Section 1602, unmanned aircraft systems (UAS) are commercially available, challenging to detect and mitigate, and capable of carrying harmful payloads and performing surveillance while evading traditional ground security measures. However, some of the most promising technical countermeasures for detecting and mitigating UAS may be construed to be illegal under certain laws that were passed when UAS were unforeseen. These laws include statutes

governing electronic communications, access to protected computers, and interference with civil aircraft.

Potential liability under such laws restricts innovation, evaluation, and operational use of technical countermeasures that can address the unique public safety and homeland security threats posed by UAS while minimizing collateral risk. The proposed legislation provides a savings clause under title 18, United States Code, for authorized development or use of such countermeasures.

This legislation provides that development or use of countermeasures against UAS must be pursuant to a coordinated, government-wide policy. A coordinated approach is critical to ensure that development and use of technical countermeasures for detecting and mitigating UAS is consistent with the safety and efficiency of the National Airspace System (NAS), the protection of privacy, civil rights, and civil liberties, and other government-wide equities. Indeed, multiple departments and agencies have responsibility for the safety or security of facilities, locations, installations, and operations that may be vulnerable to threats posed by UAS, including the Department of Homeland Security, the Department of Transportation, the Department of Justice, the Department of Defense, the Department of Energy, the Department of Agriculture, the Department of the Interior, and the Office of the Director of National Intelligence. Multiple departments and agencies also perform important operations that may be vulnerable to threats posed by UAS, including but not limited to: search and rescue operations; medical evacuations; wildland firefighting; patrol and detection monitoring of the United States border; National Security Special Events and Special Event Assessment Ratings events; fugitive apprehension operations and law enforcement investigations; prisoner detention, correctional, and related operations; securing authorized vessels, whether moored or underway; authorized protection of a person or persons; transportation of special nuclear materials; and security, emergency response, or military training and operations. The proposed legislation helps to ensure that authorized members of the Armed Forces and Federal officers, employees, contractors, and other appropriate persons designated by the heads of the executive department and agencies consistent with the requirements of the government-wide policy required by the proposed legislation will not face penalties for protecting those equities in a way that is consistent with other applicable law, including the U.S. Constitution.

Subsection (a) sets forth the savings clause discussed above. Though many provisions in Title 18 may conflict with authorized Counter-UAS activities, certain statutes are especially problematic. For example, sections 2510–2522 of title 18, United States Code (the Wiretap Act), among other things, subject any person who intentionally intercepts the "contents" of electronic communications to fines, imprisonment, and/or civil liability, and sections 3121–3127 of title 18, United States Code (the Pen/Trap Statute), among other things, generally prohibit the installation or use of a device to collect "non-content" information of electronic communications. In addition, section 1030 of title 18, United States Code (the Computer Fraud and Abuse Act) prohibits unauthorized access to and use of "protected computers." These statutes might be construed to prohibit access to or interception of the telemetry, signaling information, or other communications of UAS. Furthermore, any attempt to interfere with the flight of UAS that pose a threat to covered facilities, locations and installations or covered operations may conflict with section 32 of title 18, United States Code (the Aircraft Sabotage Act), which among other things,

imposes fines and criminal penalties on anyone who "damages, destroys, disables, or wrecks any aircraft in the special aircraft jurisdiction of the United States." In the event of unanticipated conflicts with other statutes, and in order to avoid criminalizing critically important activities by government officials that are consistent with the U.S. Constitution, the savings clause also refers generally to "any provision of title 18, United States Code." Congress has previously recognized the importance of ensuring that federal criminal laws in Title 18 do not inadvertently blunt the development or use of UAS countermeasures. The National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2017 contains two sections (Sec. 1697—codified at section 130i of title 10, U.S. Code—and Sec. 3112) authorizing the Department of Defense, and the Department of Energy, respectively, to protect certain facilities and assets from threats posed by UAS. Both sections authorize such activities "[n]otwithstanding any provision of title 18."

Subsection (b) describes the specific actions referenced in subsection (a), which relate to the UAS context. The proposed legislation would generally allow research, testing, training on, and evaluating technical means for countering UAS, as well as the use of technical means to detect, identify, monitor, and track a UAS to evaluate whether it poses a threat to the safety or security of covered facilities, locations, and installations or covered operations. With respect to the use of technical means to re-direct, disable, disrupt control of, exercise control of, seize, or confiscate UAS, the proposed legislation would allow such actions in response to a UAS posing a threat to the safety or security of covered facilities, locations, and installations or covered operations. Subsection (b)(3) of the proposed legislation would allow the use of reasonable force to disable, disrupt, damage or destroy a UAS posing a threat to the safety or security of covered facilities, locations, and installations or covered operations.

Subsection (c) authorizes, but does not require, civil forfeiture of UAS that are subject to authorized actions described in subsection (b).

Subsection (d) provides that the actions in subsections (b) and (c) may be taken only after the issuance of government-wide policy prescribing roles and responsibilities for implementing this section. That policy would be developed in consultation with appropriate departments and agencies, including the Secretary of Transportation to ensure the safety and efficiency of the NAS. Requiring the development of government-wide policy ensures that departments and agencies execute UAS countermeasures in a coordinated and effective manner, and that such activities are subject to appropriate oversight and control. A whole-of-government framework also protects the integrity of the NAS, while permitting departments and agencies to defend covered facilities and operations from malicious uses of UAS. The proposed legislation requires the government-wide policy to (1) respect privacy, civil rights and civil liberties; (2) prescribe roles and processes, as appropriate, to ensure compliance with applicable law and regulations concerning the management of the radio frequency spectrum; (3) consider each Federal department and agency's responsibilities for the safety or security of its facilities and operations; and (4) develop standards and procedures with respect to designations of covered facilities, locations, installations, covered operations, and covered persons, including by requiring that only that only individuals with appropriate training and acting subject to Federal Government oversight may be designated as such.

Subsection (e) provides that departments and agencies must issue policies, procedures, or plans to carry out this section, consistent with any limitations or specifications in the government-wide policy. Departments and agencies may also issue regulations to carry out this section. Subsection (e)(2) provides that departments and agencies must develop the actions issued under this subsection in coordination with the Secretary of Transportation. This provision intends to foster airspace safety by ensuring that departments and agencies engage with the Secretary of Transportation early on to identify and mitigate any potential collateral impacts on the NAS. In the NDAA for FY 2017, Congress similarly recognized the importance of preserving a coordinating role for the Secretary of Transportation in the development of the actions for countering UAS. The term "coordination" in subsection (e)(2) means that the heads of departments and agencies will seek the views, information, and advice of the Secretary of Transportation concerning any potential effects on the NAS as department and agencies develop the types of actions to be taken and the circumstances of execution under this provision. The Secretary of Transportation will provide such views, information, and advice in a reasonably prompt manner. If the Secretary of Transportation notifies the head of a department or agency that taking the proposed actions would affect aviation safety or NAS operations, the head of the department or agency concerned will work collaboratively with the Secretary of Transportation to consider proposed actions to mitigate or otherwise address effects on aviation safety, air navigation services, and NAS efficiency—consistent with national or homeland security and law enforcement requirements—prior to finalizing the types of actions authorized to be taken under this provision.

Subsection (e)(3) requires internal review of regulations, policies, procedures, or plans that would result in the monitoring, interception or other access to wire or electronic communications.

Subsection (f) provides that no court shall have jurisdiction to hear causes or claims, including for money damages, against a federal officer, employee, agent or contractor arising from any authorized actions described in subsections (b). This provision serves to protect individuals taking authorized actions described in subsections (b) from damages claims and official-capacity claims.

Subsection (g) clarifies that the proposed legislation does not affect Federal agencies' authority to continue testing and/or using technical means for countering UAS that comport with title 18, United States Code, and other applicable law, including the aforementioned sections of the NDAA for FY 2017. In addition, the proposed legislation clarifies that it does not restrict or limit the authority of the Federal Aviation Administration, which remains the exclusive Federal agency with authority over the nation's airspace and authority to manage the safe and efficient use of the NAS.

Subsection (h) provides exemptions from disclosure under State and Federal law for information relating to the technology used pursuant to the proposed legislation, and specific policies, procedures, or plans issued thereunder.

Subsection (i) clarifies that "unmanned aircraft" and "unmanned aircraft system" have the meanings given those terms by the FAA Modernization and Reform Act of 2012. The term

“covered facilities, locations and installations” is defined to mean non-mobile assets in the United States that are designated by the respective agency head pursuant to standards and procedures developed in government-wide policy. The term “covered person” is defined to mean any member of the Armed Forces, a Federal officer, employee, agent, or contractor, or any other individual that is designated by the respective department or agency head in accordance with the standards and procedures established in government-wide policy. The term “covered operations” is defined to mean governmental operations that are determined by an agency head, consistent with government-wide policy, to be important to public safety, law enforcement, or national or homeland security.

Subjection (j) provides that the legislation ceases to have effect on December 31, 2022.

A BILL

To authorize appropriations for fiscal year 2018 for military activities of the Department of Defense and for military construction, to prescribe military personnel strengths for such fiscal year, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “National Defense Authorization Act for Fiscal Year 2018”.

SEC. 1602. OFFICIAL ACTIONS TO ADDRESS THREATS POSED BY UNMANNED AIRCRAFT SYSTEMS TO PUBLIC SAFETY OR HOMELAND SECURITY.

(a) AUTHORITY.—Notwithstanding any provision of title 18, United States Code, the head of an Executive department or agency, while respecting privacy, civil rights, and civil liberties, including with regard to the testing of any equipment and the interception or acquisition of communications, may take, and may authorize a covered person to take, the actions described in subsection (b), to the extent otherwise in accordance with law.

(b) ACTIONS DESCRIBED.—The actions described in this subsection are as follows:

(1) Detect, identify, monitor, or track, without prior consent, an unmanned aircraft system, unmanned aircraft, or unmanned aircraft's attached system, payload, or cargo, to evaluate whether it poses a threat to the safety or security of a covered facility, location, or installation or a covered operation, including by means of interception of or other access to wire, oral, electronic, or radio communications or signals transmitted to or by an unmanned aircraft system, unmanned aircraft, or unmanned aircraft's attached system, payload, or cargo.

(2) Redirect, disable, disrupt control of, exercise control of, seize, or confiscate, without prior consent, an unmanned aircraft system, unmanned aircraft, or unmanned aircraft's attached system, payload, or cargo that poses a threat to the safety or security of a covered facility, location, or installation or a covered operation, including by intercepting, substituting, or disrupting wire, oral, electronic, or radio communications or signals transmitted to or by an unmanned aircraft system, unmanned aircraft, or unmanned aircraft's attached system, payload, or cargo.

(3) Use reasonable force to disable, disrupt, damage, or destroy an unmanned aircraft system, unmanned aircraft, or unmanned aircraft's attached system, payload, or cargo that poses a threat to the safety or security of a covered facility, location, or installation or a covered operation.

(4) Conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine its capability and utility to enable any of the actions described in paragraphs (1) through (3).

(c) FORFEITURE.—An unmanned aircraft system, unmanned aircraft, or unmanned aircraft's attached system, payload, or cargo that is disabled, disrupted, seized, controlled, confiscated, damaged, or destroyed pursuant to an action described in subsection (b) is subject to forfeiture to the United States.

(d) GOVERNMENT-WIDE POLICY.—The actions described in subsections (b) and (c) may only be taken following the issuance of Federal Government-wide policy prescribing roles and responsibilities for implementing this section. The Federal Government-wide policy shall be developed in consultation with appropriate departments and agencies, including the Department of Transportation to ensure the safety and efficiency of the National Airspace System, and shall—

(1) respect privacy, civil rights, and civil liberties, including with regard to the testing of any equipment and the interception or acquisition of communications, by, among other things, ensuring that information is intercepted, acquired, accessed, or retained pursuant to subsections (b) only where and for so long as is necessary to support one or more of the department's or agency's authorized functions and is accessible only to covered persons with a need to know the information;

(2) prescribe roles and processes, as appropriate, to ensure that departments and agencies take the actions described in subsection (b) in compliance with applicable law and regulation regarding the management of the radio frequency spectrum;

(3) consider each department's and agency's responsibilities for the safety or security of its facilities, locations, installations, and operations in the United States; and

(4) develop standards and procedures for heads of departments and agencies to designate a covered facility, location, or installation, a covered operation, or a covered person, which shall ensure that only individuals with appropriate training and acting subject to Federal Government oversight are designated as covered persons.

(e) IMPLEMENTATION.—

(1) REGULATIONS; POLICIES, PROCEDURES, OR PLANS.—Consistent with any limitations or specifications in the Federal Government-wide policy issued pursuant to subsection (d), the head of a department or agency—

(A) may prescribe regulations to carry out this section; and

(B) shall issue policies, procedures, or plans to carry out this section.

(2) COORDINATION.—Regulations, policies, procedures, or plans issued under this subsection shall develop the actions in subsection (b) in coordination with the Secretary of Transportation.

(3) PRIVACY REVIEW.—Any regulations, policies, procedures, or plans issued pursuant to this section that would result in the monitoring, interception, or other

access to wire, oral, electronic, or radio communications or signals transmitted to or by an unmanned aircraft system, unmanned aircraft, or unmanned aircraft's attached system, payload, or cargo shall be reviewed consistent with section 522 of the Consolidated Appropriations Act, 2005 (42 U.S.C. 2000ee-2), to ensure that the regulations, policies, procedures, or plans appropriately protect privacy and civil liberties.

(f) JURISDICTION.—Notwithstanding any other provision of law, no court shall have jurisdiction to hear any cause or claim, including for money damages, against a covered person arising from any authorized action described in subsection (b).

(g) RELATIONSHIP TO OTHER LAWS.—Nothing in this section shall be construed to—

(1) restrict the authority of the United States Government, a member of the Armed Forces, or a Federal officer, employee, agent, or contractor from performing any action described in subsection (b) or (c) that is in accordance with law;

(2) affect the exercise of authority granted by section 130i of title 10, United States Code, and section 4510 of the Atomic Energy Defense Act (50 U.S.C. 2661); or

(3) restrict or limit the authority of the Federal Aviation Administration under title 49, United States Code, to manage the safe and efficient use of the National Airspace System.

(h) DISCLOSURE.—Information pertaining to the technology used pursuant to this section, and any regulations, policies, procedures, and plans issued under this section, shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code, and exempt from disclosure under any State or local law requiring the disclosure of information.

(i) DEFINITIONS.—In this section:

(1) The term "covered facility, location, or installation" means any non-mobile asset in the United States that is designated by the head of a department or agency in accordance with standards and procedures established under subsection (d).

(2) The term "covered operation" means—

(A) any operation that is conducted in the United States by a member of the Armed Forces or a Federal officer, employee, agent, or contractor, that is important to public safety, law enforcement, or national or homeland security, and is designated by the head of a department or agency, consistent with the Federal Government-wide policy issued pursuant to subsection (d); and

(B) may include, but is not limited to, search and rescue operations; medical evacuations; wildland firefighting; patrol and detection monitoring of the United States border; a National Security Special Event or Special Event Assessment Ratings event; a fugitive apprehension operation or law enforcement investigation; a prisoner detention, correctional, or related operation; securing an authorized vessel, whether moored or underway; authorized protection of a person; transportation of special nuclear materials; or a security, emergency response, or military training, testing, or operation.

(3) The term "covered person" means any member of the Armed Forces, a Federal officer, employee, agent, or contractor, or any other individual that is designated by the head of a department or agency in accordance with standards and

procedures established under subsection (d), acting within their officially designated capacity.

(4) The terms “intercept” and “wire, oral, electronic, or radio communications” have the meaning given those terms in section 2510 of title 18.

(5) The terms “unmanned aircraft” and “unmanned aircraft system” have the meaning given those terms in section 331 of the FAA Modernization and Reform Act of 2012 (49 U.S.C. 40101 note).

(6) The term “United States” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possessions, territorial seas, or navigable waters of the United States.

(j) SUNSET.—This section shall cease to have effect on December 31, 2022.