SUBCOMMITTEE ON INTELLIGENCE AND SPECIAL OPERATIONS EN BLOC #1

LOG			MARKUP		MARKUP
ID	REV	MEMBER	LOC	DESCRIPTION	ACT
4784	4	Fallon, Pat	ISO	Requires DoD to provide a briefing to the House Armed Services Committee on the use of the "NOFORN" dissemination control measure and how it is applied in various contexts.	EB 1
4796	2	McCormick, Richard	ISO	Briefing on Self-Routing Edge Data Synchronization for Tactical Mobile Devices	EB 1
4808	0	Jackson, Ronny	ISO	Briefing on enhancing the dynamic sensing environment to enable Special Operations Forces	EB 1
4966	0	Scott, Austin	ISO	This amends 10 USC 333(a) by adding Space domain awareness.	EB 1
4989	0	Jackson, Ronny	ISO	Authorizes USSOCOM to develop a digital force protection pilot program.	EB 1
5135	2	Hamadeh, Abraham J.	ISO	Briefing on how U.S. Army Civil Affairs and Psychological Operations Command (Airborne) is being incorporated into Army Transition Initiative	EB 1
5195	1	Stefanik, Elise	ISO	Briefing on USSOCOM's plans to incorporate commercially off the shelf mesh radios into Remote Advise and Assist/Virtual Accompany Kit program's	EB 1
5228	1	Jacobs, Sara	ISO	Requires a report on Global Fragility Act implementation at DOD.	EB 1
5318	0	Kiggans, Jennifer A.	ISO	Brief on SOCOM's efforts to develop a maintenance program for NSW combatant craft that uses commercial tech to monitor vessel condition and operator health.	EB 1
5406	2	Davis, Donald G.	ISO	Briefing on what Personal Protective Equipment(PPE) is currently available and what can be applied for civilian use within military stockpiles.	EB 1
5436	3	Elfreth, Sarah	ISO	Requires the DoD to provide the House Armed Services Committee a report on how the Department is working to come into compliance with ICD 705, which requires SCIFs to meet various standards for security.	EB 1
5438	0	Khanna, Ro	ISO	Declassification of Records Relating to the Global War on Terror	EB 1
5461	0	McGuire, John J.	ISO	Directs a briefing by Commander of USSOCOM on the ability of existing armor systems to protect special forces from fragmentary blast threats from UAS.	EB 1

LUG ID REV MEMBER MARKUPLUC DESCRIPTION MARKUP A	LOG ID	REV	MEMBER	MARKUP LOC	DESCRIPTION	MARKUP ACT
--	--------	-----	--------	------------	-------------	------------

Offered by: Mr. Fallon from Texas

In the appropriate place in the report to accompany H.R. 3838, insert the following new Directive Report Language:

Security Classification and NOFORN Use Briefing Requirement

The committee understands that the NOFORN designation plays a legitimate role in protecting sensitive national security information. However, overreliance on such dissemination control measures could undermine efforts to build integrated deterrence, enhance interoperability, and strengthen coalition operations with trusted foreign partners and allies. The committee is interested in learning more about the Department's use of the NOFORN designation and how it is applied in various contexts.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than December 1, 2025, on the Department's policies, requirements, and regulations governing the use of the NOFORN designation within security classification guidance. The briefing shall include:

- (1) A comprehensive summary of each office, agency, or component within the Department of Defense responsible for establishing, implementing, and overseeing policies related to the use of the NOFORN marking;
- (2) A comparative data analysis of the frequency and context of NOFORN use versus other dissemination control markings;
- (3) An explanation of factors contributing to the use of NOFORN designations, including potential institutional, regulatory, or cultural drivers inconsistent with congressional intent to reduce reliance on NOFORN;
- (4) Recommendations to reduce possible overuse of NOFORN markings and facilitate timely reevaluation and potential redesignation of existing NOFORN material; and
- (5) Anything else the Secretary determines to be relevant.

The committee further directs that the briefing include written documentation supporting the Department's analysis. A classified annex may be provided, if necessary.

Offered by: Mr. McCormick

In the appropriate place in the report to accompany H.R. 3838, insert the following new Directive Report Language:

Self-Routing Edge Data Synchronization for Tactical Mobile Devices

The committee notes the utility and customization available in the Android Tactical Assault Kit (ATAK) used by United States Special Operations Command and others for communication, collaboration, and situational awareness during missions. The committee understands there is an ATAK limitation at the tactical edge since the existing fielded plugin solutions rely on specific transport mediums or require connection to a central cloud server for synchronizing critical mission data. The committee realizes that the cloud can present a single point of failure where a connection outage or disruption could render edge applications unusable.

Therefore, the committee directs the Commander, U.S. Special Operations Command, in coordination with the Chief Technology Officer of the Department of Defence, to provide a briefing to the House Committee on Armed Services by December 1, 2025. The briefing shall include:

- an assessment of the effectiveness and operational impact of commercially available cloud-optional software for ATAK that enhances data-sharing by leveraging multiple transports on end user devices without the need for significant investment in new hardware;
- (2) potential acquisition pathways to acquire such commercially available solutions command-wide; and
- (3) a plan for how cloud-optional ATAK capabilities can be integrated with other users across the joint force.

Offered by: Mr. Jackson of Texas

In the appropriate place in the report to accompany H.R. 3838, insert the following new Directive Report Language:

Enhancing the Dynamic Sensing Environment to Enable Special Operations Forces

The committee applauds U.S. Special Operations Command (USSOCOM) efforts to advance electronic warfare capabilities to meet the rapidly evolving nature of warfare and adversarial threats. The committee observes that these threats and ubiquitous technical surveillance require continued collaboration between USSOCOM, Department of Defense partners, and industry to close technical capability gaps and maintain our nation's operational edge. Furthermore, the committee understands that investment in low-cost, automated, easy-to-use radio frequency detection capabilities improve training that increases operational success and enhance operators' survivability.

Therefore, the committee directs the Commander of U.S. Special Operations Command to provide a briefing to the House Committee on Armed Services not later than December 1, 2025, on the current capabilities and requirements for countering advanced electronic warfare threats and how modular, automated, lowcost radio sensing platforms can enable spectrum awareness, increase mission success, and improve operator survivability without requiring specialized personnel.

AMENDMENT TO H.R. 3838

OFFERED BY MR. AUSTIN SCOTT OF GEORGIA

At the appropriate place in subtitle A of title XII, insert the following:

1 SEC. ____. AUTHORITY TO BUILD CAPACITY FOR SPACE DO 2 MAIN AWARENESS.

3 Section 333(a) of title 10, United States Code, is
4 amended by adding at the end the following new para5 graph:

6 "(10) Space domain awareness.".

\mathbf{V}
\sim

Amendment to H.R. 3838 Offered by Mr. Jackson of Texas

At the appropriate place in title X, insert the following:

1 SEC. 10____. PILOT PROGRAM ON DIGITAL FORCE PROTEC 2 TION FOR SPECIAL OPERATIONS FORCES.

3 ESTABLISHMENT.—The Commander of the (a) 4 United States Special Operations Command may carry out 5 a pilot program, to be known as the "Digital Force Protec-6 tion Pilot Program", to identify existing vulnerabilities in 7 digital force protection, provide targeted ubiquitous technical surveillance mitigation training, and help identify 8 9 commercially available secure communication and obfusca-10 tion technologies to protect personnel and support overall mission effectiveness. 11

12 (b) OBJECTIVES.—The objectives of a pilot program13 carried out under subsection (a) are—

(1) to increase understanding of existing digital
signature and ubiquitous technical surveillance risk
for selected Special Operations Forces units and the
associated threats to personnel and mission effectiveness that come from digital exposure and adversary
tracking;

 $\mathbf{2}$

1	(2) to strengthen digital force protection for the
2	purposes of operational security and strategic decep-
3	tion efforts across all domains of warfare; and
4	(3) to demonstrate digital force protection as a
5	critical enabler of multi-domain operations and the
6	need to ensure Special Operations Forces can oper-
7	ate seamlessly across land, air, sea, space, and
8	cyberspace without adversarial digital exploitation
9	undermining mission success.
10	(c) Recommendation of Units.—
11	(1) IN GENERAL.—If the Commander carries
12	out a pilot program under subsection (a), the Com-
13	mander shall recommend not fewer than two Special
14	Operations Forces units to carry out the pilot pro-
15	gram, which may include a command and unit ele-
16	ment.
17	(2) Considerations.—In recommending units
18	to participate in the pilot program under paragraph
19	(1), the Commander shall take into consideration—
20	(A) the need to include multiple categories
21	of personnel, including operational support
22	staff, enablers, and contractors to ensure a
23	complete assessment;
24	(B) the readiness status of the units, with
25	an emphasis on providing training to those

units most likely to deploy to areas with high
 likelihood of adversary digital surveillance; and
 (C) the need for a sufficient sample size,
 which is approximately a battalion.

5 (d) CONTRACT AUTHORITY.—If the Commander car-6 ries out a pilot program under this section, the Com-7 mander may enter into a contract for the provision of serv-8 ices to facilitate the pilot program. If the Commander uses 9 such authority to enter into a contract for training or as-10 sessment, such training and assessment shall be capable 11 of—

(1) conducting multiple realistic ubiquitous
technical surveillance training scenarios that are
consistent with observed adversarial tactics, techniques, and procedures with exploiting commercially
available data against Special Operations Forces
units;

(2) training key personnel across leadership,
operational, and support elements on the threats
posed by the commercial data economy and specific
skills development to manage digital signatures and
mitigate ubiquitous technical surveillance risks;

23 (3) providing advanced training for personnel
24 responsible for highly sensitive activities and mis25 sions;

1 (4) evaluating through red cell exercises pilot 2 program participant progress and to ensuring units are prepared for mission-critical operations in ubiq-3 4 uitous technical surveillance-intensive environments; (5) employing commercial technology solutions 5 6 previously deployed in a mission environment and 7 interoperable with legacy Department of Defense 8 systems, networks, and protocols, including deploy-9 ment of on-demand global obfuscated networks and 10 identity intelligence and management; 11 (6) assessing ubiquitous technical surveillance 12 and digital force protection holistically across var-13 ious threat vectors including electronic, travel, finan-14 cial, online, and physical or visual. 15 (e) BRIEFINGS.—If the Commander carries out a 16 pilot program under this section, not later than 90 days after concluding activities under the pilot program, the 17 18 Commander and the Assistant Secretary of Defense for 19 Special Operations and Low-Intensity Conflict shall pro-20 vide to the Committees on Armed Services of the Senate 21 and the House of Representatives a briefing that in-22 cludes-

(1) a thorough analysis identifying current capabilities and a description of gaps, deficiencies, or
other vulnerabilities, identified by the pilot program;

(2) specific recommendations for short-term (1 2 years) and long-term (3-5 years) initiatives to en hance digital force protection across special oper ations components;

5 (3) an assessment of how enhanced digital force
6 protection measures increase the difficulty, time, and
7 resources required for adversaries to conduct digital
8 surveillance, force tracking, and operational com9 promise of Special Operations Forces; and

(4) a comprehensive list of any additional authorities, appropriations, or other resources necessary to implement the recommended digital force
protection tools and practices identified pursuant to
the pilot program.

15 (f) DEFINITIONS.—In this section:

(1) The term "digital force protection" means
the policies, tools, and practices used to protect military personnel, operations, and critical assets from
adversarial exploitation of the commercial digital
surveillance economy, associated commercial data,
and digital footprints.

(2) The term "commercial digital surveillance
economy" means the ecosystem of companies and
technologies involved in collecting, analyzing, and

g:\V\G\062725\G062725.005.xml (999487|3) June 27, 2025 (9:35 a.m.)

- selling data generated by the interactions of individ uals with digital services and devices.
- 3 (3) The term "digital footprint" means the data
 4 traces left by individuals through the use of digital
 5 devices and services that can be exploited to uncover
 6 personal information, movement patterns, and other
 7 sensitive details.

8 (g) TERMINATION.—The authority to carry out a 9 pilot program under this section shall terminate on the 10 date that is one year after the date of the enactment of 11 this Act.

\times

Offered by: Mr. Hamadeh

In the appropriate place in the report to accompany H.R. 3838, insert the following new Directive Report Language:

U.S. Army Civil Affairs and Psychological Operations Command (Airborne)

The committee notes the important role U.S. Army Civil Affairs and Psychological Operations Command (Airborne) (USACAPOC(A)) has served since its inception in 1985. USACAPOC (A) accounts for approximately 75% of the Department of Defense's Civil Affairs capability and 60% of its Psychological Operations forces. The committee is concerned with planned U.S. Army Special Operations Command force structure reductions and realignments and the potential impact on USACAPOC(A)'s ability to meet emerging mission demands in the Indo-Pacific and other Geographic Combatant Command (GCC) areas of responsibility.

As the Army begins its Army Transformation Initiative (ATI), the committee believes USACAPOC(A) should be integrated into Army and joint exercises, planning, and cross-component missions to maximize its unique capabilities. Therefore, the committee directs the Secretary of the Army, in coordination with the Commanding General of United States Army Special Operations Command (USASOC), and the Chief of the Army Reserve, to provide a briefing to the House Committee on Armed Services by May 1, 2026, on how the Army is incorporating USACAPOC (A) into the ATI. The briefing should include the following:

(1) a description of the current force structure;

(2) the deployment to dwell ratio for those assigned to USACAPOC(A);

(3) the number of requests for capability by the GCCs for the past two years and the number of requests not supported;

(4) how the command recruits, trains and sustains those in the unit to ensure they can support the GCCs and USASOC;

(5) a description of any plans as part of ATI to restructure the command to better support the Army and the GCCs, such as consideration of a Reserve Information Branch under a dedicated General Officer to unify Reserve PSYOP and Information Operations units for strategic oversight and PSYWAR integration;

(6) an assessment of efforts to modernize information advantage planning and approval processes to enable timely, digitally-relevant

operations in support of Combatant Commands.

Offered by: Ms. Stefanik

In the appropriate place in the report to accompany H.R. 3838, insert the following new Directive Report Language:

Use of Mesh Radios in RAA/VAK Kit

The committee notes that the Remote Advise and Assist / Virtual Accompany Kit (RAA/VAK) program is critical to Special Operation Forces' ability to communicate with partnered forces (PF) around the world. To properly protect SOF operators while allowing PF communication, the committee recognizes that RAA/VAK should further efforts to incorporate both blue and green force tracking capabilities while preserving the ability to toggle between the two capabilities. Further, the committee encourages U.S. Special Operations Command to utilize secure COTS mesh radios that are low- cost, size, weight, and interoperable as part of the RAA/VAK program to ensure critical communications are viable in austere, off-the-grid environments globally. Therefore the committee directs the Commander of U.S. Special Operations Command to brief the House Committee on Armed Services not later than February 1, 2026 on its plans to incorporate secure commercial-off-the-shelf mesh radios into the Remote Advise and Assist/ Virtual Accompany Kit program.

Offered by: Ms. Jacobs

In the appropriate place in the report to accompany H.R. 3838, insert the following new Directive Report Language:

Global Fragility Act Implementation

The Global Fragility Act (GFA) mandates that the Department of State lead an interagency strategy, with the United States Agency for International Development and the Department of Defense, to address conflict and instability in five priority countries/regions. The interagency is currently implementing 10-year country strategies in Mozambique, Haiti, Libya, and Papua New Guinea, and a regional strategy in the Coastal West African states. The committee notes the importance of the role of the Department of Defense in GFA implementation as required by statute. Therefore, the committee directs the Secretary of Defense to provide a report to the House Committee on Armed Services no later than December 1, 2025 on the Department's implementation of GFA. The report shall include a description of the Department's contributions to GFA implementation in 2024 and 2025, planned funding levels for GFA implementation in fiscal year 2026, efforts to coordinate GFA implementation with the Department of State, and a description of challenges and lessons learned related to GFA implementation.

Offered by: Ms. Kiggans

In the appropriate place in the report to accompany H.R. 3838, insert the following new Directive Report Language:

Preventative Maintenance Program for Naval Special Warfare Combatant Craft and Operator Health

The committee is aware that Naval Special Warfare maintains a diverse fleet of combatant craft that support critical maritime special operations missions worldwide. Sustaining the operational readiness of these vessels—and ensuring the health and safety of their operators in austere environments—requires a proactive approach to maintenance and data collection. The committee notes that Naval Special Warfare currently lacks a standardized preventative maintenance program that integrates vessel condition monitoring with health and performance data on operators.

The committee believes that leveraging proven, commercially available technologies to collect, analyze, and act on vessel and operator data in real time can significantly improve material readiness, extend service life, and reduce risk to personnel. The committee is aware of technology capable of securely capturing data offline in harsh environments, offering predictive analytics for maintenance planning and monitoring operator fatigue and exposure.

Therefore, the committee directs the Commander of United States Special Operations Command to provide a briefing to the House Committee on Armed Services not later than December 1, 2025, on efforts to develop and implement a preventative maintenance program for Naval Special Warfare combatant craft that integrates vessel condition monitoring with operator health and performance data. The briefing shall include an analysis of commercially available technologies that:

- (1) enable secure, offline data capture and analysis of combatant craft mechanical systems;
- (2) provide predictive analytics to inform maintenance planning and supply chain readiness;
- (3) support monitoring of operator fatigue and environmental exposure; and
- (4) facilitate incorporation of lessons learned into training and sustainment practices.

Amendment to H.R. 3838 National Defense Authorization Act for Fiscal Year 2026

Offered by: Mr. Davis of North Carolina

In the appropriate place in the report to accompany H.R. 3838, insert the following new Directive Report Language:

Personal Protective Equipment Technology for Biological Threats

The committee is aware that there are ongoing efforts to develop personal protective equipment (PPE) that meet emerging and existing biological threats to the military and civilian population. As adversary countries along with non-state actors, continue to develop biological pathogens and biological weapons, the Department of Defense must continue prioritizing biological defense measures, including therapeutics, PPE, and other countermeasures.

The committee therefore directs the Secretary of Defense to submit to the House Armed Services Committee no later than January 31, 2026, a briefing on the following:

- (1) the inventory of next-generation PPE technology possessed by, or in development with, the Department of Defense, that can provide better protection for military personnel from biological pathogens than existing commercially available technologies; and
- (2) existing plans (ongoing or proposed) to notify the Director of the Advanced Research Projects Agency for Health (ARPA-H) and the Director of the Biomedical Advanced Research and Development Authority (BARDA) to identify which technologies may be transferred for civilian use.

Offered by: Ms. Elfreth of Maryland

In the appropriate place in the report to accompany H.R. 3838, insert the following new Directive Report Language:

Report on Complying with Intelligence Community Directive 705

The committee supports Intelligence Community Directive (ICD) 705, which requires that existing Special Access Program and Sensitive Compartmented Information facilities meet elevated standards that reflect increased counterintelligence risks. Efforts are underway across the Department of Defense and contractor facilities to assess compliance with this directive. However, the work required to meet these new standards is extensive, and the committee would like to know more about the Department's efforts to meet the scope and scale of the directive.

Therefore, the committee directs the Secretary of Defense to report to the House Committee on Armed Services no later than January 31, 2026, on the progress made to bring Department and contractor facilities into compliance with ICD 705. This report shall include the following:

- (1) corrective action timelines for each service to meet ICD 705 compliance;
- (2) total estimated costs to achieve compliance across the Department; and
- (3) total estimated costs to achieve compliance for federal contractors.

Offered by: Mr. Khanna

In the appropriate place in the report to accompany H.R. 3838, insert the following new Directive Report Language:

Declassification of Records Relating to the Global War on Terror

The committee is aware that impending timelines for the potential declassification of Department of Defense materials related to the wars in Afghanistan and Iraq, as well as the broader Global War on Terror, are likely to pose unprecedented challenges to the existing mechanisms for declassification review. The committee is concerned that absent significant investments in automation, including potential adoption of artificial intelligence and machine learning capabilities, the Department may be unable to meet classification review demands without significant, unaffordable investment in manpower.

Accordingly, the Committee directs the Secretary of Defense, in coordination with the Archivist of the United States, the Secretaries of the Army, Navy, and Air Force, and the members and Executive Secretary of the Interagency Security Classification Appeals Panel, to provide a briefing to the House Committee on Armed Services not later than January 30, 2026, regarding future declassification review demands. The briefing should address the following:

(1) current and projected declassification review demand;

(2) current and planned investments in technology designed to assist in timely declassification reviews;

(3) the potential for leveraging artificial intelligence and machine learning technologies and the maturity thereof;

(4) current and planned staffing;

(5) any additional requirements or investments needed in order to provide timely and accurate reviews of classified materials; and

(6) any other information that the Secretary of Defense deems relevant.

Amendment to H.R. 3838 Offered by: Mr. McGuire

In the appropriate place in the report to accompany H.R. 3838, insert the following new Directive Report Language:

Anti-Fragmentation Armor Systems

The committee notes that as warfare continues to evolve and the proliferation and use of inexpensive armed unmanned aircraft systems (UAS) has increased in conflicts, fragmentation blast threats to warfighters have escalated. The committee believes that efforts to modify existing conformal armor designs to increase the survivability of U.S. servicemembers, especially those in special operations forces, from these new fragmentation-related injuries are needed. The committee notes that while advances in technologies for active and passive defense against UAS exist, many are cost-prohibitive, not available in the required densities, or may have operational profiles inconsistent with the special operations mission needs.

Therefore, the committee directs the Commander of U.S. Special Operations Command in coordination with Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict to provide a briefing to the House Committee on Armed Services not later than March 1, 2026, assessing the adequacy of existing amor systems in protecting special operations forces from fragmentary blast threats from UAS. The assessment should include:

- the adequacy of current armor systems' ability to protect extremities and high-risk areas such as the femoral, brachial, and iliac arteries from fragmentation threats;
- (2) recommendations on how hard armor geometries could be optimized to provide more comprehensive coverage from energetic fragmentary threats;
- (3) options for modifying existing carriage systems to more effectively align hard armor geometries to areas of the body traditionally left unprotected from fragmentation threats; and
- (4) material alternatives for increasing mobility, thermo-regulation, fireresistance, and flexibility, and reducing weight while enhancing fragmentary coverage.