

**SECURING THE SKIES:
ADDRESSING UNAUTHORIZED
DRONE ACTIVITY OVER U.S.
MILITARY INSTALLATIONS**

HEARING

BEFORE THE
SUBCOMMITTEE ON MILITARY
AND FOREIGN AFFAIRS
OF THE
COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
ONE HUNDRED NINETEENTH CONGRESS
FIRST SESSION

APRIL 29, 2025

Serial No. 119–22

Printed for the use of the Committee on Oversight and Government Reform



Available on: *govinfo.gov*
oversight.house.gov or
docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

60–196 PDF

WASHINGTON : 2025

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio	GERALD E. CONNOLLY, Virginia, <i>Ranking</i>
MIKE TURNER, Ohio	<i>Minority Member</i>
PAUL GOSAR, Arizona	ELEANOR HOLMES NORTON, District of
VIRGINIA FOXX, North Carolina	Columbia
GLENN GROTHMAN, Wisconsin	STEPHEN F. LYNCH, Massachusetts
MICHAEL CLOUD, Texas	RAJA KRISHNAMOORTHY, Illinois
GARY PALMER, Alabama	RO KHANNA, California
CLAY HIGGINS, Louisiana	KWEISI MFUME, Maryland
PETE SESSIONS, Texas	SHONTEL BROWN, Ohio
ANDY BIGGS, Arizona	MELANIE STANSBURY, New Mexico
NANCY MACE, South Carolina	ROBERT GARCIA, California
PAT FALLON, Texas	MAXWELL FROST, Florida
BYRON DONALDS, Florida	SUMMER LEE, Pennsylvania
SCOTT PERRY, Pennsylvania	GREG CASAR, Texas
WILLIAM TIMMONS, South Carolina	JASMINE CROCKETT, Texas
TIM BURCHETT, Tennessee	EMILY RANDALL, Washington
MARJORIE TAYLOR GREENE, Georgia	SUHAS SUBRAMANYAM, Virginia
LAUREN BOEBERT, Colorado	YASSAMIN ANSARI, Arizona
ANNA PAULINA LUNA, Florida	WESLEY BELL, Missouri
NICK LANGWORTHY, New York	LATEEFAH SIMON, California
ERIC BURLISON, Missouri	DAVE MIN, California
ELI CRANE, Arizona	AYANNA PRESSLEY, Massachusetts
BRIAN JACK, Georgia	RASHIDA TLAIB, Michigan
JOHN MCGUIRE, Virginia	
BRANDON GILL, Texas	

MARK MARIN, Staff Director
JAMES RUST, Deputy Staff Director
MITCH BENZINE, General Counsel
KAITY WOLFE, Deputy Director for Oversight
GRAYSON WESTMORELAND, Senior Professional Staff Member
ALEX PHARES, Professional Staff Member
MALLORY COGAR, Deputy Director of Operations and Chief Clerk

CONTACT NUMBER: 202-225-5074

JAMIE SMITH, Minority Staff Director

CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON MILITARY AND FOREIGN AFFAIRS

WILLIAM TIMMONS, South Carolina, Chairman

MICHAEL TURNER, Ohio	SUHAS SUBRAMANYAM, Virginia <i>Ranking</i>
MICHAEL CLOUD, Texas	<i>Member</i>
ANDY BIGGS, Arizona	STEPHEN LYNCH, Massachusetts
BYRON DONALDS, Florida	KWEISI MFUME, Maryland
ANNA PAULINA LUNA, Florida	ROBERT GARCIA, California
ELI CRANE, Arizona	GREG CASAR, Texas
JOHN MCGUIRE, Virginia	<i>Vacancy</i>

C O N T E N T S

	Page
Hearing held on April 29, 2025	1

WITNESSES

Rear Admiral Paul Spedero, Jr., Vice Director for Operations, J3, Joint Chiefs of Staff (JCS), U.S. Department of Defense (DoD)	
Oral Statement	5
Mr. M. Roosevelt Ditlevson, Acting Assistant Secretary of Defense, Homeland Defense and Hemispheric Affairs, U.S. Department of Defense (DoD)	
Oral Statement	6
<i>Written opening statements and bios are available on the U.S. House of Representatives Document Repository at: docs.house.gov.</i>	

INDEX OF DOCUMENTS

- * Article, Markets and Markets, “Autonomous Ascent, How AI is Reshaping the Future of UAV Industry”; submitted by Rep. Biggs.
 - * Article, *The Wall Street Journal*, “Mystery Drones Swarmed a U.S. Military Base for 17 Days”; submitted by Rep. Biggs.
 - * Article, The Washington Times, “What We Know About the Langley Air Force Base Drone Incident”; submitted by Rep. Biggs.
 - * Advisory, “Application of Federal Laws to the Acquisition and Use of Technology to Detect Mitigate UAS”; submitted by Rep. McGuire.
- Documents are available at: docs.house.gov.*

ADDITIONAL DOCUMENTS

- * Questions for the Record: to Mr. Arel; submitted by Rep. Timmons.
 - * Questions for the Record: to Rear Admiral Spedero; submitted by Rep. Crane.
 - * Questions for the Record: to Rear Admiral Spedero; submitted by Rep. McGuire.
- These documents were submitted after the hearing, and may be available upon request.*

SECURING THE SKIES: ADDRESSING UNAUTHORIZED DRONE ACTIVITY OVER U.S. MILITARY INSTALLATIONS

Tuesday, April 29, 2025

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON MILITARY AND FOREIGN AFFAIRS
Washington, D.C.

The Subcommittee met, pursuant to notice, at 2:13 p.m., Room HVC-210, U.S. Capitol Visitor Center, Hon. William Timmons, [Chairman of the Subcommittee] presiding.

Present: Representatives Timmons, Cloud, Biggs, Luna, McGuire, Subramanyam, and Lynch.

Mr. TIMMONS. This hearing of the Subcommittee on Military and Foreign Affairs will come to order. I would like to welcome everyone. Without objection, the Chair may declare a recess at any time. I recognize myself for the purpose of making an opening statement.

Thank you for joining us today as we discuss one of the most complex and serious threats to our national security, the unauthorized use of unmanned aerial systems, or UAS, over U.S. military installations and sensitive sites. In recent years, we have seen a surge in drone incursions over military installations across the country.

In 2024, the Department of Defense stated that there are more than one million drones registered in the United States and estimated that there are more than 8,500 drones flown legally across the country every day. I have even seen some of these drone incursions firsthand during my time in the South Carolina Air National Guard.

However, these incursions are not from hobbyists being blown off course. The multitude of drones reported flying over bases in the past several years revealed a coordinated effort by our adversaries to collect valuable intelligence and surveillance of some of our most sensitive military equipment.

These incursions often are designed to disrupt important trainings and create chaos for a number of reasons. No. 1, base commanders have inadequate or nonexistent monitoring capabilities; two, a near total lack of counter-drone capabilities; three, unclear standard operating procedures to guide base commanders' responses and decisionmaking; and finally, four, ambiguous legal authorities both on and off base.

This threat is magnified by the complex regulatory and prosecutorial framework that was patched together by the previous Administration in what I would argue is a poor attempt to address this issue. Right now, the Department of Defense, Federal Aviation Administration, Intelligence Community, Department of Justice, and Department of Homeland Security are all involved in some aspects of the counter-UAS efforts. As a result, there is no agency with primary authority on countering drone incursions, leading to confusion and, more importantly, gaps on how to identify and mitigate this threat.

This interagency failure was on full display last winter when hundreds of drones were spotted in the skies above New Jersey and other parts of the Northeast. After several temporary flight restrictions and mass confusion among state, local, and Federal partners, the Biden Administration provided the public no answers to what was happening above them. However, with only a few weeks of the current Administration taking office, they revealed that the drones over New Jersey were actually authorized by the FAA. This instance raises multiple questions as to why the previous Administration left the American people in the dark for over a month when they knew the simple truth.

Another notable incident occurred at Langley Air Force Base in December 2023. Over 17 days, unidentified drones repeatedly breached our sensitive military airspace, one of America's critical installations. The F-22 Raptor squadrons were moved to alternate bases to lessen exposure, and discussions were initiated on installing physical countermeasures.

These are not isolated incidents. In February, the Commander of NORAD and NORTHCOM testified to Congress that there were over 350 detections of drones at 100 different military installations last year alone. Additionally, since 2023, two Chinese nationals have been arrested for illegally flying drones over military installations to conduct surveillance. One of these individuals was caught attempting to flee the U.S. and return to China with sensitive footage he had recorded.

Today, this Committee will hear from officials from the Department of Defense on what the Trump Administration is doing to help combat this issue and bring an end to these illegal drone incursions. We must demand full accountability, expedited technological upgrades, and enhanced oversight to safeguard our sovereignty and ensure that our military remains unexposed to foreign surveillance and potential threats. I am hopeful that our witnesses here today have suggestions on how Congress can help empower the right Federal agencies to combat this problem and secure the skies above our military bases.

I now recognize Ranking Member Subramanyam for the purpose of making an opening statement.

Mr. SUBRAMANYAM. Thank you, Mr. Chairman. Thank you for holding this important hearing, and thank you to our witnesses for being here today and for your service to our country and to making our airspace safe.

It is clear that UAS is an issue right now. It is the future of warfare from the war in Ukraine to our own military bases in the continental United States. We are seeing real time that UAS are rede-

fining how battles are fought and how intelligence is gathered. I believe it has been 350 drones that have been reported in the last year, over 100 different military installations. That is 350 different potential national security breaches that we know of. These include highly sensitive sites such as nuclear facilities and major military bases, and that is a huge threat to our national security and the lives of our service members. And unfortunately, you know, our lack of coordinated effective response needs to be addressed immediately. And I know everyone here today wants to work on it and is planning on working on it.

And so, we are familiar with this issue in my home state, in the Commonwealth of Virginia. In December 2023, service members at Langley Air Force Base in Virginia saw drones hovering over their airspace for 17 days. And Langley, for those who do not know, is home to key national security assets like the F-22 Raptor stealth fighter, and it plays an important role in keeping us safe here in our Nation's capital. And so, we also have some important naval assets in that area too.

And, you know, these drones demonstrated complicated aerial maneuvers and did not just broadcast on known frequencies, suggesting that they were not just a local hobbyist making an innocent mistake. As far as we can tell in Congress, there was and still is not a cohesive or coordinated plan for how we are going to deal with this, but maybe we can learn more today about what is happening now and what we can do moving forward.

You know, our job on this Committee is to find answers to questions, and I have a lot. You know, who was piloting these drones, for instance? Were these criminal actors? Are these foreign adversaries? Are they simply local hobbyists with advanced capabilities? I am not sure about that, but maybe that is the case. And what are they doing? Are they gathering intelligence? Are they probing for weaknesses? Are they planning an attack? And finally, what is our plan for dealing with them safely and effectively because these UAS are a clear and present danger to our national security, and we need to have a plan to counter them.

There are several areas I would like to focus on today. The first is counter-drone authorities. Right now, the U.S. law allows the Department of Energy, Justice, Defense, and Homeland Security to detect and respond to drone activities in certain situations such as nuclear facilities, for instance, missile defense assets, or other covered facilities, but only around half of all military installations actually fall under this definition of covered facility, which is why I think this may be something we should look at for change.

The second is counter-drone technologies. You know, it is not just as simple as shooting them down, as we know. You know, there are homes and businesses and parks near bases like Langley, and people live there. Children play there. Shooting down drones could endanger people in these communities, especially if we do not know what payloads the drones may carry. And a missed shot could also pose a threat to commercial air traffic as well. And so, you know, we need to find a way to safely counter some of these incursions.

And we have other technologies at our disposal like jamming and disrupting and even taking over unknown or hostile drones, but there is a lot of work to do to develop these capabilities. And some

of that work actually takes place in my district in northern Virginia.

And, you know, with that said, I do not know of a silver bullet, and so it is going to take a coordinated effort, I think, at the state, local, and Federal level, and so we are all going to have to work together because everyone has got different jurisdictions. And I would like to, on that front, see if we can work together and maybe have some sort of task force in place so that information is easily gathered and where everyone is up to date on the latest technology, as well as the best practices.

And so, this is a very timely hearing on an important issue, and I want to work with my colleagues on both sides of the aisle to come up with a plan to protect our military bases and protect the American people, so I yield back.

Mr. TIMMONS. Thank you for that.

I am pleased to welcome an expert panel of witnesses for today's discussion. I would first like to welcome Rear Admiral Paul Spedero, the Vice Director for Operations, or J3, for the Joint Chiefs of Staff.

I would also like to welcome Mr. Mark Ditlevson, who is the current Acting Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs.

Due to unforeseen circumstances, the FAA is no longer testifying at today's hearing, but they have committed to answering in writing any questions that our Members have. If any Member has questions they would like to submit to the FAA following this hearing, please get them to staff for the FAA to answer.

Now, we are going to administer the oath to the witnesses. Pursuant to Committee Rule 9(g), the witnesses will please stand and raise their right hand.

Do you solemnly swear or affirm that the testimony that you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

[Chorus of ayes.]

Mr. TIMMONS. Thank you. Please take your seat. Let the record show that the witnesses answered in the affirmative.

We appreciate you being here today and look forward to your testimony. Let me remind the witnesses that we will have read your written statement, and it will appear in full in the hearing record. Please limit your oral statement to 5 minutes.

As a reminder, please press the button on the microphone in front of you so that it is on and the Members can hear you. When you begin to speak, the light in front of you will turn green. After 4 minutes, the light will turn yellow. When the red light comes on, your 5 minutes have expired, and we would ask that you please wrap up.

I now recognize Rear Admiral Spedero for his opening statement.

**STATEMENT OF REAR ADMIRAL PAUL SPEDERO JR.
VICE DIRECTOR FOR OPERATIONS, J3
JOINT CHIEFS OF STAFF (JCS)
U.S. DEPARTMENT OF DEFENSE (DoD)**

Admiral SPEDERO. Good afternoon, Chairman Timmons, Ranking Member Subramanyam, Committee Members, ladies and gentle-

men. Thank you for the opportunity to be here today, and thank you for your support and your oversight. Admittedly, several of my opening comments will echo those of the Chairman and the Ranking Member.

The rapid emergence, proliferation, and employment of unmanned systems has fundamentally changed the way that both professional militaries, as well as terrorist organizations, conduct warfare. Over the last few years, we have seen the employment of unmanned systems, in particular unmanned aerial systems, in every major conflict, from the Russia-Ukraine war to Iran's attacks on Israel and attacks against U.S. bases and ships across the Middle East. And most tragically, an Iranian-supported militant group successfully employed a one-way attack drone on Tower 22 in Jordan, killing three U.S. service members, and wounding 40, on January 27, 2024.

Here in the homeland, as Assistant Secretary Ditlevson will note in his opening remarks, the mass drone incursions over Joint Base Langley-Eustis in December 2023 reminded us that the homeland is no longer a sanctuary. And should our adversary choose to employ drones for surveillance or even attack, we would not be prepared to adequately defend our homeland and only marginally capable to defend our military installations. The incursions over Joint Base Langley-Eustis were not the first, they have not been the last, but they were the longest and the largest series of incursions that we have seen to date.

In the comprehensive review of that event, as well as in the actions we took in follow-on incursions like those that occurred over Plant 42 in Palmdale, California, and over Picatinny Arsenal and Naval Weapons Station Earle in New Jersey, have resulted in improvements. But more action is needed, and the Joint Force has made counter-UAS our priority line of effort.

We are now better prepared to respond to incursions with the designation of Commander of U.S. Northern Command and Commander of U.S. Indo-Pacific Command as the operational synchronizers in their respective areas of responsibility. Last year and within weeks of being assigned this role, General Guillot, the Commander of U.S. Northern Command, released a comprehensive commander's assessment that has served as a roadmap to building the necessary command and control and standard operating procedures to address the drone threat.

Over the last year, we have also invested in education and training against this threat. NORTHCOM has been a central driving force for the work being done by several organizations in partnership with industry to deliver the domain awareness and counter-UAS systems that we require. And last, we are progressing well in our completion of the counter-UAS tasks assigned to us in the Fiscal Year 2025 NDAA.

We appreciate your continued support and your oversight. Thank you for the opportunity to be here today, and I will now pass to Secretary Ditlevson.

**STATEMENT OF MARK ROOSEVELT DITLEVSON
ACTING ASSISTANT SECRETARY OF DEFENSE
HOMELAND DEFENSE AND HEMISPHERIC AFFAIRS
U.S. DEPARTMENT OF DEFENSE (DoD)**

Mr. DITLEVSON. Chairman Timmons, Ranking Member Subramanyam, and distinguished Members of the Committee, thank you for the opportunity to speak here today. The events of December 2023 at Joint Base Langley-Eustis served to focus and energize DoD's counter-small UAS efforts in the homeland. During the event, DoD struggled to address the incursions in a timely and effective fashion, owing at least in part to challenges within the DoD and our ability to implement a relatively untested interagency coordination process. To some extent, those challenges from JBLE still exist. However, we have worked since then to improve and refine our processes and coordination efforts, and we have seen improvements in subsequent responses.

I can assure the Committee that the Department is as frustrated by these events as you are. However, we cannot simply focus on looking back and waste precious resources. As a department, we act, we review that action, we adjust, and we move out. Today, I am here to tell you that we are continuing to move out. I am confident that we are in a stronger position to defend DoD installations today than we were in December 2023.

We are fighting this threat on three fronts, internal process reviews, generating better domain awareness, and clarifying commanders' authority in legislation. Internally, we must focus on the ability to provide response at the speed of relevance. The designation of USNORTHCOM and USINDOPACOM late last year as the counter-UAS operational synchronizers in their respective areas of the homeland was an essential step. We have developed more streamlined interagency coordination consistent with section 130i.

We are also conducting a comprehensive review, as requested in the Fiscal Year 2025 NDAA section 925 and, where necessary, consolidating and updating DoD policy. This is an effort long overdue, and it provides us with direction and momentum.

Last, working with our interagency partners, like our colleagues from the FAA, we have enabled DoD to sponsor facilities which provide a critical mission to DoD but are not directly DoD facilities or assets.

Second, generating better domain awareness is essential to developing an understanding of what is flying in our airspace and how to separate the negligent from the nefarious. This is the fundamental issue we saw at Langley in New Jersey. DoD is working through venues like the Joint Rapid Acquisition Cell, the JRAC, to rapidly acquire the right equipment and to give commanders better tools to understand the operating environment and the ability to effectively conduct non-kinetic and kinetic mitigations. The Commander of USNORTHCOM phrased it this way in his posture hearing in February: "You cannot defeat what you cannot see."

On the legislative front, we continue to engage with Members of Congress to seek modest but important refinements to DoD's counter-UAS authorities under section 130i. Our legislative proposal is intended to allow the Department to protect additional locations and missions, add greater stability for long-term planning

and resource allocation within the Department, and facilitate improved understanding and cooperation among the U.S. interagency and local partners.

Ultimately, I believe we need to address all these issues with end users in mind, our installation commanders and the security personnel charged with the duties to protect our installations, our operations, and ultimately our personnel.

Last, the President of the United States has issued several executive orders directing the Department of Defense to take all appropriate and lawful measures to ensure the complete operational control of the border. The Department, in turn, is responding by preparing the path for employment of counter-sUAS activities along the border, both in support of DoD interests and in support of DHS as the lead Federal agency. As the operational environment, legislation, and threats evolve, policy must adapt to ensure DoD's ability to continue to advance our national defense objectives remains.

Mr. Chairman, Ranking Member Subramanyam, and distinguished Members of the Committee, in conclusion, the homeland continues to face increased and evolving threats from UAS. To address these challenges requires a whole-of-government approach and a unified effort. We must modernize the ability to assess the threat, determine its weaknesses, and acquire and deploy counter-measures. Thank you for the support of Congress and for your continued commitment in support of the Department of Defense. I look forward to your questions.

Mr. TIMMONS. Thank you. I now recognize myself for 5 minutes.

Rear Admiral SPEDERO, how many drone incursions have taken place over U.S. military installations over the past 2 years? We got the number last time we had a briefing of 350, but have they grown? Or what is the current data you are willing to share?

Admiral SPEDERO. Yes, so the exact number I would be happy to share in a classified setting, but I can tell you that it has grown.

Mr. TIMMONS. I am actually curious. Why did we get the 350 number in an unclassified setting? That was one of the questions I had.

Admiral SPEDERO. It is a great question, sir.

Mr. TIMMONS. OK.

Admiral SPEDERO. Yes.

Mr. TIMMONS. Fair enough. All right. Well, let us do this. Can you discuss procedures that DoD has in place for a base commander when the base commander gets reports of an unauthorized drone incursion?

Admiral SPEDERO. Yes, so currently, there is a standard operating procedure that has been published by the Commander of U.S. Northern Command. So, each base has been provided that standard operating procedure. The expectation is they will respond in accordance with that.

Mr. TIMMONS. When was that created?

Admiral SPEDERO. It was just published here recently, within the last month.

Mr. TIMMONS. OK.

Admiral SPEDERO. It was finalized and published.

Mr. TIMMONS. So, what percent of base commanders have any technology to actually track drones as opposed to just, ooh, I saw a drone, and then you report it?

Admiral SPEDERO. Yes, so the capabilities at each base is varied. Again, the specifics for the individual locations would be better in a classified setting, but it is not comprehensive, I can tell you that. It is not sufficient and, again, varies from base to base, from very little to somewhat more comprehensive.

Mr. TIMMONS. Is that something that Congress can help with authorizations and appropriations to get additional resources? I would feel that most bases should have, at the very least, the ability to track. Whether they have countermeasures is a different thing. But is that something that you all need? You need additional money?

Admiral SPEDERO. Yes, sir, absolutely. I think the development fielding the acquisition distribution of domain awareness sensors is the critical first step. It is not the only thing. Obviously, we need a method to exert command and control so that we can build a common operating picture because it will take layers of different sensors because one sensor may be better against certain UAVs and certain flight profiles, and you may have to rely on different sensors to round out the picture. So, being able to fuse all that together to get the complete picture will be necessary. And then, as you mentioned, getting to a point where we can actually respond, that is an entirely next investment that needs to be made.

So, yes, we do need more sensors. We are addressing the shortfall right now with the fielding of flyaway kits. So, these will be kits that will be available for bases that have very limited capability to detect on their own and build domain awareness. And should they have an incursion that they are unable to resolve, they would solicit the help from Commander of the U.S. Northern Command, and this flyaway kit, as well as expertise and additional resources that would be required would be immediately deployed to that location.

Mr. TIMMONS. So, I guess, resources are probably fairly easy, and you all are going to work on telling us what you actually need from a technology perspective, but the other side is the authority. So, I mean, does a base commander have clear authorities, what they can and cannot do relative to whether the drone is in their airspace or just outside the airspace? And is that as big or bigger of a problem?

Admiral SPEDERO. So, all of our installations have the authority that is afforded them under the standing rules of engagement and the standing rules for the use of force. You know, in those rules, if they are—can establish that there is hostile intent or hostile act—then they not only have the authority, but they have the absolute right and responsibility to respond appropriately to protect themselves, forces, as well as DoD property. So, those are standing rules that they have.

Now, being able to discern hostile intent and hostile act, as referred to in the opening comments, may be very challenging. Is this negligent activity being conducted by someone just flying a drone irresponsibly, whether that is a recreational enthusiast or it is someone that is using a drone for commercial aspects? So, it can be a challenge here in the homeland to determine that.

Mr. TIMMONS. So, a base commander has the authority to, for example, arrest a Chinese national that is a quarter mile off base?

Admiral SPEDERO. He does not have the authority to detain someone that is off base. He would have to coordinate with local law enforcement to apprehend someone that is operating a drone outside of the base. Now, I know Secretary Ditlevson will talk about 130i authorities, which is something that we really do want to talk about today because I think it is important. But under 130i authorities, there is some additional room to respond. For a covered facility, merely the presence of that drone conducting unauthorized surveillance or suspected of conducting unauthorized surveillance or interfering with operations, as you referred to in your opening statement, about the interference with F-22 operations, that would meet the standard for a response rather than having to determine hostile intent or hostile act.

Mr. TIMMONS. Thank you for that. My time has expired.

I now recognize the gentleman from Virginia, Mr. Subramanyam, for 5 minutes.

Mr. SUBRAMANYAM. Thank you, Mr. Chairman.

I wanted to go back to something I mentioned a couple of times, which is what is a covered facility and a not covered facility? And Rear Admiral Spedero, if you are not a covered facility, what does that mean? Does that impair your ability to respond? And what do covered facilities have that noncovered ones do not?

Admiral SPEDERO. Yes, so if you are not covered, you can request to be covered, but you would have to meet the criteria to become a covered facility, and that is one of the problems with the 130i authorization is meeting the criteria for covered. An example of this would be Luke Air Force Base where F-35 training takes place for roughly three-quarters of those that fly F-35s, and it is not a covered facility because training facilities are not covered. So, it would be problematic to actually get approval for Luke Air Force Base to be a 130i.

Now, as I mentioned earlier, under 130i, if a drone is conducting unauthorized surveillance or suspected even of conducting authorized surveillance, then the base commander would be able to respond to that. Unauthorized surveillance may or may not meet the criteria of hostile intent, which would give you the authority to respond under the standing rules of engagement and the standing rules for the use of force. So, it relieves some of the burden on that base commander to determine that there is an imminent threat. If this is interfering with our operations, if this is giving the potential adversary a look at our base and our sensitive activities, then we have the authority to respond.

Mr. SUBRAMANYAM. And you mentioned before having to reach out to local jurisdictions if someone is operating UAS outside of a base. And what kind of coordination is currently being done with state and local jurisdictions? Is it sort of ad hoc, or is there like a process in place right now? And does Federal law limit the extent of engagement with state and local? And how can we make that better?

Admiral SPEDERO. Yes, thank you for that question. So, each base commander, one of his imperatives is to build relationships with the local community. That would include law enforcement

agencies. It is covered extensively in all of the base commander courses. So, their part of their training and their education program, before they assume command, is building, is how to build those relationships, the importance, what the limitations of those are. So, each individual base commander is responsible.

There are additional lessons learned and protocols and best practices about how to engage law enforcement on this particular threat, but those occur at our bases and did occur at Joint Base Langley-Eustis. They had a very, very tight relationship with local law enforcement, with sheriffs, police departments, as well as other Federal agencies, law enforcement agencies that have capability in that area. And they did respond in concert together to try to apprehend individuals that were responsible for that drone activity over the base. So, that—it does occur, and it is very important.

Mr. SUBRAMANYAM. And as far as technology and mitigation, what—and I do not know if maybe this is the right forum for this, but broadly, do you think there is technology gaps currently? And do you think that there is progress being made toward kind of filling those gaps? And what can we do, both in Congress, as well as the private industry, to help kind of fill the gaps when it comes to technology if we are trying to address both kinetic and non-kinetic solutions?

Admiral SPEDERO. Yes, in general, the technology to field systems has far outpaced the technology to defeat those systems. It is a much wider, broader, deeper market for drone application for commercial and recreational purposes, so hence, that technology has evolved very quickly from radio-controlled drones to now fully autonomous drones that may or may not even rely on reception of a GPS signal, which would make it very challenging to intercept. So, on the counter-drone activity, you know, you have to come back to agencies that would be interested in that like Department of Defense, Department of Homeland Security, FBI, you know, law enforcement agencies. So, we have to partner and we have to create that demand within industry to get technology back on pace to counter this ever-increasing emergence of drone technology.

Mr. SUBRAMANYAM. Do you feel like we have the personnel right now and the expertise in the country to be able to do this?

Admiral SPEDERO. I think we have seen a good response. I will defer to Secretary Ditlevson. He can talk about DIU and other organizations that have really made a solid partnership with industry to advance this technology.

Mr. DITLEVSON. Thank you, Admiral. Yes, there are several different organizations within the DoD that are looking at this issue and moving out rapidly to acquire new capabilities such as the JRAC, the Joint Counter-UAS Office, and DIU. All of those, this is a focus area and one of their primary lines of effort.

Mr. SUBRAMANYAM. Thank you. I yield back.

Mr. TIMMONS. Thank you. I now recognize the gentleman from Virginia, Mr. McGuire, for 5 minutes.

Mr. MCGUIRE. Thank you, Mr. Chairman, and thank you to our witnesses.

Admiral, thanks for your service.

I want a yes or no from both of you. Are you aware of the August 2020 advisory? It is an advisory on the application of Federal laws

to the application and use of technologies to detect and mitigate unmanned aircraft systems. Are you two aware of that?

Admiral SPEDERO. No, sir, I am not specifically aware of that.

Mr. DITLEVSON. No, sir.

Mr. MCGUIRE. If and when appropriate, I have a copy, and I would like to admit that into the record.

Mr. TIMMONS. Without objection, so ordered.

Mr. MCGUIRE. So, I believe that is the source of a lot of the problems that we have. In the military, we have something called paralysis by analysis. Obviously, the commanders at Langley and other bases have seen drones, and they fail to act because—and I believe the source of those problems is this August 2020 advisory.

And I think I have a solution for it. I was recently at the southern border where I met with Tom Homan. I met with border control, ICE agents, mayors, sheriffs, business owners, 10th Mountain Division folks that are protecting our border from San Diego all the way to Texas, and I asked them, are you seeing drones come across the southern border and surveying our troops? And the answer was yes. And I said, is 130i working for you right now? And I know what they said, but Admiral, what do you think? Is 130i right now working for us?

Admiral SPEDERO. So, they do not have 130i. That is the first piece.

Mr. MCGUIRE. OK. That—

Admiral SPEDERO. And we are working to resolve that. So, for instance, in the national defense areas that have just been established as an annex, does not have 130i. Now—

Mr. MCGUIRE. I get it. I just am going to get to a point.

Admiral SPEDERO. Yes.

Mr. MCGUIRE. And how about do you have an opinion on 130i right now as of today?

Mr. DITLEVSON. Yes, Congressman. If we can get 130i implemented in these areas where a joint task force southwest border is operating, it should enable the commanders on the ground to have those expanded authorities that allow them to interdict and mitigate these UAS threats.

Mr. MCGUIRE. And I know you said you are working with Congress on legislation, so I would like to talk to you about an idea on a piece of legislation. It may be something that involves Judiciary and FAA, but let me run this across you.

So, we currently have troops on the border facing the cartels and our critical infrastructure. Now, of course, we have got Langley Air Force Base and other critical infrastructure as well, and, of course, we have got bad actors that have bought land next to our military bases, and they are surveilling us on a daily basis. And it is only a matter of time until we have our next 9/11 terrorist attack. The problem is bureaucracy prevents action, but this time we know about it and we can fix it. And right now, with 130i, the way it is proposed, you have to be observed or attacked and then ask for permission, and that takes delays.

I have got an idea that might speed that up. Eighteen U.S. Code 32 is treating remote-control airplanes, which I call a drone—so 18 U.S.C. 32 is treating remote-control airplanes or drones as if they are passenger airplanes, and they are not. Basically, the problem

is the government has created complex statutes to let a few bad actors possibly take action if you jump through a thousand hoops, 130i. This is not good enough. We owe it to our military and our citizens to fix this. The United States provides better protection from UAS to Saudi Arabia than we do to our own citizens.

And so, my idea for a bill is you change the word from aircraft to manned aircraft because I think every commander is afraid that if I shoot down a remote-control airplane or a drone, no one is going to back me up. I think I remember hearing the Langley commander say, are you guys going to back me up? Are you guys going to back me up? And no one answered. That may not be 100 percent true, but Admiral, do you have any comments on that idea?

Admiral SPEDERO. Yes, this is the burden of command. And you need to understand that if there is something that is assessed as a threat to your forces or your installation, then, again, you not only have the authority but the responsibility to act.

I would counter that they have authority right now on the southwest border to engage UAS. We have in the last few days alone reaffirmed that under the standing rules of engagement and the standing rules of use of force, when you take in the totality of the facts and the circumstances at the time, you have the authority.

We know that cartels have used UAS for unauthorized surveillance to assess our troop size, our movements, to solicit and enable attacks from other vectors. We know that they have used drones and kinetic attacks against Mexican——

Mr. MCGUIRE. Well, Admiral, with all due respect——

Admiral SPEDERO [continuing]. Military authorities.

Mr. MCGUIRE [continuing]. I just returned from the southern border, and I asked the commander from Texas to San Diego if he has authority to shoot down drones that he is looking at that is looking at his troops, and he still is not sure. I just left the southern border, and I think it goes back to that advisory. That advisory has created a stigma, and I think that we can mitigate or overcome that if we just change the word from aircraft to manned aircraft, and then they will not have such a huge penalty if they shoot down a drone. And certainly, if someone wants to prosecute somebody for shooting down private property, there are plenty of laws on the books for that.

But with that, I have no further questions. Thank you, Mr. Chairman. I yield back.

Mr. TIMMONS. Thank you. I now recognize the gentleman from Massachusetts, Mr. Lynch, for 5 minutes.

Mr. LYNCH. Thank you very much, Mr. Chairman, and I want to thank the witnesses for helping the Committee with its work.

I do have to say that I would prefer that we were reviewing the facts of the signal chats that were conducted by Secretary Hegseth and the Trump leadership team in order to get to the bottom of that. However, I will, at a later date in full Committee, enter a resolution of inquiry to ask the administration to provide information to this Committee, to the Oversight Committee, regarding how that happened.

It was bad enough that the last time we were here, we just knew that the initial signal chat had happened and that inadvertently they had included the editor of *The Atlantic*, who was not approved

for clearance, and that the chat included specific information about those attacks against Yemen, which could have put our sons and daughters in uniform at grave risk.

Now, that was then. Now we know that this chat also went to Secretary Hegseth's brother, his sister. I do not think his mom was in on it. She is about the only one in the family who was not in on it. And then the family attorney was in on it as well. So, that is a whole set of people who were not authorized to be on that chat, again, that disclosed, you know, classified information and actionable intelligence about an impending U.S. attack in Yemen.

And then beyond that, now we find out that Secretary Hegseth is using his Gmail account and using a phone that was listed on his sports betting app and available to the public. So, this just keeps getting worse.

I know that is not the fault of these witnesses, and they probably cannot illuminate the circumstances, but I will be filing that resolution of inquiry asking for the White House to provide that information because that is important. It is not partisan politics. It is just what the Oversight Committee should be doing to keep our military personnel safe, like what we are doing here. We are having a hearing on drones, you know, being flown in the area of, you know, U.S. bases, and that presents a danger to our sons and daughters. Well, so does, you know, using a non-secure platform to discuss actionable intelligence against our enemy who has anti-aircraft and anti-naval vessel capability. That is really important, too, and that presents a clear and present danger.

I know that there were reports in the press that the White House said that was childish, that was childish that Secretary Hegseth did that. I agree with that assessment. I think it was totally immature, and it demonstrates an unfitness and a lack of seriousness about protecting our sons and daughters in uniform.

You know, we all nominate young men and women from our district to the Military Academy at West Point and to the Naval Academy, and dear God, you cannot, you know, put a family in that position, put one of our best and brightest in that position, and then leak information to our enemies while they are going into battle.

OK. So, this Committee, myself included, investigated an attack, a 2020 attack by al-Shabaab at Manda Bay in Kenya. That was a drone attack. Several recent base attacks overseas, in fact, have involved the use of drones. So, Admiral, how has our profile, you know, countermeasures against drones, how has that changed since those initial attacks back in 2020 that resulted in U.S. casualties?

Admiral SPEDERO. Yes, so since that time, we have fielded a number of new systems across a variety of the spectrum, electromagnetic as well as electro-optical and infrared sensors to build our domain awareness. We have also fielded a number of kinetic systems that shoot interceptors or use some sort of munition, and they are deployed at our most vulnerable and most likely to be attacked facilities overseas. That is where the bulk of our counter-UAS capability is actually located is overseas, and hence, the problem here on the homeland is we have very limited and sparse and distributed capability across, you know, the multitude of installations we have.

Mr. LYNCH. Thank you, Admiral.

Thank you for your courtesy, Mr. Chairman. I yield back.

Mr. TIMMONS. Thank you. I now recognize the gentleman from Arizona, Mr. Biggs, for 5 minutes.

Mr. BIGGS. Thank you, Mr. Chairman.

I just want to briefly comment about the previous questioner, once again, going with the woke media story and not bothering to mention the success of the strikes which restored freedom of navigation, protected shipping lanes, and kept Americans safe, nor did he bother to mention that the encrypted service that was being used was one recommended by the previous Administration, by DHS guidance.

But my questions with regard to this topic is for both of you, and this is the context. So, do we have the technology to discover that there is UAVs in the neighborhood of our bases?

Mr. DITLEVSON. Yes, Congressman, we do.

Mr. BIGGS. OK. If a UAV is there, can we track it? Do we have the technology to track it?

Mr. DITLEVSON. Yes, Congressman.

Mr. BIGGS. OK. And then you could interdict it if you chose to at every base?

Mr. DITLEVSON. We have different options for interdiction, Congressman, across a spectrum——

Mr. BIGGS. Right.

Mr. DITLEVSON [continuing]. For the commander to use their best judgment.

Mr. BIGGS. But you could interdict if you chose, if you so chose. And you have authorities under 130i, perhaps, depending on the commanding chain there, right? I mean, you could make that point, right?

Mr. DITLEVSON. Depending upon the installation, whether it is a covered installation, Congressman, you would have the 130i additional authorities. But, as the Admiral has said, there is always the ability to respond if there is hostile intent for that base commander.

Mr. BIGGS. But you have to determine hostile intent, and that is the problem, right?

Admiral Spedero, could you explain how unauthorized drone activity, even when it is caused by recreational or commercial users, diverts critical security resources away from responding to legitimate national security threats, please?

Admiral SPEDERO. Yes, Congressman, thank you for your question. If we go back to New Jersey and, you know, that activity, once the FAA put the temporary flight restrictions in place and there was, you know, very broad and comprehensive coverage of that by the media, many of you spoke about it, many of the Members of Congress talked about the anxiety that was building in the community due to the high level of sightings. Once that word got out, that public messaging about responsible drone use, once the word got out about the flight restrictions, we saw a rapid decline in the number of sightings. The drone activity essentially went away. And we do not want to get to the point where we have to do that every time.

If we can message to the public that responsible commercial and recreational application of your drone is an imperative to prevent

diverting our attention and our resources both from investment, training, and response, we are going to be better at defending the homeland. But if we have to continually be aware of negligent drones flying into our base, it is going to divert attention.

That is not to say that we do not need to address this threat because, as was brought up by this Committee and we agree with, our adversary has demonstrated that they will use this type of activity for unauthorized surveillance, for espionage.

Mr. BIGGS. Yes, and let us add to that for a second, and that is the coupling of AI, which is moving rapidly forward and providing autonomous navigation, obstacle avoidance, deep learning, computer vision, easier to become weaponized, real-time image recognition, target identification. So, I would like, briefly, if you could, either one of you want to talk about the threat of AI, coupled with drone technology, to become actually an exponentially increased threat to our national security.

Mr. DITLEVSON. Congressman, it is a great question. Thank you for that. On the policy side, we need to make sure that our regulations internally at the DoD are streamlined to the extent that we stay at pace with the threat that we face outside the fence line of our installations. We need to make sure that we are giving the commanders on the ground clarity on what they have for authority and providing them the capabilities to counter those threats.

Now, I think the Admiral can speak better as far as what is actually being developed at this time and how far ahead we are in counter-UAS technologies, but as far as the policy purview is concerned, I know from the Secretary of Defense front office down, we need to give the warfighter every capability they need to keep our service members safe.

Mr. BIGGS. I know that I am not going to have time to hear your answer, Admiral, sorry, but with regard to the policy, I would ask that you work with the Chairman of the Subcommittee on policies that need to be rewritten, perhaps through legislation, that we can do to facilitate defending against this combination of AI and drone technology, which is advancing very rapidly.

Mr. Chairman, to that extent, I have some unanimous consent requests, if possible.

Mr. TIMMONS. Yes.

Mr. BIGGS. Yes, the first one is "Autonomous Ascent: How AI is Reshaping the Future of the UAV Industry." Another piece, "Mystery Drones Swarmed a U.S. Military Base for 17 days." The next one, "What We Know About the Langley Air Force Base Drone Incident."

Mr. TIMMONS. Without objection, so ordered.

Mr. BIGGS. Thank you, Mr. Chairman.

Mr. TIMMONS. Thank you. I now recognize the gentleman from Texas, Mr. Cloud, for 5 minutes.

Mr. CLOUD. Thank you, Chairman. Thank you for bringing up this very important topic that is very timely. And thank you, Admiral, especially for your service and those in uniform behind you for what you do to protect and serve our country.

It occurs to me that we are discussing this issue, but it seems to me like it is as much a system of some of the bigger issues we have seen at the Pentagon regarding our stance just on the world

stage in the sense that, you know, I wish we were talking today about how advanced we are and how forward-thinking we have thought about this and that we have invested in these new technologies and that we are leading the world in it when we look at drones and drone incursions. But yet, for me, you know, I have considered that funding our defense is our No. 1 constitutional duty in Congress.

My biggest concerns have been that sometimes we are funding legacy systems that are outdated as opposed to investing into where the puck is going, so to speak. And while the funding for this is in lots of different buckets, my analysis, looking through a bunch of this, it seems like we are spending about \$22 billion-ish in the last budget on fighter jets and maybe \$1 billion on drone and counter-drone technology together. That may be off a bit because, again, it is in a lot of different pockets.

But it is that that concerns me in the sense of, you know, we are talking about military incursions over our base. We are talking about one drone coming and what we can or cannot do about it. I think from the American taxpayer who is sitting at home going, we are spending \$800 billion roughly on defense, and we cannot shoot a drone down, it is just a frustrating experience because we want to think that we can do that.

So, as has been mentioned, us needing to do our job to make sure that you have the capabilities to do it, but I would also wonder how much of this is a little bit of a reactive stance in command being more concerned about CYA, so to speak, as opposed to protecting the assets and the intelligence and the information that is available on that base.

You mentioned that you recently developed the SOP, I guess, about a month ago. That was news to me. Could we get a copy of that sent to this Committee?

Admiral SPEDERO. Yes, sir. I do not see a problem with that. I will coordinate with the Commander, U.S. Northern Command.

Mr. CLOUD. OK. That would be much appreciated.

And, you know, we all remember, what I would call, Biden's balloon blunder where we had this balloon come across. We sat here and watched it for days. I went to a meteorologist at one of the local news stations, and he was tracking it and predicting where it was going to go, and yet we were watching it go over bases and not doing anything about it. How much of this is just not the will to act versus legitimately you being prohibited legally from doing things? There is a difference between not having a clear authority and being prohibited from doing something, I guess is what I am trying to draw on.

Mr. DITLEVSON. Yes, Congressman. That is a great question. For us on the policy side, we seek to clarify the authorities for base commanders so that they understand exactly what they are able to do. And, as you pointed out, sometimes there may be a little bit of confusion because of how the language is given out or guidance is pushed down to the lower levels.

During our review of counter-UAS policies, as prescribed in section 925 of the Fiscal Year 2025 NDAA, we have gone back and we have reviewed all of our counter-UAS documentation. For example, section 130i, it was at about 130 pages. We have cut that down to

20 pages now. So, we are looking to streamline our processes as much—

Mr. CLOUD. Yes.

Mr. DITLEVSON [continuing]. As possible so commanders understand what they have for authorities.

Mr. CLOUD. That is certainly very helpful. I guess, you know, if I could convey kind of the angst of the American people, you know, we are looking at this and thinking, OK, there is drone incursion into the United States. You know, there are bad actors within our borders now who have the ability to even attack infrastructure. And we are talking military bases, but it could be electric powerlines, it could be pipelines, it could be anything at this point, and we seem very—like we are approaching this from a very bureaucratic standpoint as opposed to something that literally could be a problem next week. And I am wondering what we can do, and what we can help you do, in the sense of the sense of urgency that could be needed.

Again, we have bad actors even at the state level within our borders because, you know, we had open borders for the last 4 years, so the terrorist activity that is now in our country and bad actors from other states that do not have the best interest of our country in mind are here with this kind of capability. And what can we do to speed up this process so that it is handled with the urgency as opposed to kind of, like, this curious bureaucratic question that needs to be resolved?

That is a question. What can we do to speed it up both from DoD and from Congress' standpoint to support what you need?

Mr. DITLEVSON. Thank you for the question, Congressman. We have a legislative proposal working through the Pentagon right now focused on three areas where we could improve section 130i. In the Department's opinion, we do not want this provision to sunset. We want to make sure that the authorities continue forward. There is an expiration date on 130i authorities next year.

We also want to expand the locations and missions covered under 130i. As we have discussed today, the bases are not all covered. Not all installations qualify as one of the nine mission areas under 130i, so we would like to expand that to cover all installations.

And then we would also like to facilitate data sharing because, right now, data sharing from the DoD side is limited only in the pursuit of a legal case against a particular individual or group. We are not able to share data with our interagency partners to improve our tactics, techniques, or procedures. And to your point, Congressman, earlier about driving cost efficiencies, being able to share data to produce better technology would help us be more efficient with taxpayer money.

Mr. TIMMONS. Thank you for that. The gentleman's time has expired.

The Chair now recognizes the gentlelady from Florida, Ms. Luna, for 5 minutes.

Ms. LUNA. Thank you, Chairman.

Here is what every American needs to know that is watching this currently. In 2024 alone, 350 drones were detected flying over our military installations, over 100 to be exact, and that came straight out of the mouth of General Gregory Guillot, Commander of

NORAD and U.S. Northern Command. These were not just toys. These were intelligence-gathering, signal-jamming, and potentially weaponized drones. These incursions happened while the Biden Administration sat on their hands allowing bureaucracy and inter-agency dysfunction to run the show. I see a lot of military here right now. You guys all know that bureaucracy, many times, can be our worst enemy.

Now that President Trump is back in office, thank God, we finally have strong leadership again, but cleaning up Biden's national security blunder is no small task. Our military installations are still extremely vulnerable. As hearing just sitting here from some of my colleagues, we have the CCP, Iranian proxies, Mexican cartels, they all know this.

We are here today to fix that. And let me be crystal clear. As I am sure many of you would agree, if you are flying unauthorized drones over military installations, you should expect it to be shot down. Do not expect Uncle Sam to pay for it either. My opinion is play stupid games, win stupid prizes.

Now, Admiral Spedero, I have heard directly from General Guillot, in February, 350 drone incursions over 100 military installations in 1 year. I know that this is not your fault directly, but this is a massive security gap and utter failure. Under current authorities, what is preventing base commanders from neutralizing these immediately, in my opinion, going out there with a shotgun and shooting these things down?

Admiral SPEDERO. Thank you, ma'am, for the question. I wish it were as simple as shooting it with a shotgun, but it is not.

Ms. LUNA. Depending on elevation. But what is stopping it? Is it still the bureaucratic red tape and sign-offs? Because in my opinion, if you are flying something like this that can jam communications, maybe carry explosives, collect surveillance on classified systems, I do not think that you should have to be required to make a phone call. I think that if you see it, you should shoot it down.

Admiral SPEDERO. Yes, under 130i, unauthorized surveillance would meet the standard for engagement. If it were interfering with your operations, it would meet the standard for engagement. If you are not at 130i, then again, back to the rules of engagement and establishing hostile intent or hostile act. But you may get there, so just the presence of that drone over your base may meet hostile intent or hostile act. There is not a set of circumstances I can tell you in every case and go down a checklist, OK, you have met it, go ahead and shoot.

Ms. LUNA. Sir, I mean, I think you might agree. If you are flying a drone in any capacity, I do not care if it is civilian or not, over a military installation, I do not even think you should have to go to a checklist. I think that it should automatically be taken down.

Admiral SPEDERO. Yes, and that is the preference to invoke 130i is to relieve that burden because we do agree that unauthorized access to our bases poses a threat. Even if there are not sensitive activities, it does provide surveillance of our force posture, our weak points, our vulnerabilities, you know, descriptions, geographic details of the base.

Ms. LUNA. All of the information, right?

Admiral SPEDERO. They can gather intelligence piece by piece by any means necessary, so we do want 130i protection because we would like to relieve that burden. Now, engagement still needs to meet the standard, the responsible standard, and you have to do a collateral damage assessment before you can engage anywhere.

Ms. LUNA. Well, I have a feeling with this Administration and the Members on this panel, I think that you will probably get there. So, help is on the way in that regard.

Mr. Ditlevson—hopefully, I said that OK—do you believe that foreign adversaries like China and Iran exploit the jurisdictional chaos under the previous Administration to increase their drone activity over U.S. territories?

Mr. DITLEVSON. Yes, Congresswoman. I think our adversaries take advantage of every weakness that we have in our system, and they are constantly probing, trying to find an entry point.

Ms. LUNA. OK. Well, let me just be crystal clear for the record. If you fly a drone over an American military base, it should be blown out of the sky. I do not think that this is a controversial perspective to have. No phone calls, no paperwork, no permission slips. But under the Biden message, I think it was more or less the message of fly wherever you want, we will kind of deal with it later. But be crystal clear, under this Administration, the message is FAFO. For decorum's sake, we will not interpret that, but just mess around, find out. You guys all know what that means.

We have the technology, we have the capability, but what we have lacked up until now is the courage to act without apology. This is not about drones. It is about deterrence. It is about restoring the kind of unapologetic strength that keeps our enemies at bay and our warfighters safe.

I yield my time. Thank you guys so much for being here today. You guys look great in uniform, and you do too, ladies.

Mr. TIMMONS. Thank you. In closing, I want to thank our witnesses once again for their testimony today.

I now yield to Ranking Member Subramanyam for closing remarks.

Mr. SUBRAMANYAM. Thank you, Mr. Chair. I think I will keep it brief.

I think we have some good ideas that we can maybe turn into legislation, and we can hopefully make sure that we empower bases to both have the right technologies to address this, as well as to make sure more military installations are covered under statute potentially, make sure there is better coordination with state, local, and Federal, and make sure that overall we have a workforce and the capacity to be able to address these challenges. So, I am glad we are all on the same page on that front, and I look forward to working on this together.

Thank you. I yield back.

Mr. TIMMONS. Thank you. I now recognize myself for closing remarks.

It seems that we are a bit paralyzed here in Congress to deal with emerging technology. I have been working on cybersecurity legislation for the last six-plus years, and the bill that we need, a comprehensive bill would have to go through at least ten, maybe more, committees of jurisdiction to get it right in the House and

probably another five-plus in the Senate. And we are just unable to do what we need to do to address real national security issues in the realm of cybersecurity. And I fear that it is going to take some tragedy to cause us to act in that capacity on cybersecurity.

I do not think drones are much different both because of the complexity, the challenges that we face from a legislative perspective, whether it is authorizing and appropriating the money to purchase the necessary technology to monitor, to then engage with and disarm drones that are posing a threat, or whether it is the authority side to address the legal concerns that are very real. And it is probably not going to get done in one bill. It is going to probably be a number of bills, and, you know, there is going to be a lot of interest surrounding how we do it.

You know, as I think about this issue, the Chinese New Year drone was one of the most amazing things I have ever seen, and it also was very troubling. That display of—I mean, I guess it was an AI-enabled drone swarm that was basically providing entertainment. But while it was very entertaining, it is also terrifying. And I think that the capabilities of our adversaries and seeing how war has evolved in Ukraine and how the Russians and the Ukraine military are largely relying on drones, I mean, a huge portion of that conflict is being used as technology as opposed to traditional warfare.

So, we have got to get moving on this. We have to enhance our capacity. Congress has to act, but a lot of this is the private sector getting up to speed. A lot of this is our Defense Department telling us exactly what they need. And we do not have time to waste. We have spent enormous amounts of resources to make sure that we have a 24/7, 365 air alert mission for fighter jets to be deployed. And I am not sure how good that capacity is right now, considering that a couple dozen drones could severely impede our ability to get jets off the ground. So, I mean, this is a huge, huge challenge, and we need to act before it is too late.

I appreciate you all taking the time to come here today. It seems that we are moving in the right direction, and I appreciate your work to help get us where we need to be. And I look forward to working with my friend, the Ranking Member, to craft some legislation.

And with that, I will yield back. Thank you again for being here today.

Without objection, all Members have five legislative days within which to submit materials and additional written questions for the witnesses, which will be forwarded to the witnesses. If there is no further business, without objection, the Subcommittee stands adjourned. Thank you.

[Whereupon, at 3:15 p.m., the Subcommittee was adjourned.]

