (WA)

Robert A. Brady (PA)

Susan A. Davis (CA)

James R. Langevin (RI)

Rick Larsen (WA)

Jim Cooper (TN)

Madeleine Z. Bordallo (GU)

Joe Courtney (CT)

Niki Tsongas (MA)

John Garamendi (CA)

Jackie Speier (CA)

Marc A. Veasey (TX)

Tulsi Gabbard (HI)

Beto O'Rourke (TX)

Donald Norcross (NJ)

Ruben Gallego (AZ)

Seth Moulton (MA)

Colleen Hanabusa (HI)

Carol Shea-Porter (NH)

Jacky Rosen (NV)

A. Donald McEachin (CA)

Salud O. Carbajal (CA)

Anthony G. Brown (MD)

Stephanie N. Murphy (FL)

Ro Khanna (CA)

Tom O'Halleran

Thomas R. Suozzi

(vacancy)