En Bloc Amendments to H.R. 5515		
Subcommittee on Emerging Threats and Capabilities En Bloc #2		
Log #	**Sponsor**	**Description**
125r1	Hunter	Briefing on current and planned U.S. support to Ukrainian special operations and land forces training.
185r1	Rosen	Directs the Secretary of Defense to provide a briefing to the committee on the status and evolution of automated cyber defense capabilities, to include those that automatically detect and mitigate malware and other threats.
189r1	Shuster	Directs the Department of Defense to provide a briefing to the committee on steps it is taking to protect autonomous systems from cyber attacks.
196	Langevin	Requires a briefing on methods to safeguard defense industrial base (DIB) critical technologies and supply chains.
239	Murphy	Directs the SECDEF to provide a briefing on actions taken to identify and address data collection, analysis, and sharing issues that limit robust modeling and simulation.
243	Scott	Amends the urban warfare training report section to include an assessment on the feasibility of utilizing current private facilities.
249r1	Gallagher	Directs a briefing outlining the resources and recommendations required to fully address the requirements of section 1653 of the FY17 NDAA regarding continuous monitoring capabilities and a comply-to-connect policy.
321r2	Khanna	DRL requiring the Secretary of Defense to provide a detailed briefing to the HASC detailing information security technologies the Department employs to protect the official unclassified email and official unclassifed mobile communications of its employees.

LOG125r1

Amendment to H.R. 5515
National Defense Authorization Act for Fiscal Year 2019

Offered by: Mr. Hunter

[For new Directive Report Language, please use the following:]

In the appropriate place in the report to accompany H.R. 5515, insert the following new Directive Report Language:

[Briefing on Ukrainian Special Operations Forces Training]

[The committee recognizes the critical role played by U.S. and partner assistance in training, advising, and equipping Ukrainian military and security forces over the last several years, especially at the International Peacekeeping and Security Center in Yavoriv, Ukraine. This training facility has facilitated the successful completion of numerous joint, combined exercises up to the battalion level and has better enabled multi-domain readiness of Ukrainian forces. By employing the instrumented training capability at this center, United States Army Europe has led the Joint Multinational Training Group-Ukraine in greatly enhancing the operational capability, performance, and professionalism of Ukrainian forces.

The committee further understands that such joint, combined training is scheduled to conclude in 2020 and that the Ukrainian General Staff is aware of acute needs, identified in October 2016 and restated in December 2017, to modernize the International Peacekeeping and Security Center before such training ends. These requirements include refurbishing and adding multiple integrated laser engagement systems, enhancing range and battlefield effects, and developing an urban operations training system.

Finally, the committee understands that since their establishment in 2016, Ukrainian special operations forces have grown in both numbers and capabilities with a focus on unconventional missions such as counterterrorism and drug interdiction operations. In addition, Ukrainian land forces have grown, requiring additional training to support skills development in support of combined exercises with NATO and U.S. forces. Therefore, the committee directs the Secretary of Defense to provide the congressional defense committees, not later than September 30, 2018, with a briefing on current and planned U.S. support to Ukrainian special operations and land forces training, including but not limited to: detailed assessments of both the training center at Berdychiv, Ukraine and a land forces training complex in the Mykolaiv District near Odessa, Ukraine; analysis of

training requirements; and a plan for potential U.S. funding assistance to new or modernized training facilities.]

Log 185 Revised
LOG 185-1

Amendment to H.R. 5515
National Defense Authorization Act for Fiscal Year 2019

Offered by: Ms. Rosen of Nevada

In the appropriate place in the report to accompany H.R. 5515, insert the following new Directive Report Language:

Network Protection

The committee is aware that open, highly scalable network protection platforms that allow for integration of both government and commercial off-the-shelf capabilities, may allow for the Department of Defense to keep pace with evolving threats. The committee believes expeditious detection and mitigation is critical, especially as the Department makes greater use of commercial cloud computing and other commercial capabilities.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than February 5, 2019, on the status and evolution of automated cyber defense capabilities, to include those that automatically detect and mitigate malware and other threats. The briefing should include a description of efforts to acquire an open, scalable platform that can integrate commercial and government off-the-shelf technologies, and an evaluation of the potential effectiveness of a capability that can be deployed within and across network boundaries and endpoints.

Log 189 "Revised" LOG189H

Amendment to H.R. 5515
National Defense Authorization Act for Fiscal Year 2019

Offered by: Rep. Bill Shuster

[For new Directive Report Language, please use the following:]

In the appropriate place in the report to accompany H.R. 5515, insert the following new Directive Report Language:

Mitigation of Autonomous Systems

AMENDMENT TO THE REPORT

TITLE XVI

SUBTITLE D – CYBER-RELATED MATTERS

Mitigation of Autonomous Systems

The Committee notes the Department's increased reliance on autonomous systems and their associated datalinks and sensors. While the Committee supports increased investments in these systems, the rapid research, development, and deployment of autonomous equipment presents unique challenges to cyber vulnerability. Therefore, the committee directs the Secretary of Defense to provide a briefing by December 1, 2018 outlining the specific steps the Department is taking to protect autonomous systems from cyberattack, including mitigations resulting from the cyber vulnerability evaluations of major weapon systems that were conducted as directed by Section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92). The briefing should address layered cyber defense of associated datalinks, sensors, and onboard systems, technologies used to secure the communication architecture and RF links, and any other approaches used to improve the cyber security in these systems.

Amendment to H.R. 551[illegible] **Log 196**
National Defense Authorization Act for

Offered by Mr. Langevin of Rhode Island

In the appropriate place in the report to accompany H.R. 5515, insert the following new Directive Report Language:

Protect DIB Critical Technologies

The committee recognizes the importance of safeguarding defense industrial base (DIB) critical technologies from cyber and economic actions conducted by our adversaries. The challenge in doing so is particularly acute as supply chains become increasingly globalized, as noted in the report published by the RAND Corporation entitled "U.S. Authorities and DoD Options for Protecting the Defense Industrial Base from Cyber Intrusions and Economic Enticement, Influence, and Control." The report calls attention to the difficulties in protecting DIB members with supply chains in foreign countries and the resulting risks to the integrity of various critical technologies and materials.

Therefore, the committee directs the Undersecretary of Defense for Research and Engineering (R&E) to provide a briefing to the House Armed Services Committee no later than 1 March 2019 on activities and investments the Department is making with respect to foreign suppliers of critical technologies to national defense to ensure their integrity, including microelectronics.

Log 239

Amendment to H.R. 5515
National Defense Authorization Act for Fiscal Year 20__

Offered by: Rep. Stephanie Murphy (FL-07)

In the appropriate place in the report to accompany H.R. 5515, insert the following new Directive Report Language:

Common Data Environment for Modeling and Simulation

The committee recognizes that common data environments can yield benefits, such as increased interoperability and strong modeling and simulation capabilities (M&S). The committee supports continued funding for projects that provide critical Department of Defense-wide data services, such as the Army's Enterprise Data Services Common Data Production Environment. The committee is aware that in the committee report (S. Rept. 115-125) accompanying the National Defense Authorization Act for Fiscal Year 2018, the Senate Committee on Armed Services directed the Secretary of Defense to take actions to identify and address data collection, analysis, and sharing issues that limit robust M&S. Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by November 1, 2018, on the Department's findings from the directive in S. Rept. 115-125.

Log 243

Amendment to H.R. 5[illegible]
National Defense Authorization Act for Fiscal Year 2019

Offered by: Rep Austin Scott (GA-08)

URBAN WARFARE TRAINING

In the portion of the report to accompany H.R. 5515 titled "[URBAN WARFARE TRAINING]", insert at [4a], the following new text: "*feasibility of utilizing existing private facilities and contracting training iterations until a final DOD facility can be constructed*".

Log 249 r1

Amendment to H.R. 5515
National Defense Authorization Act for Fiscal Year 2019

Offered by:
Rep. Mike Gallagher

In the appropriate place in the report to accompany H.R. 5515, insert the following new Directive Report Language:

Information Security Continuous Monitoring and Comply-to-Connect Implementation

While the Committee understands that pursuant to the requirements established in Section 1653 of the National Defense Authorization Act for Fiscal Year 2017, the Department of Defense included language relating to a Department-wide automated information security continuous monitoring capability and a comply-to-connect policy in its Fiscal Year 2019 budget request, the Committee is concerned that this language failed to adequately explain the Department's implementation strategy and the resources it will require. The Committee therefore directs the Director of Cost Assessment and Program Evaluation to provide the Committee on Armed Services of the House of Representatives, no later than December 1, 2018, a briefing specifically outlining the resources and any recommendations that will be required to fully address the requirements contained within Section 1653 of the National Defense Authorization Act for Fiscal Year 2017.

Log 321r2

Amendment to H.R. 5515
National Defense Authorization Act for Fiscal Year 2019

Offered by: Congressman Ro Khanna

In the appropriate place in the report to accompany H.R. 5515, insert the following new Directive Report Language:

Securing Personally Identifiable Information

"The committee recognizes that the Department of Defense takes extensive measures to protect the personally identifiable information (PII) of its Servicemembers and civilian employees but that more remains to be done, especially with advances in technological communications and evolving threats. For instance, the use of smartphone devices invites new security threats that could potentially exploit the integrity of PII. Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by October 31, 2018 detailing information security technologies that the Department employs to protect the official unclassified email and official unclassified mobile communications of its employees."