COUNTER-UNMANNED AIRCRAFT SYSTEMS NATIONAL ACTION PLAN

LEGISLATIVE PROPOSAL

PROPOSED BILL TEXT

SECTION _____. REAUTHORIZATION.

Section 210G of the Homeland Security Act of 2002 (6 U.S.C. 124n) is amended by striking the existing text and replacing it with the following section:

"SEC. 210G. PROTECTION OF CERTAIN FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT.

"(a) AUTHORITY FOR THE DEPARTMENTS OF HOMELAND SECURITY AND JUSTICE.—Notwithstanding section 46502 of title 49, United States Code, or any provision of title 18, United States Code, the Secretary and the Attorney General may, for their respective Departments, take, and may authorize personnel with assigned duties that include the safety, security, or protection of people, facilities, or assets to take such actions as are described in subsection (d)(2) that are necessary to detect, identify, monitor, track, and mitigate a credible threat (as defined by the Secretary and the Attorney General, in consultation with the Secretary of Transportation through the Administrator of the Federal Aviation Administration) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset.

"(b) ADDITIONAL LIMITED AUTHORITY FOR DETECTION, IDENTIFICATION, MONITORING, AND TRACKING.—

"(1) Notwithstanding sections 1030 and 1367 and chapters 119 and 206 of title 18, United States Code, any State, local, tribal, or territorial law enforcement agency, the Department of Justice, the Department of Homeland Security, and owners or operators of airports or critical infrastructure may authorize personnel, with assigned duties that include the safety, security, or protection of people, facilities, or assets to use equipment

authorized under this subsection to take such actions as are described in subsection (d)(1) that are necessary to detect, identify, monitor, or track an unmanned aircraft system or unmanned aircraft within their respective areas of responsibility or jurisdiction.

"(2) Equipment authorized for unmanned aircraft system detection, identification, monitoring, or tracking under this subsection shall be limited to systems or technologies that have been tested and evaluated by the Department of Homeland Security or Justice; determined by the Federal Communications Commission and the National Telecommunications and Information Administration not to adversely impact the use of the communications spectrum; determined by the Federal Aviation Administration not to adversely impact the use of the aviation spectrum or otherwise adversely impact the national airspace system; and, included on a list of authorized equipment maintained by the Department of Homeland Security, in coordination with the Department of Justice, the Federal Aviation Administration, the Federal Communications Commission, and National Telecommunications and Information Administration.

"(3) State, local, tribal, and territorial law enforcement agencies and owners or operators of airports or critical infrastructure acting pursuant to this subsection—

"(A) Shall, prior to any such action, issue a written policy certifying compliance with the privacy protections of subsections (i)(2)(A) through (D); and

"(B) Shall comply with any additional guidance issued by the Secretary or the Attorney General.

"(4) Nothing in this subsection shall authorize the taking of any action described in subsection (d) other than those described in paragraph (1) of subsection (d).

"(c) PILOT PROGRAM FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL LAW ENFORCEMENT. —

"(1) GENERAL.—The Secretary and the Attorney General may carry out a pilot program to evaluate the potential benefits of State, local, tribal, and territorial law enforcement taking actions that are necessary to mitigate a credible threat that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset.

"(2) DESIGNATION.—The Secretary or the Attorney General, with the concurrence of the other and of the Secretary of Transportation (through the Administrator of the Federal Aviation Administration), may, as part of a pilot program, designate a State, local, tribal or territorial law enforcement agency approved by the respective chief executive officer of each state or territorial or tribal entity to engage in the activities authorized in subsection (c)(4) under the direct oversight of the Departments of Homeland Security or Justice, in carrying out the missions described in subsection (q)(5)(C)(v). The Secretary and the Attorney General may designate between them no more than 12 distinct agencies per year in each 12-month period for a period of five years, to begin six months after the date of enactment of this section, not including any agencies that have been designated previously. After consulting with each other and the Secretary of Transportation (through the Administrator of the Federal Aviation Administration), the Secretary or the Attorney General may revoke a designation, and shall revoke a designation if the other or the Secretary of Transportation through the Administrator of the Federal Aviation Administration withdraws concurrence.

"(3) TERMINATION.—The authority to designate an agency for inclusion in the pilot program under this subsection shall terminate after five years, to begin on a date that is six months after [enactment date]. The authority of a designated agency to exercise any of the authorities granted under the pilot program shall terminate after six years, to begin on a date that is six months after the date of enactment of this section.

"(4) AUTHORIZATION.—Notwithstanding section 46502 of title 49, United States Code, or any provision of title 18, United States Code, any State, local, tribal or territorial law enforcement agency designated pursuant to subsection (c)(2) may authorize personnel with assigned duties that include the safety, security, or protection of people, facilities, or assets to take such actions as are described in subsection (d)(2) that are necessary to detect, identify, monitor, track, or mitigate a credible threat (as defined by the Secretary and Attorney General, in consultation with the Secretary of Transportation, including the Federal Aviation Administration) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset under subsection (q)(5)(C)(v).

"(5) EXEMPTION.— The Federal Communications Commission, in consultation with the National Telecommunications and Information Administration, shall implement a process for considering exemptions of law enforcement agencies so designated or any stations operated by such an agency from a provision of Title III of the Communications Act of 1934, as amended, to the extent that the designated agency takes such actions as are described in subsection (d)(2) and may establish conditions or requirements for such exemption. The Commission may grant such exemptions only if it finds that a grant is necessary to achieve the purposes of this Act and will serve the public interest. Any such

exemption shall terminate automatically if the designation of the agency under paragraph (2) is revoked by the Secretary or the Attorney General.

"(6) REPORTING.—No later than two years after the date on which the first agency is designated under paragraph (2), the Secretary and the Attorney General shall fully inform the appropriate congressional committees in writing about the use of the authorities in paragraph (4).

"(7) OTHER REQUIREMENTS.—Entities acting pursuant to this subsection—

"(A) May do so only using equipment authorized by the Department of Homeland Security, in coordination with the Department of Justice, the Federal Communications Commission, the National Telecommunications and Information Administration, and the Department of Transportation through the Federal Aviation Administration;

"(B) Shall, prior to any such action, issue a written policy certifying compliance with the privacy protections of subsections (i)(2)(A) through (D);

"(C) Must ensure that all personnel undertaking any actions listed under subsection (c) are properly trained according to criteria that the Secretary and Attorney General shall collectively establish, in consultation with the Secretary of Transportation, the Administrator of the Federal Aviation Administration, the Federal Communications Commission, and the Assistant Secretary of Commerce for Communications and Information of the National Telecommunications and Information Administration; and

"(D) Shall comply with any additional guidance issued by the Secretary or Attorney General.

"(d) ACTIONS DESCRIBED.—

"(1) The actions authorized in subsection (b)(1) are the following: during the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

"(2) The actions authorized in subsections (a) and (c)(4) are the following—

"(A) During the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft;

"(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and direct or indirect physical, electronic, radio, and electromagnetic means;

"(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft;

"(D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft;

"(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft; and

"(F) Use reasonable force, if necessary, to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

"(e) RESEARCH, TESTING, TRAINING AND EVALUATION.—

"(1) REQUIREMENT.—Notwithstanding section 46502 of title 49, United States Code, or any provision of title 18, the Secretary, the Attorney General, and the heads of agencies designated pursuant to subsection (c)(2) shall conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine its capability and utility prior to the use of any such technology for any action described in subsection (d). Personnel and contractors who do not have duties that include the safety, security, or protection of people, facilities, or assets may engage in research, testing, training, and evaluation activities pursuant to this section.

"(2) TRAINING OF PERSONNEL.—The Attorney General, through the Director of the Federal Bureau of Investigation, may provide training on measures to mitigate a credible threat that an unmanned aircraft or unmanned aircraft system poses to the safety or security of a covered facility or asset to any personnel who are authorized to take such measures, including personnel authorized to take the actions described in subsection (d), and may establish or designate one or more facilities or training centers for such purpose.

"(3) COORDINATION FOR RESEARCH, TESTING, TRAINING AND EVALUATION.—The Secretary, the Attorney General, and the heads of agencies designated pursuant to

subsection (c)(2) shall coordinate their procedures governing research, testing, training, and evaluation for carrying out any provision in this section with the Administrator of the Federal Aviation Administration before initiating such activities so the Administrator may ensure the activities do not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system. The heads of agencies designated pursuant to subsection (c)(2) shall coordinate their procedures governing research, testing, training, and evaluation, through the Secretary and the Attorney General, with the Federal Aviation Administration.

"(f) FORFEITURE.—Any unmanned aircraft system or unmanned aircraft described in subsection (a) that is seized by the Secretary or the Attorney General is subject to forfeiture to the United States pursuant to the provisions of chapter 46 of title 18, United States Code.

"(g) REGULATIONS AND GUIDANCE.—The Secretary, the Attorney General, and the Secretary of Transportation may prescribe regulations and shall issue guidance in the respective areas of each Secretary or the Attorney General to carry out this section. All guidance and regulations under this subsection shall be developed in consultation with the Federal Communications Commission, the National Telecommunications and Information Administration, and the Federal Aviation Administration.

"(h) COORDINATION.—

"(1) The Secretary and the Attorney General shall coordinate with the Administrator of the Federal Aviation Administration prior to any action authorized by this section so the Administrator may ensure the action does not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.

"(2) Before issuing any guidance, or otherwise implementing this section, the Secretary and the Attorney General shall respectively coordinate with:

(A) the Secretary of Transportation so the Secretary of Transportation may ensure such guidance or implementation does not adversely impact or interfere with any critical national transportation infrastructure; and

(B) the Administrator of the Federal Aviation Administration so the Administrator may ensure such guidance or implementation does not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.

"(3) The Secretary and the Attorney General shall coordinate the development of their respective guidance under subsection (g) with the Secretary of Transportation through the Administrator of the Federal Aviation Administration.

"(4) The Secretary and the Attorney General, and the heads of any agencies designated pursuant to subsection (c)(2), through the Secretary and the Attorney General, shall coordinate the development for their respective Departments or agencies of the actions described in subsection (d) with the Secretary of Transportation (through the Administrator of the Federal Aviation Administration) and the Assistant Secretary of Commerce for Communications and Information of the National Telecommunications and Information Administration.

"(5) Prior to any action authorized by subsection (c)(4), the heads of agencies designated under subsection (c)(2) shall coordinate, through the Secretary and the Attorney General—

"(A) with the Secretary of Transportation, so that the Administrators of non-aviation modes of the Department of Transportation may elevate whether the action has adverse impacts on critical non-aviation transportation infrastructure;

"(B) with the Administrator of the Federal Aviation Administration, so the Administrator may ensure the action has no adverse impact or would not interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system; and

"(C) to allow the Departments of Justice and Homeland Security to ensure that any action authorized by this section is consistent with Federal law enforcement or in the interest of national security.

"(i) PRIVACY PROTECTION.—

"(1) The regulations or guidance issued to carry out actions authorized under subsection (d) by the Secretary or the Attorney General, as the case may be, shall ensure for their respective departments that—

"(A) the interception or acquisition of, or access to, or maintenance or use of, communications to or from an unmanned aircraft system under this section is conducted in a manner consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal law;

"(B) communications to or from an unmanned aircraft system are intercepted or acquired only to the extent necessary to support an action described in subsection (d);

"(C) records of such communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Secretary or the

Attorney General determine that maintenance of such records is required under Federal law; is necessary for the purpose of any litigation; or is necessary to investigate or prosecute a violation of law, directly support an ongoing security operation, or protect against dangerous or unauthorized activity by unmanned aircraft systems or unmanned aircraft; and

"(D) such communications are not disclosed outside the Department of Homeland Security or the Department of Justice unless the disclosure—

"(i) is necessary to investigate or prosecute a violation of law;

"(ii) would support the Department of Defense, a Federal law enforcement, intelligence, or security agency, a State, local, tribal, or territorial law enforcement agency, or other relevant entity or person if such entity or person is engaged in a security or protection operation;

"(iii) is necessary to support a department or agency listed in clause (ii) in investigating or prosecuting a violation of law;

"(iv) would support the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory, statutory, or other enforcement action relating to, an action described in subsection (d);

"(v) is between the Department of Homeland Security and the Department of Justice in the course of a security or protection operation of either agency or a joint operation of such agencies; or

"(vi) is otherwise required by law;

"(2) In exercising the authorities described in subsections (b) or (c), State, local, tribal, and territorial law enforcement agencies and owners or operators of airports or critical infrastructure shall ensure that—

"(A) the interception or acquisition of, or access to, or maintenance or use of, communications to or from an unmanned aircraft system under this section is conducted in a manner consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal, and where required, State, local, tribal, and territorial law;

"(B) communications to or from an unmanned aircraft system are intercepted or acquired only to the extent necessary to support an action described in subsection (d);

"(C) records of such communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Secretary, the Attorney General, or the head of an agency designated under subsection (c) determines that maintenance of such records is required under Federal, State, local, tribal, or territorial law; is necessary for the purpose of any litigation; or is necessary to investigate or prosecute a violation of law, directly support an ongoing security operation, or protect against dangerous or unauthorized activity by unmanned aircraft systems or unmanned aircraft; and

"(D) such communications are not disclosed outside the agency or entity unless the disclosure—

"(i) is necessary to investigate or prosecute a violation of law;

"(ii) would support the Department of Defense, a Federal law enforcement, intelligence, or security agency, or a State, local, tribal, or territorial law enforcement agency;

"(iii) would support the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory, statutory, or other enforcement action relating to, an action described in subsection (d);

"(iv) is to the Department of Homeland Security or the Department of Justice in the course of a security or protection operation of either agency or a joint operation of such agencies; or

"(v) is otherwise required by law.

"(j) BUDGET.— The Secretary and the Attorney General shall submit to Congress, as a part of the homeland security or justice budget materials for each fiscal year after fiscal year 2023, a consolidated funding display that identifies the funding source for the actions described in subsection (d) within the Department of Homeland Security or the Department of Justice. The funding display shall be in unclassified form but may contain a classified annex.

"(k) PUBLIC DISCLOSURES.—

"(1) Notwithstanding any other provision of State, local, tribal, or territorial law, the following information shall be governed exclusively by the disclosure obligations set forth in section 552 of title 5, United States Code—

"(A) Information pertaining to the capabilities, limitations, or sensitive details of the specific operation of the technologies used to carry out activities described in subsection (d)(1) of this section.

"(B) Operational procedures and protocols used to carry out this section.

"(2) Information described in subsection (k)(1) that is obtained by a State, local, tribal, or territorial agency from a Federal agency under this section shall remain subject to the control of the Federal agency, notwithstanding that the State, local, tribal, or territorial agency has the information in its possession, and any State, local, tribal, or territorial law authorizing or requiring disclosure shall not apply to such information. Any requests for public access to this information shall be submitted to the originating Federal agency which shall process the request as required by section 552(a)(3) of title 5, United States Code.

"(l) ASSISTANCE AND SUPPORT.—

"(1) FACILITIES AND SERVICES OF OTHER AGENCIES AND NON-FEDERAL ENTITIES.—The Secretary or Attorney General is authorized to use or accept from any other federal agency, or any other public or private entity supplies or services to facilitate or take the actions provided for in subsection (d). The Secretary and the Attorney General may accept such supplies or services with or without reimbursement and notwithstanding any provision of law that would prevent such use or acceptance. The Secretary and the Attorney General in implementing (q)(5)(C) may enter into agreements with other executive agencies and with appropriate officials of other non-federal public or private agencies or entities, as may be necessary and proper to carry out their responsibilities under this section.

"(2) MUTUAL SUPPORT.—The Secretary or Attorney General are authorized to provide support or assistance, upon the request of an agency or department conducting a mission specified in section (q)(5)(C), or a mission specified in section 130i of title 10,

United States Code, or section 4510 of the Atomic Energy Defense Act (50 U.S.C. 2661), in fulfilling the requesting agency's or department's roles and responsibilities for that mission, when exigent circumstances exist, limited to a specified timeframe and location, within available resources, on a non-reimbursable basis, in coordination with the Federal Aviation Administration.

"(m) SEMIANNUAL BRIEFINGS AND NOTIFICATIONS.—

"(1) IN GENERAL.—On a semiannual basis beginning 6 months after the date this section is enacted, the Secretary and the Attorney General shall, respectively, provide a briefing to the appropriate congressional committees on the activities carried out pursuant to this section.

"(2) REQUIREMENT.—Each briefing required under paragraph (1) shall be conducted jointly with the Secretary of Transportation.

"(3) CONTENT.—Each briefing required under paragraph (1) shall include—

"(A) policies, programs, and procedures to mitigate or eliminate impacts of such activities to the national airspace system and other critical national transportation infrastructure;

"(B) a description of instances in which actions described in subsection (d) have been taken, including all such instances that may have resulted in harm, damage, or loss to a person or to private property;

"(C) a description of the guidance, policies, or procedures established to address privacy, civil rights, and civil liberties issues implicated by the actions allowed under this section, as well as any changes or subsequent efforts that would significantly affect privacy, civil rights, or civil liberties;

"(D) a description of options considered and steps taken to mitigate any identified impacts to the national airspace system related to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (d)(2);

"(E) a description of instances in which communications intercepted or acquired during the course of operations of an unmanned aircraft system were held for more than 180 days or shared outside of the Department of Justice or the Department of Homeland Security;

"(F) how the Secretary, the Attorney General, and the Secretary of Transportation have informed the public as to the possible use of authorities under this section;

"(G) how the Secretary, the Attorney General, and the Secretary of Transportation have engaged with Federal, State, tribal, and local law enforcement agencies to implement and use such authorities;

"(H) an assessment of whether any gaps or insufficiencies still remain in current authorities, regulations, and policies that impede the ability of the Federal Government, State, tribal, and local governments, and critical infrastructure owners or operators to counter the threat posed by the malicious use of UAS;

"(I) recommendations to remedy any such gaps or insufficiencies, including but not limited to necessary changes in law, regulations, or policies;

"(J) a description of the impact of the authorities granted under this section on lawful operator access to national airspace, and UAS integration into the national airspace system; and

"(K) a summary from the Secretary, if applicable, on any data and results obtained pursuant to section (r), including an assessment of how the details of the incident were obtained and whether the operation involved a violation of Federal Aviation Administration aviation regulations.

"(4) UNCLASSIFIED FORM.—Each briefing required under paragraph (1) shall be in unclassified form but may be accompanied by an additional classified briefing.

"(5) NOTIFICATION.—Within 30 days after an authorized department or agency deploys any new technology to carry out the actions described in subsection (d), the Secretary and the Attorney General shall, respectively or jointly as appropriate, submit a notification to the appropriate congressional committees. Such notification shall include a description of options considered to mitigate any identified impacts to the national airspace system related to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (d).

"(n) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

"(1) vest in the Secretary, the Attorney General, or any agency designated under subsection (c), any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration;

"(2) vest in the Secretary of Transportation, the Administrator of the Federal Aviation Administration, or any agency designated under subsection (c), any authority of the Secretary or the Attorney General;

"(3) vest in the Secretary or any agency designated under subsection (c) any authority of the Attorney General;

"(4) vest in the Attorney General or any agency designated under subsection (c) any authority of the Secretary; or

"(5) provide a new basis of liability for any state, local, tribal, or territorial law enforcement officers designated under subsection (c) or who participate in the protection of a mass gathering identified by the Secretary or Attorney General under subsection (n)(4)(C)(iii)(II), act within the scope of their authority, and do not exercise the authority granted to the Secretary and Attorney General by this section.

"(o) TERMINATION.—The authority to carry out any action authorized in this section under subsection (c), or any action authorized in this section under subsection (b) if performed by a non-federal entity, shall terminate on the date that is five years and six months after [enactment date], except for any authority to operate given to a State, local, tribal, or territorial entity pursuant to subsection (c)(2), which shall terminate on the date that is six years and six months after [enactment date].

"(p) SCOPE OF AUTHORITY.—Nothing in this section shall be construed to provide the Secretary or the Attorney General with additional authorities beyond those described in subsections (a), (b), (c), (e), and (q)(5)(C)(iii).

"(q) DEFINITIONS.—In this section—

"(1) The term "air navigation facility" has the meaning given that term in section 40102(a)(4) of title 49, United States Code.

"(2) The term "airport" has the meaning given that term in section 47102(2) of title 49, United Sates Code.

"(3) The term "appropriate congressional committees" means—

"(A) the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on the Judiciary of the Senate; and

"(B) the Committee on Homeland Security, the Committee on Transportation and Infrastructure, the Committee on Energy and Commerce, and the Committee on the Judiciary of the House of Representatives.

"(4) The term "budget", with respect to a fiscal year, means the budget for that fiscal year that is submitted to Congress by the President under section 1105(a) of title 31, United States Code.

"(5) The term "covered facility or asset" means any facility or asset that—

"(A) is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Secretary or the Attorney General, or by the chief executive of the jurisdiction in which an agency designated pursuant to subsection (c) operates after review and approval of the Secretary or the Attorney General, in coordination with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section. In the case of the missions described in subparagraph (C)(i)(II) and (C)(iii)(I), such missions shall be presumed to be for the protection of a facility or

asset that is assessed to be high-risk and a potential target for unlawful unmanned aircraft activity;

"(B) is located in the United States (including the territories and possessions, territorial seas or navigable waters of the United States); and

"(C) directly relates to one or more—

"(i) missions authorized to be performed by the Department of Homeland Security, consistent with governing statutes, regulations, and orders issued by the Secretary, pertaining to—

"(I) security or protection functions of the U.S. Customs and Border Protection, including securing or protecting facilities, aircraft, and vessels, whether moored or underway;

"(II) United States Secret Service protection operations pursuant to sections 3056(a) and 3056A(a) of title 18, United States Code, and the Presidential Protection Assistance Act of 1976 (18 U.S.C. 3056 note);

"(III) protection of facilities pursuant to section 1315(a) of title 40, United States Code; or

"(IV) transportation security functions of the Transportation Security Administration.

"(ii) missions authorized to be performed by the Department of Justice, consistent with governing statutes, regulations, and orders issued by the Attorney General, pertaining to—

"(I) personal protection operations by—

"(aa) the Federal Bureau of Investigation as specified in section 533 of title 28, United States Code; and

"(bb) the United States Marshals Service as specified in section 566 of Title 28, United Stated Code.

"(II) protection of penal, detention, and correctional facilities and operations conducted by the Federal Bureau of Prisons and prisoner operations and transport conducted by the United States Marshals Service;

"(III) protection of the buildings and grounds leased, owned, or operated by or for the Department of Justice, and the provision of security for Federal courts, as specified in section 566 of title 28, United State Code; or

"(IV) protection of an airport or air navigation facility;

"(iii) missions authorized to be performed by the Department of Homeland Security or the Department of Justice, acting together or separately, consistent with governing statutes, regulations, and orders issued by the Secretary or the Attorney General, respectively, pertaining to—

"(I) protection of a National Special Security Event (NSSE) and Special Event Assessment Rating (SEAR) event;

"(II) the provision of support to State, local, tribal, or territorial law enforcement, upon request of the chief executive officer of the State or territory, to ensure protection of people and

property at mass gatherings, that is limited to a specified timeframe and location, within available resources, and without delegating any authority under this section to State, local, tribal, or territorial law enforcement;

"(III) protection of an active Federal law enforcement investigation, emergency response, or security function, that is limited to a specified timeframe and location;

"(IV) the provision of security or protection support to critical infrastructure owners or operators, for static critical infrastructure facilities and assets upon their request;

"(iv) missions authorized to be performed by the United States Coast Guard, including those described in clause (iii) as directed by the Secretary, and as further set forth in section 528 of title 14, United States Code, and consistent with governing statutes, regulations, and orders issued by the Secretary of the Department in which the Coast Guard is operating; and

"(v) responsibilities of agencies designated pursuant to subsection (c) pertaining to—

"(I) protection of NSSEs, SEAR events, or other mass gatherings within the agency's jurisdiction;

"(II) protection of critical infrastructure assessed by the Secretary as high-risk for Unmanned Aircraft System attack or disruption, including airports within the agency's jurisdiction; or

"(III) protection of sensitive government buildings, assets, or facilities within the agency's jurisdiction.

"(6) The term "critical infrastructure" has the meaning given that term in section 1016(e) of Public Law 107-56 (42 U.S.C. 5195c(e)).

"(7) The terms "electronic communication", "intercept", "oral communication", and "wire communication" have the meaning given those terms in section 2510 of title 18, United States Code.

"(8) The term "homeland security or justice budget materials", with respect to a fiscal year, means the materials submitted to Congress by the Secretary and the Attorney General in support of the budget for that fiscal year.

"(9) The term "personnel" means:

"(A) officers, employees, and contractors of the Department of Homeland Security and the Department of Justice, with assigned duties that include safety, security, or protection of personnel, facilities, or assets, and employees authorized to perform law enforcement and security functions on behalf of agencies designated under subsection (c) who are trained and certified to perform such duties, including training specific to countering unmanned aircraft threats and mitigating risks in the national airspace. To qualify for use of the authorities in subsections (a) and (b), contractors conducting operations under subsections (a) and (b) must:

"(i) be directly contracted by the federal department or agency;

"(ii) operate at a government owned or government leased facility or asset;

"(iii) not conduct inherently governmental functions; and

"(iv) be trained and certified by the contracting department or agency to meet established department guidance and regulations.

"(B) for purposes of subsection (b)(1), personnel also includes officers, employees, and contractors with assigned duties that include the safety, security, or protection of people, facilities, or assets, of;

"(i) State, local, tribal or territorial law enforcement agencies; and

"(ii) owners or operators of airports or critical infrastructure.

"(10) The terms "unmanned aircraft" and "unmanned aircraft system" have the meanings given those terms in section 44801, of title 49, United States Code.

"(11) For purposes of this section, the term "risk-based assessment" includes an evaluation of threat information specific to a covered facility or asset and, with respect to potential impacts on the safety and efficiency of the national airspace system and the needs of law enforcement and national security at each covered facility or asset identified by the Secretary, the Attorney General, respectively, of each of the following factors—

"(A) Potential impacts to safety, efficiency, and use of the national airspace system, including potential effects on manned aircraft and unmanned aircraft systems, aviation safety, airport operations, infrastructure, and air navigation services related to the use of any system or technology for carrying out the actions described in subsection (d)(2).

"(B) Options for mitigating any identified impacts to the national airspace system related to the use of any system or technology, including minimizing when

possible the use of any technology which disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (d)(2).

"(C) Potential consequences of the impacts of any actions taken under subsection (b)(1) to the national airspace system and infrastructure if not mitigated.

"(D) The ability to provide reasonable advance notice to aircraft operators consistent with the safety of the national airspace system and the needs of law enforcement and national security.

"(E) The setting and character of any covered facility or asset, including whether it is located in a populated area or near other structures, whether the facility is open to the public, whether the facility is also used for nongovernmental functions, and any potential for interference with wireless communications or for injury or damage to persons or property.

"(F) The setting, character, timeframe, and national airspace system impacts of National Special Security Event and Special Event Assessment Rating events to the extent not already discussed in the National Special Security Event and Special Event Assessment Rating nomination process.

"(G) Potential consequences to national security, public safety, or law enforcement if threats posed by unmanned aircraft systems are not mitigated or defeated.

"(r) U.S. GOVERNMENT DATABASE.— The Department of Homeland Security is authorized to develop a U.S. government database to enable the transmission of Federal, State, local, tribal and territorial law enforcement data concerning security-related incidents in the

United States (including the territories and possessions, territorial seas or navigable waters of the United States) involving unmanned aircraft and unmanned aircraft systems for purposes of conducting analyses of such threats in the United States. Prior to implementation of the U.S. government database, the Secretary shall develop policy, plans, and procedures for the implementation of such a database in coordination with the Attorney General, the Secretary of Defense, and the Secretary of Transportation through the Administrator of the Federal Aviation Administration, including the development of criteria for Federal, State, local, tribal and territorial UAS incident reporting."

Proposed Reauthorization of the Preventing Emerging Threats Act (6 U.S.C. § 124n) – Section-by-Section Analysis

Background

In the Preventing Emerging Threats Act of 2018 ("the Act"), Congress granted authority to the Department of Homeland Security ("DHS") and the Department of Justice ("DOJ") to engage in activities to protect covered facilities and assets against credible threats posed by unmanned aircraft or unmanned aircraft systems ("UAS"), notwithstanding laws such as the Wiretap Act or the Aircraft Sabotage Act, that could otherwise limit such activities. The Federal Bureau of Investigation ("FBI") has used the authority to protect numerous large public events, such as the Super Bowl. DHS components, including the U.S. Secret Service and the Federal Protective Service, have used UAS detection and counter-UAS technologies over 200 times, often in sensitive protective missions. As the Act requires, the operations have been conducted in close coordination with the Department of Transportation and pursuant to DHS and DOJ guidance, which addresses how authorized Department agencies and components may exercise the authority granted by the Act. The authority expires on October 5, 2022. The importance of this authority and the successful four-year track record of implementation support making it permanent.

In congressional testimony in 2018, FBI Director Christopher Wray provided the FBI's assessment that "given their retail availability, lack of verified identification requirement to procure, general ease of use, and prior use overseas, UAS will be used to facilitate an attack in the United States against a vulnerable target, such as a mass gathering."[1] This continues to be the FBI's assessment and it is now the Intelligence Community's assessment as well. Since 2018, the number of UAS flights has increased. It remains difficult for law enforcement to distinguish dangerous UAS from UAS flown by responsible operators. The Federal Aviation Administration ("FAA") reports that there are over 800,000 registered UAS in the United States.[2]

One of the most significant UAS incursions outside a combat zone took place at the United Kingdom's Gatwick Airport. The incursion led to the diversion or cancellation of more than 1,000 flights, affected over 140,000 passengers, and caused significant financial losses.[3] A UAS also disrupted flights at Newark International Airport in New Jersey.[4] Such incidents illustrate the ease with which UAS can upend operations without being identified or the operators facing consequences. According to the Federal Aviation Administration (FAA), reports of UAS "sightings from pilots, citizens and law enforcement have increased dramatically over the past two years." The FAA "now receives more than 100 such reports each month." While a

[1] Statement of FBI Director Christopher Wray, Senate Homeland Security and Governmental Affairs Committee, "Threats to the Homeland" hearing, Oct. 10, 2018.
[2] *Drones by the Numbers*, FEDERAL AVIATION ADMINISTRATION (Feb. 23, 2022, 9:51:42 AM), https://www.faa.gov/uas/resources/by_the_numbers/ (according to the FAA, as of February 23, 2022, there were 858,242 registered drones in the United States).
[3] Justin Rowlatt, *Gatwick Drone Attack Possible Inside Job, Say Police*, BBC NEWS (Apr. 14, 2019), https://www.bbc.com/news/uk-47919680.
[4] *Mitigating the Risk of UAS Incursions*, BUS. AVIATION INSIDER (July 1, 2019), https://nbaa.org/aircraft-operations/emerging-technologies/uas/mitigating-risk-uas-incursions/.

sighting is an unconfirmed report of a UAS and may not be indicative of unlawful or even dangerous UAS activity, there were nearly 700 such sightings in the fourth quarter of 2021.[5]

Of even greater concern is the threat UAS pose in the hands of terrorists, criminals, and nation-state adversaries. Terrorist and armed groups overseas, such as the Houthis in Yemen and Shiite militia groups in Iraq, increasingly turn to armed UAS to conduct attacks. Terrorist groups continue to develop such capabilities[6] and may receive support from Iran or other state sponsors. In the United States, criminals, including drug cartels, regularly use UAS for smuggling contraband into prisons, cross-border trafficking, and related surveillance. Mexican narco-terrorist gangs are using weaponized UAS only a short distance from the U.S. border to conduct bombings and other attacks.[7] Adversaries can also use UAS to surveil sensitive sites, interfere with government operations, place surveillance and espionage devices, or enable cyber intrusion operations. The threat will grow rapidly as technology advances, including technology that can link UAS together as a swarm.[8]

The proposed legislation

The proposed legislation would permanently authorize the critical authority Congress provided to DHS and DOJ in 2018. Based on experience implementing the Act, the Administration recommends expanding the legislation in targeted areas, subject to the same or similar detailed limitations in the existing statute.

Specifically, the legislation would enhance the existing authority in the Act in each of the important areas listed below. Each would be subject to the statute's requirements for close coordination with the FAA. Following a six-month NSC-led policy process with contributions from all interagency stakeholders, the Administration seeks the expansion of the existing authority in each of these areas.

(1) The legislation would authorize DOJ and DHS ("the departments") to use the authority in the Act to protect airports from UAS-based threats. The existing statute does not clearly authorize using UAS mitigation (*i.e.*, counter-UAS) authorities to provide ongoing or long-term protection to airports.

(2) The legislation would authorize the departments to use the authority in the Act to protect critical infrastructure.

---

[5] *UAS Sightings Report,* FEDERAL AVIATION ADMINISTRATION (Dec. 21, 2021), https://www.faa.gov/uas/resources/public_records/uas_sightings_report/.

[6] *See, e.g.*, Don Rassler, Muhammad al-'Ubaydi, *Anticipating Future Directions of Tech-Enabled Terror*, LAWFARE BLOG (Dec. 12, 2021), https://www.lawfareblog.com/anticipating-future-directions-tech-enabled-terror (last visited Dec. 23, 2021).

[7] See, *e.g.*, Karol Suarez, *Drug Cartels Attack Enemies and Spread Terror with Weaponized Drones in U.S., Mexico*, COURIER JOURNAL (May 24, 2021), https://www.courier-journal.com/story/news/crime/2021/05/24/el-mencho-cjng-mexican-drug-lords-use-drones-spread-terror/5131708001/ (last visited Dec. 23, 2021).

[8] Tom Donilon, *The Drone Threat Comes Home*, FOREIGN AFFAIRS (Jan. 28, 2022), https://www.foreignaffairs.com/articles/world/2022-01-28/drone-threat-comes-home (Feb. 23, 2022).

(3) The legislation would authorize state, local, tribal, and territorial ("SLTT") entities; and owners or operators of airports or critical infrastructure; to use certain UAS detection-only capabilities subject to specified conditions and safeguards. That technology would be tested and evaluated by DHS or DOJ and approved by the FAA, the Federal Communications Commission ("FCC"), and the National Telecommunications and Information Administration ("NTIA"). The activities would be governed by the privacy requirements in the Act and guidance from DOJ and DHS, coordinated with the FAA.

(4) The legislation would authorize a limited pilot program, subject to a five-year sunset provision, under which DHS and DOJ could designate annually up to 12 SLTT entities to use the detection and mitigation authorities in the Act, subject to oversight by DOJ and DHS and approval by FAA.

To ensure airspace safety and the proper use of the radiofrequency spectrum, the proposed legislation requires coordination with the FAA and FCC. The legislation also maintains the existing statute's strong privacy protections. The legislation by itself will not eliminate the threats presented by malicious and irresponsible use of UAS but it builds on the departments' strong track record implementing the existing authority to enhance the nation's ability to mitigate the threat. This is done in a manner that is measured, responsible, and consistent with the FAA mandate to integrate UAS safely into the national airspace system.

Subsection (a) – Authorities granted to the Departments of Homeland Security and Justice

The legislative proposal amends subsection (a) of the Act in the following three ways:

First, it amends the language in the notwithstanding clause of the section to conform to the notwithstanding clause in 10 U.S.C. § 130i, the counter-UAS authority for the Department of Defense ("DOD"). The current statute provides the Attorney General and Secretary of Homeland Security the authority to engage in the actions authorized by the Act "[n]otwithstanding . . . sections 32, 1030, 1367 and chapters 119 and 206 of Title 18." These provisions generally prohibit aircraft sabotage, computer fraud and abuse, interfering with the operation of a satellite, wiretapping, and the use of pen registers and trap-and-trace devices. The proposal would grant the authority "[n]otwithstanding any provision of Title 18," consistent with the language in 10 U.S.C. § 130i. Besides conforming the provision to section 130i of Title 10, this change simplifies the implementation of section 124n by clarifying that the actions authorized under the Act and implementing guidance do not violate any criminal laws. This will eliminate a potential source of delay in reviewing and approving operations.

Second, the proposal would clarify that the requirement for the Secretary and Attorney General to consult with the Secretary of Transportation may be satisfied by consultation with the Administrator of the FAA. Specifically, the new language would provide that the authorized actions must be undertaken "in consultation with the Secretary of Transportation through the Administrator of the Federal Aviation Administration." This change would streamline the formal process for concurrence while allowing the FAA to continue to consult with the Secretary of Transportation as necessary.

Third, it makes a conforming change to the title of the subsection to account for the new authorities provided to other entities in new subsections (b) and (c). The change in title of the subsection from "Authority" to "Authority for the Departments of Homeland Security and Justice" describes more clearly the scope of the subsection.

Subsection (b) – Detection-only equipment

Subsection (b) of the proposed legislation would authorize SLTT law enforcement agencies and owners or operators of airports or other critical infrastructure to use equipment to detect UAS notwithstanding the federal laws that may otherwise bar its use.[9] The equipment must be approved for use by the federal government pursuant to a list of authorized equipment to be maintained by the Secretary, in coordination with the Attorney General, Secretary of Defense, and Administrator of the Federal Aviation Administration. It does not authorize the use of counter-UAS systems, technologies, or capabilities under any circumstances. This provision does not authorize the use of capabilities that go beyond monitoring UAS traffic, such as a capability that would allow the operator to disrupt a drone's flight. In addition, for the departments, the new subsection would authorize the use of such equipment for missions beyond those specifically identified in the existing statute. Many detection technologies can monitor UAS activities in ways that do not adversely affect the safety and efficiency of the airspace. Some emit low levels of signals and others do not emit signals that are likely to harm either manned or unmanned aviation. Indeed, inclusion on the DHS list of authorized equipment would be predicated on a determination by the FAA that the system or technology (based on specified technical settings and parameters) does not adversely impact the national airspace system. Any non-federal entity using detection-only authority must issue a written policy certifying compliance with the privacy protections set forth in subsections (i)(2)(A) through (D) and comply with any guidance issued by the Secretary of the Attorney General.

Notably, this provision will only apply to detection equipment that has been:

- Tested and evaluated by DHS or DOJ.
- Determined by the NTIA and the FCC "not to adversely impact the use of the communications spectrum."
- Determined by the FAA "not to adversely impact the use of the aviation spectrum or otherwise adversely impact the national airspace system."

Detection-only capabilities may assist SLTT law enforcement agencies and the operators of critical infrastructure in carrying out important missions. For example, the capabilities could enable:

[9] These are the provisions of Title 18 most likely to restrict the use of detection technologies: section 1030 ("Fraud and related activity in connection with computers"); section 1367 ("Interference with the operation of a satellite"); chapter 119 ("Wire and electronic communications interception and interception of oral communications"); and chapter 206 ("Pen registers and trap and trace devices").

- The operator of an oil refinery to detect an unauthorized UAS operating nearby and take precautions with respect to the refinery, such as sounding an alarm. Additionally, the operator may be able to seek help from law enforcement.

- An airport operator to detect an unauthorized UAS near a runway and respond accordingly, consistent with established airport response plans.

- A local police department to detect an unauthorized UAS approaching a crowded political protest or sports event and take safety precautions or locate the operator.

For the departments, this authority may aid other missions besides those specifically identified elsewhere in the Act. For example:

- An agency such as Customs and Border Protection may be conducting its own UAS or manned flight operations in an area and need awareness of UAS traffic.

- An agency such as the Drug Enforcement Administration ("DEA") may need to detect UAS as they are used in drug trafficking or determine whether DEA personnel conducting enforcement activities are under surveillance by drug cartels using UAS.

DHS and DOJ would not be required to coordinate further with the FAA prior to use of certain detection-only technologies once they have been authorized for use via inclusion of the system, with specified parameters for use, in the DHS list of authorized equipment, as FAA coordination would have been completed prior to such inclusion to ensure the system as authorized would not have adverse impacts on the national airspace system. However, the established coordination provisions in subsection (h) would apply to any other DHS or DOJ proposed research, testing, training, evaluation, or other use of a UAS detection capability not included in the DHS list of authorized equipment or which would involve use under different technical parameters or settings from what has been previously coordinated with the FAA.

Subsection (c) – SLTT pilot program

Subsection (c) would authorize a temporary pilot program under which a limited number of approved SLTT law enforcement entities could engage in authorized UAS detection and mitigation activities following federal safeguards, notwithstanding the federal laws that may otherwise bar such activities. It takes an interim, temporary step that will let Congress, the Executive Branch, and the State, local, tribal, and territorial agencies evaluate the costs and benefits associated with a possible future expansion of the authority. The proposal is a first step to address the problem that the departments do not have the equipment and personnel needed to deploy counter-UAS measures to the many events and locations that may be subject to dangerous UAS activity, especially as the number of UAS in the airspace proliferates. The departments must turn down many requests to protect significant events, including requests from state governors.

Participation in the pilot will be subject to numerous protections, including:

- The Secretary, the Attorney General, and the Administrator of the FAA all must concur in the designation of each participating SLTT law enforcement agency.

- If any one of the concurring officials withdraws concurrence, the designation will be revoked.

- The governor of the state (or the chief executive officer of a territorial or tribal entity) must approve the participation by the SLTT agency.

- Because regulation of spectrum uses by SLTT entities, unlike that of federal entities, is subject to FCC authority under Title III of the Communications Act of 1934, the FCC is given authority to issue exemptions from the statutory requirements to the extent necessary to allow their participation in the pilot program.

- The SLTT agency may only use equipment that DHS has approved after a process that involves coordination with other federal agencies.

- The SLTT agency must conduct its counter-UAS activities under the "direct oversight" of DHS or DOJ, which would be required to coordinate each proposed use (including testing) of a system on behalf of the pilot program participant, with the FAA.

- The SLTT agency must comply with any additional guidance issued by the Secretary or the Attorney General, including requirements for development of an operational response plan, training of personnel, and issuance of a written policy certifying compliance with the privacy protections set forth in subsections (i)(6) through (9). These requirements are similar to those that apply to the use of the detection-only authority described above.

The pilot program will begin six months after its authorization by Congress. Once the program begins, the Secretary and the Attorney General may, between them, identify up to 12 participating agencies in each of the five following years, for a total of up to 60 participants over the course of five years. At the end of the five-year designation period, the designations will continue to be effective for one additional year, provided that the Secretary, the Attorney General, and the Administrator of the FAA continue to concur on an agency's participation. Without this additional year, a pilot program participant designated in the last year would have very little time to use the counter-UAS authorities.

Two years after the first SLTT agency designation, the Departments are to "fully inform the appropriate congressional committees . . . about the use of the authorities" under the pilot program.

Subsection (d) – Counter-UAS actions

Subsection (d) identifies the actions to protect against drone threats that authorized entities may take in accordance with subsections (a) through (c), respectively. It is closely modeled on the current statute, and paragraphs (d)(2)(A) – (F) of the proposed legislation are identical to paragraphs (b)(1)(A) – (F) of the current statute.

The principal change in the proposed statute is the addition of a new paragraph (1). The new paragraph lists only actions to "detect, identify, monitor, and track" drones and is included to identify separately the subset of actions that may be taken using the detection-only authority provided in new subsection (b), as described above.

Subsection (e) – Research, testing, training, and evaluation

1. Subsection (e)(1)

Consistent with subsections (b)(3) and (b)(4) of the existing statute, subsection (e)(1) of the draft legislation provides that "[t]he Secretary and the Attorney General shall conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine its capability and utility prior to the use of any such technology for any action described in subsection (b)(1)." Subsection (e)(1), however, provides the following three additions to the testing provisions in the existing statute:

First, it provides that the Secretary and Attorney General shall conduct specified testing activities "notwithstanding sections 46502 of title 49 or any provision of title 18." The testing mandate above, in the existing statute, does not include a notwithstanding clause. The testing provision should clearly state that testing activities carried out consistent with the statute do not violate criminal laws, which is the intent. The wording of the notwithstanding clause conforms to the change to the notwithstanding clause discussed above with respect to subsection (a).

Second, it provides that, in addition to the Secretary and Attorney General, "the heads of agencies designated pursuant to subsection (c)(2) shall conduct [the specified testing activities]." This language accounts for the entities that may be authorized under the SLTT pilot in subsection (c). The SLTT agencies need to have the authority to conduct research, testing, training, and evaluation of the tools that the proposed legislation would authorize them to use under direct federal oversight, subject to appropriate coordination with the FAA. Therefore, the proposed legislation adds the heads of agencies designated pursuant to subsection (c)(2) to the list of actors expected to conduct research, testing, training, and evaluation prior to use of equipment.

Third, it provides that "[p]ersonnel and contractors who do not have duties that include the safety, security, or protection of people, facilities, or assets may engage in research, testing, training, and evaluation activities pursuant to this section." It is important to clarify that for such activities, which do not involve operations, relevant departments and agencies can draw on a wider range of personnel, including contractors, with expertise in counter-UAS technology.

2. Subsection (e)(2)

This new provision provides that the Attorney General, through the Director of the FBI:

> may provide training on measures to mitigate a credible threat that an unmanned aircraft or unmanned aircraft systems pose to the safety or security of a covered facility or asset to any personnel who are authorized to take such measures . . . and may establish one or more training centers for such purpose.

The provision authorizes the FBI to establish one or more counter-UAS training centers and to conduct training for those engaged in authorized counter-UAS activities. The focus of the training is expected to be on federal employees and on SLTT law enforcement personnel who have counter-UAS responsibilities because their agencies are participating in the pilot program established in subsection (c).

3. Subsection (e)(3)

Whereas the current statute contains a general coordination provision that applies to "any action authorized by this section,"[10] the proposed legislation specifically lays out the coordination requirements for testing and training. It provides that the Secretary, the Attorney General, and the heads of agencies participating in the SLTT pilot "shall coordinate their procedures governing research, testing, training, and evaluation for carrying out any provision" of the statute with the FAA so that the FAA may ensure that "the activities do not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system." It also specifies that the SLTT pilot program participants are to coordinate their procedures through the departments. This reflects the role of the departments in managing the pilot program and establishes a clear hierarchy of communication.

Subsection (f) – Forfeitures

This provision modifies the language in the existing statute to add the underlined language: "Any unmanned aircraft system or unmanned aircraft described in subsection (a) that is seized by the Secretary or the Attorney General is subject to forfeiture to the United States pursuant to the provisions of chapter 46 of title 18." The reference to Title 18 was added to identify clearly the legal provision under which forfeiture would occur.

Subsection (g) – Regulations and guidance

This provision modifies the language in the existing statute to add the underlined language:

> The Secretary, the Attorney General, and the Secretary of Transportation may prescribe regulations and shall issue guidance in the respective areas of each

[10] *See* 6 U.S.C. § 124n(b)(4) ("The Secretary and the Attorney General shall coordinate with the Administrator of the Federal Aviation Administration when any action authorized by this section might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace").

Secretary or the Attorney General to carry out this section. All guidance and regulations under this subsection shall be developed in consultation with the Federal Communications Commission, the National Telecommunications and Information Administration, and the Federal Aviation Administration.

The first sentence is the same as the provision in current subsection 124n(d)(1). The second sentence is new and reflects the need to coordinate regulations and guidance controlling activities having an impact on the radiofrequency spectrum. It also makes clear the need to coordinate such regulations and guidance with the FAA.

Subsection (h) – Coordination

Subsection (h) of the legislative proposal expands and clarifies the requirements in the existing statute for the Secretary and the Attorney General to coordinate actions with the Administrator of the FAA. It also applies to the heads of agencies designated under the new SLTT pilot authority.

Subsection (h)(1) of the legislative proposal corresponds with current subsection 124n(b)(4). It adds a requirement that coordination should occur "prior to any action" authorized by section 124n, clarifying the language of (b)(4) of section 124n, which states that coordination should occur "when any action authorized by this section might" adversely affect specified FAA activities. The updated language ensures that the coordination is proactive rather than responsive to adverse effects. Additionally, (h)(1) lists interference with "safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system" as actions that trigger the need for coordination between the Secretary and Attorney General and Administrator of the Federal Aviation Administration. detection and/or counter-UAS activities.

Subsection (h)(2) of the legislative proposal corresponds with subsections (b)(2) and (b)(4) of section 124n. Subsection (h)(2) calls for proactive communication with the Secretary of Transportation before issuing any guidance or otherwise implementing the legislation so that the Administrator of the FAA "may ensure that the guidance or implementation does not interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system" and the Secretary of Transportation may evaluate potential impacts on other critical national transportation infrastructure together with other modes of the Department of Transportation. Similar to the updated language of (h)(1), the updated language of (h)(2) clarifies, broadens, and makes more proactive the scope of communication expected between the Secretary and Attorney General and other agency heads—in this case, the Secretary of Transportation—in advance of issuing guidance or implementing action related to this legislation.

Subsection (h)(3) of the proposal corresponds with current subsection 124n(d)(2)(A). It adds that coordination with the Secretary of Transportation should occur through the Administrator of the FAA. This change is not intended to alter the substance of the consultation that is required, but rather it is intended to clearly identify the FAA's role in this area.

Subsection (h)(4) accounts for the need to coordinate counter-UAS activities with the NTIA in case these activities have an impact on the communications spectrum. It also underscores the need to coordinate such activities with the Secretary of Transportation through the FAA.

Subsection (h)(5)(A) provides that SLTT pilot program agency heads shall coordinate through the Secretary and the Attorney General with the Secretary of Transportation, and others, to ensure counter-UAS action will not have an adverse impact on critical national transportation infrastructure. Subsection (h)(5)(B) ensures that actions authorized by the section are consistent with federal law enforcement and are in the interest of national security.

Subsection (i) – Privacy protection

This subsection retains most of the current protections found subsection 124n(e), including the important requirement that communications to or from UAS are intercepted "only to the extent necessary" to support one of the counter-UAS actions authorized by the statute. This provision is consistent with existing Executive Branch policies and regulations. Finally, for agencies participating in the SLTT pilot and for entities (outside the departments) acquiring detection-only equipment, the subsection requires comparable privacy protections.

The proposed legislation makes two additional changes to the current provisions:

- The current subsection 124n(e)(3) prohibits the departments from retaining intercepted UAS communications for longer than 180 days except in certain narrowly defined circumstances, such as when necessary for purposes of litigation. The proposal adds a new category to allow retention of these communications for a longer period when "necessary to . . . protect against dangerous or unauthorized activity by unmanned aircraft systems or unmanned aircraft." For example, it may be important to retain information about UAS repeatedly sighted near aircraft in flight or sensitive facilities such as nuclear power plants or prisons. Not all such drones will present a danger, but retaining information about their activity may be vital to identifying a possible threat if the drone appears later at the same location or elsewhere. As with other extended retention categories in the current statute, the approval of the Attorney General or the Secretary would be required.

- The current subsection 124n(e)(5) authorizes the departments, "to the extent necessary," to share "threat information" with SLTT law enforcement agencies. The threat information, however, may not include "communications." This restriction unduly limits how federal counter-UAS teams can share real-time threat information, potentially harming mission effectiveness in high-tempo operational environments. The proposed subsection (i)(1)(D) authorizes the departments to share communications and information (including non-threat information) gathered from tracking and monitoring UAS with relevant SLTT counterparts. It also allows the sharing of this information with other relevant persons or entities, such as the operator of a power plant provided that "such person or entity is engaged in a security or protection operation." These tailored changes

to the provisions governing information sharing will enable better protection against UAS threats.

Subsection (j) – Budget

This provision of the current section 124n requires the Secretary and the Attorney General to submit to Congress annually a "consolidated funding display" meeting certain requirements. The proposed legislation continues this requirement.

Subsection (k) – Public disclosures

Records regarding counter-UAS operations held by a federal agency are subject to federal disclosure laws. To protect sensitive federal law enforcement information about counter-UAS operations provided to SLTT participants in training or through other means, and prevent unauthorized disclosure of that information, the proposal requires that the provisions of the Freedom of Information Act ("FOIA") be followed. Such sensitive information includes information about the capabilities, limitations, or sensitive details of specific technologies used for counter-UAS activities; operational procedures; protocols; and counter-UAS tactics, techniques, and procedures. The proposed statute also makes it clear that FOIA applies to certain information originating from a federal agency once communicated to SLTT participants; that state public disclosure laws do not apply to these categories of information even when that information is in the possession of the SLTT entity; and that requests for public access to this information must be submitted to the originating federal agency for processing in accordance with FOIA. This provision invoking FOIA ensures that requests for federal counter-UAS records are not handled by state authorities and that the appropriate federal agency retains oversight over the processing and release of the records, which may be protected from release by the exemptions found in FOIA. This is critical to ensure uniformity of disclosure practices and the protection of sensitive federal information.

Subsection (l) – Assistance and support

This subsection contains two new provisions that (1) authorize the departments to receive support provided by public and private sector entities in connection with the counter-UAS activities authorized in the statute, and (2) authorize mutual support activities by the departments.

1. Facilities and services of other agencies and non-Federal entities

This proposed subsection would authorize the Secretary or the Attorney General to accept from public or private entities "supplies or services to facilitate or take" the counter-UAS actions authorized by the statute, notwithstanding other laws that might prohibit their use or acceptance or require reimbursement from the Government. The provision allows DHS and DOJ to use C-UAS equipment that is owned and pre-positioned by operators of critical infrastructure. Critical Infrastructure operators do not have the authority to use C-UAS equipment but may benefit from site specific installations that could not be replicated by responding agencies who are authorized to use the equipment. This equipment can be available to authorized departments and agencies at

no charge should the need arise. The provision also authorizes the departments to enter into agreements with such other entities. Having these agreements in place will enable authorized departments to respond to a potential threat more quickly, and begin operations quickly upon arrival, using the pre-positioned equipment. The departments anticipate that these agreements would include controls to ensure that unauthorized persons cannot access, test, or operate the counter-UAS equipment.

2. Mutual support

Subsection (l) would also authorize the departments to provide support to each other and to certain other federal agencies "when exigent circumstances exist" and when other requirements are met. The current statute does not provide that the departments can protect another agency's facilities or assets. For example, neither Customs and Border Protection nor DEA could protect a DOD facility on the Southwest border from a UAS incursion, even if DOD lacked capabilities in the area. A Pentagon-led tabletop exercise in 2021 identified the lack of this authority as a gap in the nation's UAS protection framework. Also in 2021, there was a situation in which one agency had authority but no capability to respond to a sustained, repeated threat, and another agency had technology but no authority to act. The proposal authorizes DOJ and DHS to conduct operations to assist with missions of the other department, or the missions of DOD and the Department of Energy, upon request.

Subsection (m) – Semiannual briefings and notifications

Proposed subsection (m) corresponds to subsection (g) of the current section 124n. It details the semiannual briefings and notifications that the Secretary and Attorney General will provide to the appropriate congressional committees on the activities they have carried out pursuant to this legislation. Subsection (m)(1) substantively mirrors subsection (g)(1) in section 124n. While (g)(1) states that the semiannual briefings will occur until the date specified in subsection (i), subsection (m)(1) lists no end date for the briefings. This change reflects the elimination in the proposed legislation of the sunset for the authorized federal activities.

The provisions of subsections (m)(2) and (m)(4) are identical to the current law. Subsection (m)(3) details the content of the briefings and also is largely identical to current law. It slightly expands the requirements of subsection (m)(3)(A) and adds requirements for briefings on gaps in authorities to counter UAS threats; the impact of the authorities granted by the statute on legitimate UAS use and UAS integration into U.S. airspace; and the new U.S. government database authorized by subsection (r) for security-related UAS incidents. *See* subsections (m)(3)(H) - (K).

Finally, the notification provision, subsection (m)(5), states that it applies when there is a deployment of new technology by "an authorized department or agency." Research, testing, and evaluation involving a new technology is not a deployment, and the notification provision does not apply to a use only for these purposes.

Subsection (n) – Rule of construction

Subsection (n) of the legislative proposal corresponds with subsection 124n(h). It details limits on how this legislation is to be construed. There are no substantive changes between (n) of the legislative proposal and (h) of section 124n, but in (n)(1) through (n)(5), the legislative proposal adds limitations on the authorities of agencies designated for inclusion in the SLTT pilot. This addition corresponds with the delegation of supervised authorities to certain agencies under subsection (c) and ensures that limitations on their authorities are accounted for in the rule of construction section.

Subsection (o) – Termination

The authorities granted by the current section 124n terminate on October 5, 2022. The proposal removes the sunset provision for the authority granted to the departments. Congress will retain oversight of DOJ's and DHS's use of the authority through the required semi-annual briefings and the appropriations process. In contrast to the authority given to the departments, the SLTT pilot program will be time-limited to five-years for designating participants, with one additional year at the end for participation in the program. The pilot should provide valuable information about whether the authority to detect and mitigate UAS could be effectively and appropriately extended further, and if so, what associated federal oversight and safeguards might be necessary, as well as the associated resource costs to enable further expansion.

The growth of UAS threats since 2018 demonstrates the enduring need for the departments to retain and develop the section 124n authorities in coordination with the FAA and other affected entities. At a time of constrained budgets and major cost increases, the security components of the departments do not have resources for equipment that may have a limited lifespan. Nor do they have resources to develop a UAS detection and counter-UAS program and recruit and train appropriate personnel if that program is regularly subject to termination or major statutory changes. Rather, it is challenging for Departments to prioritize efforts that are likely to contribute to long-term mission success, such as counter UAS procurement, recruiting and training the appropriate personnel, when the authorization language sunsets. For example, the Joint Explanatory Statement accompanying the 2021 Consolidated Appropriations Act (Public Law 116-260) directs the FBI to study the feasibility of establishing a counter-UAS training center, but any such study rests on assumptions about the kinds of UAS detection and counter-UAS activities that will be lawful.[11] A permanent grant of authority to the departments will ensure that operational components can prioritize this critical mission within their broader resource planning frameworks.

Subsection (p) – Scope of authority

This provision provides that nothing in the proposed legislation "shall be construed to provide the Secretary or the Attorney General with additional authorities beyond those described" in subsections (a), (b), (c), and (e) above or the missions identified in the part of the definition of "covered facility or asset." (The definition referred to is found at subsection

[11] Subsection (e)(2) of the proposed legislation also gives the Attorney General authority to establish training centers or facilities.

(q)(5)(C)(iii), which identifies certain missions to be performed together or separately by the departments). The provision closely follows a similar provision in the current section 124n.

Subsection (q) – Definitions

Many of the definitions in the proposed legislation are the same as in the current section 124n. Set forth below are the more significant changes to the definitions:

Subsection (q)(1) – Definition of air navigation facility

The proposed legislation adds a definition of the term "air navigation facility," a term that is also used in the existing legislation. Air navigation facilities covers more than just airport control towers and approach signals and includes flight control centers that are not necessarily at airports. The definition of "air navigation facility" in the proposed legislation cross references 40102(a)(4) of title 49, which defines the term in detail. This definition is necessary in the context of the proposal to include protection of air navigation facilities in the definition of covered facility or asset.

Subsection (q)(5) – Definition of covered facility or asset

The Act authorizes the departments to take the counter-UAS actions authorized by subsection (a) to protect against a credible threat to a "covered facility or asset." The definition of this term thus serves to identify the facilities, assets, and missions, which may be protected by the departments based on the authority granted by subsection (a). The proposed legislation makes a number of changes to the definition that will better enable the government to counter emerging UAS threats.

Protection of transportation

The draft legislative text authorizes DHS to protect the nation's transportation facilities, including airports, surface modes, and air navigation facilities, on a proactive or persistent basis by adding the Transportation Security Administration's ("TSA's") missions of transportation security functions. The draft text authorizes DHS to protect static transportation facilities, as well as mobile assets and runway exclusion zones. The draft also authorizes DOJ/FBI – pursuant to its responsibility to investigate and respond to possible federal crimes of terrorism and other federal crimes – to engage in quick-response airport protection efforts, either in a lead or support role to DHS.

To protect transportation modes from UAS threats, the Departments must currently rely on authority to conduct missions related to the "protection of an active Federal law enforcement investigation, emergency response, or security function, that is limited to a specified timeframe and location" pursuant to subsection 124n(k)(3)(C)(iii)(III). While this section provides authority in the case of an emergency or security incident, the Departments do not have sufficient authority to proactively protect transportation sites, leaving aviation and surface modes vulnerable to UAS threats.

The legitimate safety concerns about deploying counter-UAS technologies in airport environments make the statute's extension to transportation missions crucial for ensuring safe deployment. Under the Act, and as implemented, the departments must coordinate with the FAA regarding all UAS detection missions, with limited exception for systems authorized for use pursuant to subsection (b), and counter-UAS missions that might affect aviation safety before deployment. Consistent with section 383 of the FAA Reauthorization Act of 2018, the FAA is launching efforts to test and evaluate technologies and systems that could detect and mitigate potential safety risks posed by UAS at and near airports. FAA's efforts in this area, as well as TSA's testing of UAS detection technology at airports, will support DHS's and DOJ's implementation of section 124n authorities. Existing FAA coordination requirements will ensure UAS detection and that counter-UAS protection missions will continue to have no adverse impacts on U.S. airspace, as the expanded authorities being requested will rely on the effective coordination procedures and processes used to date and further incorporated into the existing National Security Council-approved "Core 30" Concept of Operations.[12]

Protection of critical infrastructure

Similarly, the proposal authorizes the departments to deploy counter-UAS resources to protect critical infrastructure (as defined at 42 U.S.C. § 5195c) at the request of the infrastructure facility's operator or owner. Currently, no entity, public or private, may lawfully use counter-UAS in accordance with the Act to protect critical infrastructure, except possibly in the narrow circumstances outlined above when an active federal investigation, security function, or emergency response takes place at a critical infrastructure site, and only DHS or DOJ might then take counter-UAS protection measures. The legislative proposal will allow DHS to separately establish a process by which (i) critical infrastructure owners/operators may request federal counter-UAS assistance (mirroring established processes for counter-UAS support to Special Event Assessment Rating ("SEAR") events or emerging processes such as the FAA's Section 2209 application for flight restrictions) and (ii) requests are adjudicated against a risk-based methodology. Establishment and implementation of the process will include coordination with all necessary parties, including, but not limited to, DHS, OMB, Sector Risk Management Agencies, and the FAA.

USMS Prisoner Transport

The current statute authorizes the U.S. Marshals Service ("USMS") to protect courthouses, federal judges and specified others from the threat posed by UAS but lacks explicit authority to protect prisoner transports using counter-UAS technology, even though USMS is

[12] Following the UAS incident at Gatwick Airport in December 2018, the Government developed the *Unified National Level Response to Persistent UAS Disruption of Operations at Core 30 Airports Concept of Operations* [add date], which outlines how federal departments and agencies will organize and carry out quick-response actions to mitigate a persistent disruption of air traffic operations caused by UAS activity at these identified Core 30 airports. It describes roles and responsibilities across the federal government related to these activities. It identifies TSA as the lead federal agency to initiate and coordinate an emergency response to a persistent UAS threat, with DOJ and DOD counter-UAS capability in support and designates the FBI as the lead agency for investigation and any law enforcement response.

authorized to conduct such transports. Under 28 CFR §§ 0.111(j) and (k), respectively, the Director of the USMS directs and supervises (i) the receipt, processing, and transportation of prisoners held by the USMS or transported by the USMS under cooperative or intergovernmental agreements, and (ii) the custody of federal prisoners from time of arrest by or remand to a marshal by the court until such time as the prisoner is committed by the court to the custody of the Attorney General for the service of sentence (*e.g.*, to the Federal Bureau of Prisons ("BOP") or other custodial facility), otherwise released from custody by the court, or returned to the custody of the U.S. Parole Commission or BOP. The proposal would close this gap, allowing comprehensive counter-UAS coverage of prisoner transport and operations similar to the authority that BOP has for coverage of prisons; the description of the missions of USMS is harmonized with that of other agencies.

Thus, the proposed legislation makes two changes to the description of USMS missions that DOJ counter-UAS actions may support. First, to what is now a mission of the BOP it adds the underlined text: "protection of penal, detention, and correctional facilities and operations conducted by the Federal Bureau of Prisons and prisoner operations and transport conducted by the United States Marshals Service." Second, the current section 124n includes as an authorized USMS mission that counter-UAS actions may support "personal protection operations by . . . the United States Marshals Service of Federal jurists, court officers, witnesses, and other threatened persons in the interests of justice, as specified in section 566(e)(1)(A) of Title 28." This has been simplified and now reads "personal protection operations by . . . the United States Marshals Service as specified in section 566 of Title 28."

Subsection (q)(9) – Definition of personnel

The current section 124n has a limited definition of "personnel" that does not include contractors and thus does not permit them to carry out any of the authorized counter-UAS activities. This limitation is a significant constraint on DHS's and DOJ's ability to conduct UAS detection and counter-UAS activities, especially given the mission expansions contemplated by the proposal. The proposal therefore authorizes the departments to use contractors during UAS detection and counter-UAS operations, subject to all of the statute's requirements that apply to DHS and DOJ employees. They are also subject to all Executive Branch and departmental policies regarding the use of contractors, and in no circumstances does the proposal require the use of contractors. Contractors performing counter-UAS operations must: (1) be directly contracted by the federal department or agency; (2) operate at a government-owned or government-leased facility or asset; (3) not conduct inherently governmental functions; and (4) be trained and certified by the contracting department or agency to meet established department guidance and regulations. Notably, the draft would not permit SLTT agencies to use contractors within the context of the pilot program; only SLTT law enforcement or other authorized personnel may participate in the pilot program.

Subsection (q)(11) – Definition of risk-based assessment

The proposed legislation does not substantively alter the definition of "risk-based assessment." The only proposed change clarifies that a risk-based assessment conducted pursuant to this statute need not duplicate an evaluation of the impact of the National Special Security

Event and Special Event Assessment Rating events that have already been discussed through those nomination processes.

Subsection (r) – Database of security-related incidents

This new provision gives DHS explicit authority to develop a database of security-related UAS incidents that occur inside the United States. It provides that:

> The Department of Homeland Security is authorized to develop a U.S. government database to enable the transmission of Federal, State, local, tribal, and territorial law enforcement data concerning security-related incidents in the United States (including the territories and possessions, territorial seas, or navigable waters of the United States) involving unmanned aircraft and unmanned aircraft systems for purposes of conducting analyses of such threats in the United States. Prior to implementation of the U.S. government database, the Secretary shall develop policy, plans, and procedures for the implementation of such a database in coordination with the Attorney General, the Secretary of Defense, and the Secretary of Transportation through the Administrator of the Federal Aviation Administration, including the development of criteria for Federal, State, local, tribal, and territorial UAS incident reporting.

This provision authorizes (but does not require) DHS to establish such a database. The intent behind this provision is that DHS, working with federal departments and agencies, will create a UAS incident tracking database for incidents assessed as meeting a federal threshold, to be defined by an interagency working group including DHS, DOD, DOJ, FAA, and members of the Intelligence Community. This federal reporting threshold will not replace department internal definitions, reporting standards, or processes. Rather, the database will provide a consistent method for the interagency to review and analyze security-related UAS incidents and to work with the FAA to determine whether a verified incident involved apparent or actual violations of the federal aviation regulations. Incidents in the database may include information about UAS that repeatedly violate altitude or other federal aviation regulations in ways that may be dangerous or harmful to national defense or security.

DEPARTMENT OF DEFENSE

SEC. __. ENHANCED PROTECTION OF CERTAIN FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT THREATS.

Section 130i of title 10, United States Code, is amended—

(1) in subsection (a)—

(A) by striking "members of the armed forces and officers and civilian employees of the Department of Defense" and inserting "covered personnel"; and

(B) by inserting "or a temporarily covered facility or asset for the duration of the period in which the temporarily covered facility is at high risk or a potential target" after "a covered facility or asset";

(2) by striking subsection (i) and inserting the following new subsection:

"(i) LIMITATION ON ACTIVITIES BY CONTRACTOR PERSONNEL AND OVERSIGHT.—In carrying out this section, the Secretary shall ensure that—

"(1) contractor personnel are not directed or permitted to perform any action that is an inherently governmental function as that term is defined in the Federal Activities Inventory Reform Act of 1998 (31 U.S.C. 501 note; Public Law 105–270); and

"(2) the Department conducts appropriate oversight of contract personnel."; and

(3) in subsection (j)—

(A) in subparagraph (C) of paragraph (3)—

(i) in clause (viii), by striking "; or" and inserting a semicolon;

(ii) in clause (ix), by striking the period and inserting "; or"; and

(iii) by adding at the end the following new clause:

"(x) a military airport or airfield that is not intended to be temporary.";

(B) by redesignating paragraphs (4), (5), and (6) as paragraphs (5), (6), and (8), respectively;

(C) by inserting after paragraph (3) the following new paragraph:

"(4) The term 'covered personnel' means—

"(A) members of the armed forces;

"(B) civilian employees of the Department of Defense; and

"(C) personnel of entities under contract to the Department of Defense with assigned duties that include safety, security, or protection of a Government-owned, contractor-operated facility and who are trained and certified to perform such duties, including training specific to countering unmanned aircraft threats and mitigating risks in the national airspace."; and

(D) by inserting after paragraph (6), as redesignated by subparagraph (B) of this paragraph, the following new paragraph:

"(7) The term 'temporarily covered facility or asset' means a facility or asset located in the United States and identified by the Secretary of Defense, in consultation with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment for the purposes of this section, to be temporarily at high risk or a potential target for unlawful unmanned aircraft activity.".

[Please note: the "changes to existing law" section below sets out in red-line format how the legislative text above would amend existing law.]

Section-by-Section Analysis

Errantly or maliciously operated unmanned aircraft increase risks to the Department's installations, activities, and personnel. This proposal would amend section 130i of title 10, United States Code, to close critical gaps in the Department's authority to mitigate the threats posed by an unmanned aircraft system or unmanned aircraft.

This proposal would permit the Secretary of Defense to authorize contractor personnel performing functions under contract with the Department of Defense (DoD) that include safety, security, or protection of a Government-owned, contractor-operated facility, and who are trained and certified to perform such duties, to assist in mitigating the threat of unmanned aircraft in accordance with section 130i. The Departments of the Army, Navy, and Air Force are responsible for Government-owned, contractor-operated facilities that produce munitions and other sensitive items. There is an insufficient number of military and civilian personnel to allocate those that would be necessary to provide for the safety, security, and protection of these Government-owned, contractor-operated facilities. The Military Departments rely on contractor personnel to perform such duties under the oversight of military or DoD civilian employees. In the absence of this change, the Departments of the Army, Navy, and Air Force would have to either assign military or civilian personnel to protect such facilities, thereby undermining other DoD missions, or accept that these facilities will remain vulnerable.

This proposal would authorize the Secretary of Defense to take the actions authorized by section 130i with respect to a temporarily covered facility or asset. DoD facilities or assets not directly associated with a covered mission identified in section 130i(j) can temporarily be at a high risk of threat from an unmanned aircraft system or unmanned aircraft due to a specific, highly significant vulnerability. Examples of such a vulnerability include: (i) a port of embarkation for military personnel, weapon systems, or munitions being deployed by ship to conduct combat operations in an overseas conflict; (ii) the headquarters of the combatant commander responsible for commanding military forces engaged in an overseas conflict; (iii) a vehicle or aircraft transporting high-risk or very important persons, or sensitive materials; or (iv) a public event at a military installation involving hundreds of non-DoD personnel. In addition, a DoD facility or asset not directly associated with a covered mission may temporarily be indicated to be at a high risk due to specific intelligence or law enforcement information that such a DoD facility or asset is a target for hostile action by an adversary.

This proposal would also repeal the partial termination clause in subsection (i) of section 130i. Section 130i has been in effect for nearly six years, and DoD has used the authority responsibly. Other Federal departments (e.g., the Department of Homeland Security and the Department of Justice) have since been granted similar authorities. Repealing the partial termination subsection would enable planning, programming, and budgeting across the Future Years Defense Program (FYDP) to develop, test, and field capabilities designed specifically to operate safely in the national airspace system of the United States rather than in operations abroad. Contrarily, retaining the partial termination subsection would continue to undermine DoD's planning, programming, and budgeting, as well as DoD's contingency planning as such plans would have to exclude the protection of facilities and assets subject to the subsection or be updated when the subsection takes effect.

Finally, this proposal would amend subsection (j)(3)(C) of section 130i by updating the definition of a covered facility or asset to include a military airport or airfield that is not intended to be temporary. Errantly or nefariously operated unmanned aircraft systems or unmanned

aircraft create a flight hazard or a threat to military aircraft operations and training in the United States. Including permanent military airports and airfields would extend the authority provided by section 130i to encompass permanent military airports and airfields not associated with the missions specified by this section. In circumstances when military airports and airfields are part of a joint use facility with a civilian airport or airfield, DoD's authority would be limited to the protection of military facilities and assets. The protection of civilian facilities and assets would remain the purview of those entities responsible for the security and safety of civilian airports and airfields. If this proposal is enacted, DoD will, as required by section130i, coordinate with the Federal Aviation Administration (FAA) on how to use this authority responsibly at joint use airfields. Since enactment of section 130i, DoD and the FAA have had a thorough and successful process in place for coordination which would be used to facilitate coordination of identification of permanent military airports, including joint use airfields, as covered facilities under section 130i.

Resource Information: The resources required are reflected in the table below and are included within the Fiscal Year (FY) 2023 President's Budget.

RESOURCE IMPACT ($MILLIONS)									
Program	**FY 2023**	**FY 2024**	**FY 2025**	**FY 2026**	**FY 2027**	**Appropriation**	**Budget Activity**	**BLI/SAG**	**Program Element (for all RDT&E programs)**
Air Force	27.2 19.3 25.2	28.9 14.3 11.6	28.9 14.3 11.5	29.5 14.7 11.7	30.1 14.9 11.9	AF O&M AF RDTE AF PROC	01 04 03	O12C 640410 834140	0207522F
Army	9.2 1.6 33.7	9.2 1.6 19.0	9.3 1.6 4.1	9.3 1.6 18.7	9.3 1.6 9.3	Army O&M Army RDTE Army PROC	01 04 02	1SAG 122 FG5 0219AD0 500	0305208 A 0604741 A 0605531 A
Navy	30.1	35.7	16.9	17.1	17.2	Navy O&M, Procurement, RDTE	01 01 04 04 07 04 04	1C6C 1C6C 4B2N 5509 8128 3241 3177	0604636 N 0603654 N
USMC	23.2	12.2	12.6	12.8	13.1	USMC O&M, Procurement, RDT&E	01 03 07	1A2A 3006 0605520 M	0206626 M 0206211 M

									0605520 M
Total	169.5	132.5	99.2	115.4	107.4				

Resubmission Information: This proposal is being resubmitted. The proposal was submitted in FY 2022 (LP #061) and transmitted to Congress, but not included in the House or Senate versions of the National Defense Authorization Act for Fiscal Year 2022 or the final bill.

Component Subject Matter Expert: Col Laura "Lori" Ambers, OASD(HD&GS), (703) 695-1157, laura.l.ambers.mil@mail.mil

Reviewing Legal Counsel: Kyle Jacobson, DoD OGC, (571) 256-8380, kyle.r.jacobson.civ@mail.mil

Reviewing Comptroller POC: Col Laura "Lori" Ambers, OASD(HD&GS), (703) 695-1157, laura.l.ambers.mil@mail.mil

Component Contact for OMB: Col Laura "Lori" Ambers, OASD(HD&GS), (703) 695-1157, laura.l.ambers.mil@mail.mil

Changes to Existing Law: This proposal would amend section 130i of title 10, United States Code, as follows:

§ 130i. Protection of certain facilities and assets from unmanned aircraft

(a) AUTHORITY.—Notwithstanding section 46502 of title 49, or any provision of title 18, the Secretary of Defense may take, and may authorize ~~members of the armed forces and officers, and civilian employees of the Department of Defense~~ covered personnel with assigned duties that include safety, security, or protection of personnel, facilities, or assets, to take, such actions described in subsection (b)(1) that are necessary to mitigate the threat (as defined by the Secretary of Defense, in consultation with the Secretary of Transportation) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset or a temporarily covered facility or asset for the duration of the period in which the temporarily covered facility is at high risk or a potential target.

(b) ACTIONS DESCRIBED.—(1) The actions described in this paragraph are the following:

(A) Detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and direct or indirect physical, electronic, radio, and electromagnetic means.

(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft

by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

(D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.

(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

(F) Use reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

(2) The Secretary of Defense shall develop the actions described in paragraph (1) in coordination with the Secretary of Transportation.

(c) FORFEITURE.—Any unmanned aircraft system or unmanned aircraft described in subsection (a) that is seized by the Secretary of Defense is subject to forfeiture to the United States.

(d) REGULATIONS AND GUIDANCE.—(1) The Secretary of Defense and the Secretary of Transportation may prescribe regulations and shall issue guidance in the respective areas of each Secretary to carry out this section.

(2)(A) The Secretary of Defense and the Secretary of Transportation shall coordinate in the development of guidance under paragraph (1).

(B) The Secretary of Defense shall coordinate with the Secretary of Transportation and the Administrator of the Federal Aviation Administration before issuing any guidance or otherwise implementing this section if such guidance or implementation might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of airspace.

(e) PRIVACY PROTECTION.—The regulations prescribed or guidance issued under subsection (d) shall ensure that—

(1) the interception or acquisition of, or access to, an unmanned aircraft system or communications to or from an unmanned aircraft system under this section is conducted in a manner consistent with the fourth amendment to the Constitution and applicable provisions of Federal law;

(2) communications to or from an unmanned aircraft system are intercepted, acquired, or accessed only to the extent necessary to support a function of the Department of Defense;

(3) records of such communications are not maintained for more than 180 days unless the Secretary of Defense determines that maintenance of such records—

(A) is necessary to support one or more functions of the Department of Defense; or

(B) is required for a longer period to support a civilian law enforcement agency or by any other applicable law or regulation; and

(4) such communications are not disclosed outside the Department of Defense unless the disclosure—

(A) would fulfill a function of the Department of Defense;

(B) would support a civilian law enforcement agency or the enforcement activities of a regulatory agency of the Federal Government in connection with a

criminal or civil investigation of, or any regulatory action with regard to, an action described in subsection (b)(1); or

(C) is otherwise required by law or regulation.

(f) BUDGET.—The Secretary of Defense shall submit to Congress, as a part of the defense budget materials for each fiscal year after fiscal year 2018, a consolidated funding display that identifies the funding source for the actions described in subsection (b)(1) within the Department of Defense. The funding display shall be in unclassified form, but may contain a classified annex.

(g) SEMIANNUAL BRIEFINGS.—(1) On a semiannual basis during the five-year period beginning March 1, 2018, the Secretary of Defense and the Secretary of Transportation, shall jointly provide a briefing to the appropriate congressional committees on the activities carried out pursuant to this section. Such briefings shall include—

(A) policies, programs, and procedures to mitigate or eliminate impacts of such activities to the National Airspace System;

(B) a description of instances where actions described in subsection (b)(1) have been taken;

(C) how the Secretaries have informed the public as to the possible use of authorities under this section; and

(D) how the Secretaries have engaged with Federal, State, and local law enforcement agencies to implement and use such authorities.

(2) Each briefing under paragraph (1) shall be in unclassified form, but may be accompanied by an additional classified briefing.

(h) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

(1) vest in the Secretary of Defense any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration under title 49; and

(2) vest in the Secretary of Transportation or the Administrator of the Federal Aviation Administration any authority of the Secretary of Defense under this title.

~~(i) PARTIAL TERMINATION.—(1) Except as provided by paragraph (2), the authority to carry out this section with respect to the covered facilities or assets specified in clauses (iv) through (viii) of subsection (j)(3)(C) shall terminate on December 31, 2023.~~

~~(2) The President may extend by 180 days the termination date specified in paragraph (1) if before November 15, 2023, the President certifies to Congress that such extension is in the national security interests of the United States.~~

(i) LIMITATION ON ACTIVITIES BY CONTRACTOR PERSONNEL AND OVERSIGHT.—In carrying out this section, the Secretary shall ensure that—

(1) contractor personnel are not directed or permitted to perform any action that is an inherently governmental function as that term is defined in the Federal Activities Inventory Reform Act of 1998 (31 U.S.C. 501 note; Public Law 105–270); and

(2) the Department conducts appropriate oversight of contract personnel.

(j) DEFINITIONS.—In this section:

(1) The term "appropriate congressional committees" means—

(A) the congressional defense committees;

(B) the Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Commerce, Science, and Transportation of the Senate; and

(C) the Permanent Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Transportation and Infrastructure of the House of Representatives.

(2) The term "budget", with respect to a fiscal year, means the budget for that fiscal year that is submitted to Congress by the President under section 1105(a) of title 31.

(3) The term "covered facility or asset" means any facility or asset that—

(A) is identified by the Secretary of Defense, in consultation with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section;

(B) is located in the United States (including the territories and possessions of the United States); and

(C) directly relates to the missions of the Department of Defense pertaining to—

(i) nuclear deterrence, including with respect to nuclear command and control, integrated tactical warning and attack assessment, and continuity of government;

(ii) missile defense;

(iii) national security space;

(iv) assistance in protecting the President or the Vice President (or other officer immediately next in order of succession to the office of the President) pursuant to the Presidential Protection Assistance Act of 1976 (18 U.S.C. 3056 note);

(v) air defense of the United States, including air sovereignty, ground-based air defense, and the National Capital Region integrated air defense system;

(vi) combat support agencies (as defined in paragraphs (1) through (4) of section 193(f) of this title);

(vii) special operations activities specified in paragraphs (1) through (9) of section 167(k) of this title;

(viii) production, storage, transportation, or decommissioning of high-yield explosive munitions, by the Department; ~~or~~

(ix) a Major Range and Test Facility Base (as defined in sections 4173(i) of this title)~~.~~; or

(x) a military airport or airfield that is not intended to be temporary.

(4) The term "covered personnel" means—

(A) members of the armed forces;

(B) civilian employees of the Department of Defense; and

(C) personnel of entities under contract to the Department of Defense with assigned duties that include safety, security, or protection of a Government-

owned, contractor-operated facility and who are trained and certified to perform such duties, including training specific to countering unmanned aircraft threats and mitigating risks in the national airspace.

(45) The term “defense budget materials”, with respect to a fiscal year, means the materials submitted to Congress by the Secretary of Defense in support of the budget for that fiscal year.

(~~5~~6) The terms “electronic communication”, “intercept”, “oral communication”, and “wire communication” have the meanings given those terms in section 2510 of title 18.

(7) The term “temporarily covered facility or asset” means a facility or asset located in the United States and identified by the Secretary of Defense, in consultation with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment for the purposes of this section, to be temporarily at high risk or a potential target for unlawful unmanned aircraft activity.

(~~6~~8) The terms "unmanned aircraft" and "unmanned aircraft system" have the meanings given those terms in section 44801 of title 49.

Department of State Domestic Protection Mission

(NEW AUTHORITY)

(a)AUTHORITY

(1) Notwithstanding section 46502 of title 49, or any provision of title 18, the Secretary of State may take, and may authorize appropriate personnel, including Bureau of Diplomatic Security personnel and contractors, with assigned duties that include safety, security, or protection of personnel, facilities, or assets, to take, such actions described in subsection (b)(1) that are necessary to mitigate a credible threat (as defined by the Secretary of State, in consultation with the Federal Aviation Administration) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset.

(b)ACTIONS DESCRIBED.—

(1) In General

The actions described in this paragraph are the following:

(A) During the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and direct or indirect physical, electronic, radio, and electromagnetic means.

(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft

system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

(D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.

(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

(F) Use reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

(2) Research, Testing, Training, and Evaluation

(A) Notwithstanding section 46502 of title 49 or any provision of title 18, the Secretary of State shall conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine its capability and utility prior to the use of any such technology for any action described in subsection (b)(1). Personnel, including contractors, who do not have duties that include the safety, security, or protection of people, facilities, or assets may engage in research, testing, training, and evaluation activities pursuant to this section.

(B) Coordination for Research, Testing, Training, and Evaluation

The Secretary shall coordinate procedures governing research, testing, training, and evaluation for carrying out any provision in this section with the Administrator of the Federal Aviation Administration before initiating such activities so the Administrator may ensure the activities do not adversely impact

or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.

(c)FORFEITURE.— Any unmanned aircraft system or unmanned aircraft described in subsection (a) that is seized by the Secretary of State is subject to forfeiture to the United States pursuant to the provisions of chapter 46 of title 18.

(d)REGULATIONS AND GUIDANCE— (1) The Secretary of State and the Secretary of Transportation, in consultation with the Assistant Secretary of Commerce for Communications and Information of the National Telecommunications and Information Administration, may prescribe regulations and shall issue guidance in the respective areas of each Secretary to carry out this section.

(e) Coordination

(1) The Secretary of State shall develop the actions described in subsection (b)(1) in coordination with the Secretary of Transportation (through the Administrator of the Federal Aviation Administration), and the Assistant Secretary of Commerce for Communications and Information of the National Telecommunications and Information Administration.

(2) The Secretary of State shall coordinate with the Administrator of the Federal Aviation Administration prior to any action authorized by this section so the Administrator may ensure the action does not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.

(3) The Secretary of State shall coordinate the development of guidance and regulations under subsection (d) with the Federal Aviation Administration, the Federal

Communications Commission, and the National Telecommunications and Information Administration.

(4) The Secretary of State shall coordinate with the Federal Aviation Administration before issuing any guidance, or otherwise implementing this section so the Federal Aviation Administration may ensure such guidance or implementation does not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.

(f)PRIVACY PROTECTION.—The regulations prescribed or guidance issued under subsection (d) shall ensure that—

(1) the interception or acquisition of, or access to, communications to or from an unmanned aircraft system under this section is conducted in a manner consistent with the First and Fourth Amendments to the Constitution and applicable provisions of Federal law;**(2)** communications to or from an unmanned aircraft system are intercepted, acquired, or accessed only to the extent necessary to support the actions described in subsection (b);

(3) records of such communications are not maintained for more than 180 days unless the Secretary of State determines that maintenance of such records—

(A) is necessary to support one or more functions of the Department of State; or

(B) is required by any other applicable law or regulation; and

(4) such communications are not disclosed outside the Department of State unless the disclosure—

(A) would fulfill a function of the Department of State;

(B) would support a law enforcement or national security agency or the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory action with regard to, an action described in subsection (b)(1);

(C) is necessary to protect against dangerous or unauthorized activity by unmanned aircraft systems or unmanned aircraft; or

(D) is otherwise required by law or regulation.

(g) BUDGET.—The Secretary of State shall submit to Congress, as a part of the budget presentation documents for each fiscal year following the enactment of this provision, a consolidated funding display that identifies the funding source for the actions described in subsection (b)(1) within the Department of State. The funding display shall be in unclassified form but may contain a classified annex.

(h) SEMIANNUAL BRIEFINGS.—

(1) On a semiannual basis beginning six months following the enactment of this provision during the five-year period beginning [upon enactment of this provision], the Secretary of State and the Secretary of Transportation shall jointly provide a briefing to the appropriate congressional committees on the activities carried out pursuant to this section. Such briefings shall include—

(A) policies, programs, and procedures to mitigate or eliminate impacts of such activities to the National Airspace System;

(B) a description of instances where actions described in subsection (b)(1) have been taken;

(C)how the Secretaries have informed the public as to the possible use of authorities under this section; and

(D)how the Secretaries have engaged with Federal, State, and local law enforcement agencies to implement and use such authorities.

(2) Each briefing under paragraph (1) shall be in unclassified form but may be accompanied by an additional classified briefing.

(I) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

(1) vest in the Secretary of State any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration under title 49; and

(2) vest in the Secretary of Transportation or the Administrator of the Federal Aviation Administration any authority of the Secretary of State.

(j) DEFINITIONS.—In this section:

(1) The term "appropriate congressional committees" means—

(A) the Senate Foreign Relations Committee and the House Foreign Affairs Committee;

(B) the Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Commerce, Science, and Transportation of the Senate; and

(C) the Permanent Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Transportation and Infrastructure of the House of Representatives.

(2) The term "budget", with respect to a fiscal year, means the budget for that fiscal year that is submitted to Congress by the President under section 1105(a) of title 31.

(3) The term "covered facility or asset" means any facility or asset that—

(A) is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Secretary of State, in coordination with the Federal Aviation Administration, with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section;

(B) is located in the United States (including the territories and possessions of the United States); and

(C) directly relates to the security and protective missions of the Department of State, including those consistent with:

(i) The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (22 U.S.C. § 4801, et seq.)

(ii) Section 37 of the State Department Basic Authorities Act of 1956 (22 U.S.C. § 2709)

(4) The terms "electronic communication", "intercept", "oral communication", and "wire communication" have the meanings given those terms in section 2510 of title 18.

(5) The term "personnel" means officers, employees, and contractors of the Department of State with assigned duties that include safety, security, or protection of personnel, facilities, or assets and who are trained and certified to perform such duties, including training specific to countering unmanned aircraft threats and mitigating risks in the national airspace. To qualify under this provision, contractors conducting operations under sections (a) and (b) must:

(i) be directly contracted by the Department of State;

(ii) operate at a government owned or government leased facility;

(iii) not conduct inherently governmental functions; and

(iv) be trained and certified by the Department of State as meeting established Department guidance and regulations.

(6) For purposes of this section, the term "risk-based assessment" includes an evaluation of threat information specific to a covered facility or asset and, with respect to potential impacts on the safety and efficiency of the national airspace system and the needs of law enforcement and national security at each covered facility or asset identified by the Secretary, of each of the following factors:

(A) Potential impacts to safety, efficiency, and use of the national airspace system, including potential effects on manned aircraft and unmanned aircraft systems, aviation safety, airport operations, infrastructure, and air navigation services related to the use of any system or technology for carrying out the actions described in subsection (b)(1).

(B) Options for mitigating any identified impacts to the national airspace system related to the use of any system or technology, including minimizing when possible the use of any technology which disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1).

(C) Potential consequences of the impacts of any actions taken under subsection (b)(l) to the national airspace system and infrastructure if not mitigated.

(D)The ability to provide reasonable advance notice to aircraft operators consistent with the safety of the national airspace system and the needs of law enforcement and national security.

(E) The setting and character of any covered facility or asset, including whether it is located in a populated area or near other structures, whether the facility is open to the public, whether the facility is also used for nongovernmental functions, and any potential for interference with wireless communications or for injury or damage to persons or property.

(7) The terms "unmanned aircraft" and "unmanned aircraft system" have the meanings given those terms in section 44801 of title 49.

Section-by-Section Analysis

This proposal is intended to address a gap in the U.S. government's authority to protect against unmanned aircraft systems (UAS) domestically. Despite having its own domestic security and protection missions, the Department of State does not have relief from federal criminal laws to adequately counter the threat posed by UAS to its missions. In addition, the Department is limited as to its domestic UAS detection and C-UAS research, testing, training, and evaluation operations due to lack of relief from those same federal criminal laws, which also impacts the ability for the Department to support its broad overseas security and protective missions.

The proposed legislation would authorize the Secretary of State to take—and to authorize appropriate personnel, including Bureau of Diplomatic Security personnel and contractors, to take—certain actions necessary to detect and mitigate a credible threat posed by a UAS to a covered facility or asset, notwithstanding certain otherwise potentially applicable federal criminal laws.

The proposed legislation is consistent with current Department authorities. For example, the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (22 U.S.C. § 4801, et seq.) and section 37 of the State Department Basic Authorities Act of 1956 (22 U.S.C. § 2709), among other authorities, identify the security functions and responsibilities of the Secretary of State regarding the protection of foreign missions and international organizations, foreign officials, and diplomatic personnel in the United States, as authorized by law; physical protection of Department of State facilities, communications, and computer and information systems in the United States; and the performance of other security, investigative, and protective matters as authorized by law. Additionally, section 7070 of the Department of State, Foreign Operations, and Related Programs Appropriations Act, 2021 (Div. K, P.L. 116-260), as carried forward by the Continuing Appropriations Act, 2022 (Div. A, P.L. 117-43), extends protection to former or retired senior Department of State officials or employees who face a credible threat from a foreign power as determined by the Secretary of State, in coordination with the Director of National Intelligence.

The Department recognizes that deployment of UAS detection and C-UAS technologies has implications for the FAA. Any use of UAS detection andC-UAS technology will include a robust system of internal checks and be coordinated with the FAA, FCC, and NTIA.

Absence of relief creates gaps and vulnerabilities in the Department's ability to protect national security interests. For example, the Department of State hosts an average of three-to-five diplomatic summits or conferences each year that do not meet the threshold of a National Special Security Event (NSSE) and, as such, do not fall within the current text of, or proposed revisions to, 6 U.S.C. § 124n. In these cases, the Department of State is the lead agency for event security. Moreover, diplomatic summits and conferences are often held with little advance notice, in response to emerging global issues, and to negotiate diplomatic resolutions to conflicts and other pressing national security matters. Diplomatic summits and conferences are typically hosted by the Secretary of State or other senior Department officials and attended by Foreign Ministers or their delegates. Given this high-level representation and multilateral engagement on sensitive subject matters, diplomatic summits and conferences are attractive targets for terrorist groups, criminals, non-state actors, or proxies who wish to disrupt diplomatic efforts for their own nefarious purposes. UAS are increasingly being used by these groups due to the availability and relatively low costs of commercial UAS, their ease of operation, and their ability to carry out attacks from a distance. Diplomatic Security also carries out over two hundred protective operations per year. While the vast majority of those are for temporary visits, security details for the Secretary of State and other protectees are long term operations and include 24/7 coverage, including at residences or other fixed locations. In the last year, security details have had numerous sightings of suspected UAS near or around protected persons. In very limited circumstances where there are multiple sightings near a protected person's home, office, or other fixed location, Diplomatic Security may seek to conduct UAS detection and C-UAS operations. This proposal will assist the Department in effectively detecting and countering credible UAS threats.

Contractors play a critical part in the Department's mission to physically protect domestic Department of State facilities. Any limitation on the ability of contractors to carry out the authorized UAS detection and C-UAS operations within the proposed legislation would be a significant constraint on the Department's protective operations at domestic Department facilities, many of which are secured by contractors. The proposal therefore authorizes the Department to use contractors for UAS detection and C-UAS operations, subject to the same requirements in the legislation applicable to Department employees. The proposal does not change any Department policies regarding the use of contractors, and in no circumstances does it require their use for UAS detection and C-UAS operations.

The proposed legislation allows for retention of records of communications to or from an unmanned aircraft system for a period longer than 180 days when "necessary to support one or more functions of the Department of State" or when "required by any other applicable law or regulation." This is prudent, among other things, for establishing patterns of suspicious activity and aiding investigations.

The proposed legislation also authorizes the Secretary of State and authorized personnel

to take actions "[n]ot withstanding section 46502 of title 49, or any provision of Title 18." This language is identical to that contained in 10 U.S.C. § 130i, DoD's C-UAS authority, as well as the revisions proposed for 6 U.S.C. § 124n (DOJ/DHS's C-UAS authority), and it removes the need for analysis and review of the various provisions of Title 18 when action is taken consistent with the proposed legislation.

The proposed legislation would allow the Department to conduct domestic research, testing, training on, and evaluation of a wide array of UAS detection and C-UAS technologies, thereby also increasing the Department's ability to protect against a broader range of UAS threats both domestically and abroad. Without relief from potentially applicable federal criminal laws, the Department's ability to effectively select equipment to meet its mission needs will be limited. Moreover, interagency partners have different mission sets, and relying on their research and development efforts could create capability gaps insufficient to support the Department of State security and protective missions.

The growing public safety and national security threat posed by UAS requires clear, long-term authority for appropriate government agencies to engage in UAS detection and C-UAS operations, notwithstanding laws that could otherwise limit such activities. Without it, the Department of State is limited in its available tools to counter, consistent with its missions, the national security threats posed by UAS.

Budget Implications: If the proposed legislation is passed, the Department will require new budget authority upwards of $20 million to support research, testing and evaluation, travel, third party contract personnel, government personnel, training, and logistics for the effective implementation of the domestic C-UAS authorities.

Resubmission Information: This proposal is being submitted for the first time.

Component Subject Matter Expert: Jerry Kessler, Branch Chief, Systems Integration and Management, (571) 777-6859, kesslerj3@state.gov

Reviewing Legal Counsel: Matthew Eible, Attorney-Adviser, State Department Office of the Legal Adviser, (202) 230-3608, eiblemj@state.gov

Reviewing Comptroller POC: Robert J. Baldre, Comptroller, Bureau of Diplomatic Security, (703) 875-5400, baldrerj@state.gov

Component Contact for OMB: Jerry Kessler, Branch Chief, Systems Integration and Management, (571) 777-6859, kesslerj3@state.gov

Changes to Existing Law: This proposal would be a new standalone authority and would not amend any existing law.

Central Intelligence Agency Domestic Protection Mission
(NEW AUTHORITY)

(a) AUTHORITY.—Notwithstanding section 46502 of Title 49, or any provision of Title 18, United States Code, the Director may take, and may authorize Agency personnel with assigned duties that include the security or protection of people, facilities, or assets within the United States to take:

(1) such actions described in subsection (b)(1) that are necessary to mitigate a credible threat (as defined by the Director, in consultation with the Secretary of Transportation) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset; and

(2) such actions described in subsection (b)(3).

(b) ACTIONS.—

(1) ACTIONS DESCRIBED.—The actions described in this paragraph are the following:

(A) During the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and by direct or indirect, physical, electronic, radio, and electromagnetic means.

(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

(D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.

(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

(F) Use reasonable force, if necessary, to seize or otherwise disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

(2) COORDINATION.—The Director shall develop the actions described in paragraph (1) in coordination with the Secretary of Transportation.

(3) RESEARCH, TESTING, TRAINING, AND EVALUATION.— The Director shall conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine the capability and utility of the equipment prior to the use of the equipment for any action described in paragraph (1). Personnel and contractors who do not have duties that include the safety, security, or protection of people, facilities, or assets may engage in research, testing, training, and evaluation activities pursuant to this section.

(4) FAA COORDINATION.—The Director shall coordinate with the Administrator of the Federal Aviation Administration on any action described in paragraph (1) and (3) so the Administrator may ensure that unmanned aircraft system detection and mitigation systems do not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.

(c) FORFEITURE.—Any unmanned aircraft system or unmanned aircraft described in subsection (a) that is seized by the Director is subject to forfeiture to the United States.

(d) REGULATIONS AND GUIDANCE.—

(1) ISSUANCE.—The Director and the Secretary of Transportation may each prescribe regulations, and shall each issue guidance, to carry out this section.

(2) COORDINATION.—

(A) REQUIREMENT.—The Director shall coordinate the development of guidance under paragraph (1) with the Secretary of Transportation.

(B) AVIATION SAFETY.—The Director shall coordinate with the Secretary of Transportation and the Administrator of the Federal Aviation Administration before issuing any guidance, or otherwise implementing this section, so the Administrator may ensure that unmanned aircraft system detection and mitigation systems do not adversely impact or interfere with safe airport operations,

navigation, air traffic services, or the safe and efficient operation of the national airspace system.

(e) PRIVACY PROTECTION.—The regulations prescribed or guidance issued under subsection (d) shall ensure that—

(1) the interception or acquisition of, or access to, or maintenance or use of, communications to or from an unmanned aircraft system or unmanned aircraft under this section is conducted in a manner consistent with the First and Fourth amendments to the Constitution of the United States and applicable provisions of Federal law;

(2) communications to or from an unmanned aircraft system or unmanned aircraft are intercepted or acquired only to the extent necessary to support an action described in subsection (b);

(3) records of such communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Director determines that maintenance of such records for a longer period is necessary for the investigation or prosecution of a violation of law, to fulfill a duty, responsibility, or function of the Agency, is required under Federal law, or for the purpose of any litigation;

(4) such communications are not disclosed outside the Agency unless the disclosure—

(A) is necessary to investigate or prosecute a violation of law;

(B) would support the Agency, the Department of Defense, a Federal law enforcement, intelligence, or security agency, a State, local, tribal, or territorial law enforcement agency, or other relevant person or entity if such entity or person is engaged in a security or protection operation;

(C) is necessary to support a department or agency listed in subparagraph (B) in investigating or prosecuting a violation of law;

(D) would support the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory, statutory, or other enforcement action relating to, an action described in subsection (b);

(E) is necessary to protect against dangerous or unauthorized activity by unmanned aircraft systems or unmanned aircraft;

(F) is necessary to fulfill a duty, responsibility, or function of the Agency; or

(G) is otherwise required by law.

(f) BUDGET.—The Director shall submit to the congressional intelligence committees, as a part of the budget requests of the Agency for each fiscal year after fiscal year 2023, a consolidated funding display that identifies the funding source for the actions described in subsection (b)(1) within the Agency. The funding display shall be in unclassified form, but may contain a classified annex.

(g) SEMIANNUAL BRIEFINGS AND NOTIFICATIONS.—

(1) BRIEFINGS.—Beginning 6 months after the date of enactment of this section, and

semiannually thereafter, the Director shall provide congressional intelligence committees, congressional judiciary committees, and congressional transportation and infrastructure committees a briefing on the activities carried out pursuant to this section during the period covered by the briefing.

(2) REQUIREMENT.—Each briefing under paragraph (1) shall be conducted jointly with the Secretary of Transportation.

(3) CONTENTS.—Each briefing under paragraph (1) shall include—

(A) policies, programs, and procedures to mitigate or eliminate impacts of such activities to the national airspace system and other critical national transportation infrastructure;

(B) a description of instances in which actions described in subsection (b)(1) have been taken, including all such instances that may have resulted in harm, damage, or loss to a person or to private property;

(C) a description of the guidance, policies, or procedures established to address privacy, civil rights, and civil liberties issues implicated by the actions allowed under this section, as well as any changes or subsequent efforts that would significantly affect privacy, civil rights or civil liberties;

(D) a description of options considered and steps taken to mitigate any identified impacts to the national airspace system related to the use of any system or technology, including the minimization of the use of any technology that disrupts

the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1);

(E) a description of instances in which communications intercepted or acquired during the course of operations of an unmanned aircraft system or unmanned aircraft were maintained for more than 180 days or disclosed outside the Agency;

(F) how the Director and the Secretary of Transportation have informed the public as to the possible use of authorities under this section; and

(G) how the Director and the Secretary of Transportation have engaged with Federal, State, local, territorial, or tribal law enforcement agencies to implement and use such authorities.

(4) FORM.—Each briefing under paragraph (1) shall be in unclassified form, but may be accompanied by an additional classified report.

(5) NOTIFICATION.—Within 30 days of deploying any new technology to carry out the actions described in subsection (b)(1), the Director shall submit to the congressional intelligence committees a notification of the use of such technology. Such notification shall include a description of options considered to mitigate any identified impacts to the national airspace system related to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1).

(h) RULE OF CONSTRUCTION.—Nothing in this section may be construed to—

(1) vest in the Director any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration; or (2) vest in the Secretary of Transportation or the Administrator of the Federal Aviation Administration any authority of the Director.

(i) SCOPE OF AUTHORITY.—Nothing in this section shall be construed to provide the Director or the Secretary of Transportation with additional authorities beyond those described in subsections (a) and (c).

(j) DEFINITIONS.—In this section:

(1) BUDGET.—The term 'budget', with respect to a fiscal year, means the budget for that fiscal year that is submitted to Congress by the President under section 1105(a) of Title 31, United States Code.

(2) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term 'congressional intelligence committees' means—

(A) the Permanent Select Committee on Intelligence of the House of Representatives; and,

(B) the Select Committee on Intelligence of the Senate.

(3) CONGRESSIONAL JUDICARY COMMITTEES.—The term 'congressional judiciary committees' means—

(A) the Committee on Judiciary of the House of Representatives; and,

(B) the Committee on Judiciary of the Senate.

(4) CONGRESSIONAL TRANSPORTATION AND INFRASTRUCTURE COMMITTEES.—The term ‘congressional transportation and infrastructure committees’ means—

(A) the Committee on Transportation and Infrastructure of the House of Representatives; and

(B) the Committee on Commerce, Science, and Transportation of the Senate.

(5) TITLE 18 TERMS.—The terms ‘electronic communication', ‘intercept’, ‘oral communication’, and ‘wire communication’ have the meanings given those terms in section 2510 of Title 18, United States Code. The term “United States” has the meaning given that term in section 5 of Title 18, United States Code.

(6) TITLE 47 TERMS.—The term ‘radio communication’ has the meaning given that term in section 153 of Title 47, United States Code.

(7) TITLE 49 TERMS.—The terms ‘unmanned aircraft’ and ‘unmanned aircraft system’ have the meanings given those terms in section 44801 of Title 49, United States Code.

(8) COVERED FACILITY OR ASSET.—The term ‘covered facility or asset’ means the Agency Headquarters Compound and the property controlled and occupied by the

Federal Highway Administration located immediately adjacent to such Compound (subject to a risk-based assessment as defined for purposes of this section), or any other Agency installation and protected property where the facility or asset:

(A) is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Director, in coordination with the Secretary of Transportation, with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section;

(B) is located in the United States;

(C) is listed as a covered facility or asset with reference to this section in the classified annex of this Act or any subsequent Intelligence Authorization Act; and

(D) directly relates to one or more functions authorized to be performed by the Agency, pursuant to the National Security Act of 1947 or this Act (Central Intelligence Agency Act of 1949).

(9) RISK-BASED ASSESSMENT.—For purposes of this section, the term 'risk-based assessment' includes an evaluation of threat information specific to a covered facility or asset and, with respect to potential impacts on the safety and efficiency of the national airspace system and the needs of national security at each covered facility or asset identified by the Director, of each of the following factors:

(A) Potential impacts to safety, efficiency, and use of the national airspace system, including potential effects on manned aircraft and unmanned aircraft systems, aviation safety, airport operations, infrastructure, and air navigation

services related to the use of any system or technology for carrying out the actions described in subsection (b)(1);

(B) Options for mitigating any identified impacts to the national airspace system related to the use of any system or technology, including minimizing when possible the use of any system or technology which disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b)(1);

(C) Potential consequences of the impacts of any actions taken under subsection (b)(1) to the national airspace system and infrastructure if not mitigated;

(D) The ability to provide reasonable advance notice to aircraft operators consistent with the safety of the national airspace system and the needs of national security;

(E) The setting and character of any covered facility or asset, including whether it is located in a populated area or near other structures, and any potential for interference with wireless communications or for injury or damage to persons or property; and

(F) Potential consequences to national security if threats posed by unmanned aircraft systems or unmanned aircraft are not mitigated or defeated.

Section-by-Section Analysis

This proposal is intended to provide relief from certain federal laws to allow the CIA to properly respond to a full range of threats posed by Unmanned Aircraft Systems (UAS), subject to appropriate limitations, oversight, and safeguards implemented through a coordinated approach with the Federal Aviation Administration and Department of Transportation. This proposal is closely modeled on authority, found at 6 U.S.C. § 124n, that provides relief to the

Departments of Justice and Homeland Security to take actions against UAS posing a credible threat, notwithstanding otherwise potentially conflicting provisions of federal law.

In particular, the CIA seeks this authority to effectively respond to hostile foreign intelligence services collecting sensitive information about its personnel, facilities, and activities in the United States. The CIA's primary objective is to gain situational awareness of airspace over its facilities via UAS detection in order to protect sensitive national security activities. The CIA plans to invoke the proposed relief to take actions to protect a small number of facilities that would be identified in a classified annex. All such protected facilities would be in fixed locations, which are currently located within airspace subject to FAA-established flight restrictions or other special air traffic rules restricting UAS operations. Except in instances involving imminent physical threats or compromises to national security, the CIA would respond to unauthorized UAS overflight by using means other than interfering with or otherwise countering UAS operations.

Budget Implications: This proposal has no budgetary impact. The CIA already maintains a robust security program and Counter-UAS capability. The intent of this proposal is to authorize the CIA to employ its existing Counter-UAS capabilities to protect its domestic facilities.

Resubmission Information: This proposal was submitted to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence for inclusion in the FY2022 Intelligence Authorization Act.

Component Subject Matter Expert: James Turk, CIA Office of Security, (571) 280-7075, johntd3@ucia.gov

Reviewing Legal Counsel: William Reed, CIA Office of Security, (571) 204-6394, willirr2@ucia.gov

Reviewing Comptroller POC: James Turk, CIA Office of Security, (571) 280-7075, johntd3@ucia.gov

Component Contact for OMB: William Reed, CIA Office of Security, (571) 204-6394, willirr2@ucia.gov

Changes to Existing Law: This proposal would add a new section to the Central Intelligence Agency Act of 1949, codified at 50 U.S.C. § 3501 *et seq*, the full text of which is shown in the legislative language above.

NASA C-UAS Action Plan

Proposed Final Text for Legislative Language

51 U.S.C. § 20150

Detecting, identifying, monitoring, and tracking unmanned aircraft that threaten certain facilities and assets

(a) AUTHORITY FOR NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Notwithstanding section 46502 of title 49 or any provision of title 18, the Administrator may take, and may authorize personnel with assigned duties that include the safety, security, or protection of people, facilities, or assets to take, such actions as are described in subsection (b) that are necessary to detect, identify, monitor, and track a credible threat (as defined by the Administrator, in consultation with the Secretary of Transportation through the Administrator of the Federal Aviation Administration) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset.

(b) ACTIONS DESCRIBED

The actions authorized in subsection (a) are the following: during the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

(c) RESEARCH, TESTING, TRAINING, AND EVALUATION

(1) Requirement

For any action described in subsection (b), notwithstanding section 46502 of title 49 or any provision of title 18, the Administrator shall conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine its capability and utility prior to the use of any such technology for any action described in subsection (b). Personnel and contractors who do not have duties that include the safety, security, or protection of people, facilities, or assets may engage in research, testing, training, and evaluation activities pursuant to this section.

(2) Training of Personnel

The Administrator may provide training on measures to detect, identify, monitor, and track dangerous or illegally operated unmanned aircraft or unmanned aircraft systems to any personnel who are authorized to take such measures, including personnel authorized to take the actions described in subsection (b).

(3) Coordination for Research, Testing, Training, and Evaluation

The Administrator shall coordinate the Administration's procedures governing research, testing, training, and evaluation for carrying out any provision in this section with the Administrator of the Federal Aviation Administration before initiating such activities so the Administrator may ensure the activities do not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.

(d) FORFEITURE

Any unmanned aircraft system or unmanned aircraft described in subsection (a) may be seized by, and subject to forfeiture to, the United States.

(e) REGULATIONS AND GUIDANCE

The Administrator and the Secretary of Transportation may prescribe regulations and shall issue guidance in the respective areas of the Administrator or the Secretary of Transportation to carry out this section. All guidance and regulations under this subsection shall be developed in consultation with the Federal Communications Commission and the Assistant Secretary of Commerce for Communications and Information of the National Telecommunications and Information Administration and the Administrator of the Federal Aviation Administration.

(f) COORDINATION

(1) The Administrator shall coordinate with the Administrator of the Federal Aviation Administration prior to any action authorized by this section so the Administrator may ensure the action does not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.

(2) The Administrator shall respectively coordinate with

a. the Secretary of Transportation before issuing any guidance, or otherwise implementing this section so the Secretary of Transportation may ensure such guidance or implementation does not adversely impact critical national transportation infrastructure; and,

b. the Administrator of the Federal Aviation Administration so the Administrator may ensure such guidance or implementation does not adversely impact or

interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system

(3) The Administrator shall coordinate the development of guidance under subsection (e) with the Secretary of Transportation through the Administrator of the Federal Aviation Administration.

(4) The Administrator shall coordinate the development of the actions described in subsection (b) with the Secretary of Transportation (through the Administrator of the Federal Aviation Administration), and the Assistant Secretary of Commerce for Communications and Information of the National Telecommunications and Information Administration.

(g) PRIVACY PROTECTION

The regulations or guidance issued to carry out actions authorized under this section by the Administrator shall ensure that—

(1) the interception or acquisition of, or access to, or maintenance or use of, communications to or from an unmanned aircraft system under this section is conducted in a manner consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal law;

(2) communications to or from an unmanned aircraft system are acquired only to the extent necessary to support an action described in subsection (b);

(3) records of such communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Administrator determines that maintenance of such records is required under Federal law; is necessary for the purpose of any litigation; or is necessary to investigate or prosecute a violation of law, directly support

an ongoing security operation, or protect against dangerous or unauthorized activity by unmanned aircraft systems or unmanned aircraft; and

(4) such communications are not disclosed outside the National Aeronautics and Space Administration unless the disclosure—

(A) is necessary to investigate or prosecute a violation of law;

(B) would support the Department of Defense, a Federal law enforcement, intelligence, or security agency, or other relevant entity or person if such entity or person is engaged in a security or protection operation;

(C) is necessary to support a department or agency listed in subparagraph (B) in investigating or prosecuting a violation of law;

(D) would support the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory, statutory, or other enforcement action relating to, an action described in subsection (b); or

(E) is necessary to protect against dangerous or unauthorized activity by unmanned aircraft systems or unmanned aircrafts; or

(F) is otherwise required by law.

(h) ASSISTANCE AND SUPPORT

The Administrator is authorized to provide support or assistance, upon the request of an agency or department conducting a mission specified in section 130i of title 10, 210G of the Homeland Security Act of 2002 (6 U.S.C. 124n) or section 4510 of the Atomic Energy Defense Act (50 U.S.C. 2661), in fulfilling the requesting agency's or

department's roles and responsibilities for that mission, when exigent circumstances exist, limited to a specified timeframe and location, within available resources, on a non-reimbursable basis, in coordination with the Federal Aviation Administration.

(i) SEMIANNUAL BRIEFINGS AND NOTIFICATIONS

(1) IN GENERAL

On a semiannual basis beginning 6 months after the date this section is enacted, the Administrator shall provide a briefing to the appropriate congressional committees on the activities carried out pursuant to this section.

(2) REQUIREMENT

Each briefing required under paragraph (1) shall be conducted jointly with the Secretary of Transportation.

(3) CONTENT

Each briefing required under paragraph (1) shall include—

(A) policies, programs, and procedures to mitigate or eliminate impacts of such activities to the national airspace system and other critical national transportation infrastructure;

(B) a description of instances in which actions described in subsection (b) have been taken, including all such instances that may have resulted in harm, damage, or loss to a person or to private property;

(C) a description of the guidance, policies, or procedures established to address privacy, civil rights, and civil liberties issues implicated by the actions allowed under this section, as well as any changes or subsequent efforts that would significantly affect privacy, civil rights or civil liberties;

(D) a description of options considered and steps taken to mitigate any identified impacts to the national airspace system related to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b);

(E) a description of instances in which communications acquired during the course of operations of an unmanned aircraft system were held for more than 180 days or shared outside of the National Aeronautics and Space Administration;

(F) how the Administrator and the Secretary of Transportation have informed the public as to the possible use of authorities under this section;

(G) how the Administrator and the Secretary of Transportation have engaged with Federal, state, local, territorial and tribal law enforcement agencies to implement and use such authorities;

(H) an assessment of whether any gaps or insufficiencies still remain in current authorities, regulations, and policies that impede the ability of the National Aeronautics and Space Administration to detect, identify, monitor, and track the threat posed by the malicious use of unmanned aircraft systems and unmanned aircrafts ;

(I) recommendations to remedy any such gaps or insufficiencies, including but not limited to necessary changes in law, regulations, or policies; and

(J) a description of the impact of the authorities granted under this section on legitimate operator access to national airspace, and unmanned aircraft systems' and unmanned aircrafts' integration into the national airspace system;

(4) UNCLASSIFIED FORM

Each briefing required under paragraph (1) shall be in unclassified form, but may be accompanied by an additional classified briefing.

(j) RULE OF CONSTRUCTION

Nothing in this section may be construed to—

(1) vest in the Administrator any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration; or

(2) vest in the Secretary of Transportation or Administrator of the Federal Aviation Administration any authority of the Administrator of the National Aeronautics and Space Administration.

(k) SCOPE OF AUTHORITY

Nothing in this section shall be construed to provide the Administrator with additional authorities beyond those described in subsections (a), (c), and (d).

(l) DEFINITIONS

In this section:

(1) The term "appropriate congressional committees" means—

(A) the Committee on Commerce, Science, and Transportation of the Senate, and

(B) the Committee on Transportation and Infrastructure and the Committee on Science, Space, and Technology of the House of Representatives.

(2) The term "covered facility or asset" means any facility or asset that—

(A) is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Administrator, in coordination with the Secretary of Transportation

with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section;

(B) is located within the property of the National Aeronautics and Space Administration; and

(C) directly relates to the missions of the National Aeronautics and Space Administration pertaining to—

(i) launch services

(ii) reentry services; or

(iii) the protection of space support vehicles or payloads.

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

(4) The terms “launch services,” “reentry services,” “space support vehicle,” and “payload” have the meaning given those terms in section 50902 of this title.

(5) The term “personnel” means officers, employees, and contractors of the National Aeronautics and Space Administration, with assigned duties that include safety, security, or protection of personnel, facilities, or assets. To qualify under this provision, contractors conducting operations under subsection (b) must:

(i) be directly contracted by the National Aeronautics and Space Administration;

(ii) operate at a government-owned or government-leased facility;

(iii) not conduct inherently governmental functions; and

(iv) be trained and certified by the National Aeronautics and Space Administration to meet established guidance and regulations.

(6) For purposes of this section, the term "risk-based assessment" includes an evaluation of threat information specific to a covered facility or asset and, with respect to potential impacts on the safety and efficiency of the national airspace system and the needs of law enforcement and national security at each covered facility or asset identified by the Administrator of each of the following factors:

(A) Potential impacts to safety, efficiency, and use of the national airspace system, including potential effects on manned aircraft and unmanned aircraft systems, aviation safety, airport operations, infrastructure, and air navigation services related to the use of any system or technology for carrying out the actions described in subsection (b).

(B) Options for mitigating any identified impacts to the national airspace system related to the use of any system or technology, including minimizing when possible the use of any technology which disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (b).

(C) Potential consequences of the impacts of any actions taken under subsection (b) to the national airspace system and infrastructure if not mitigated.

(D) The ability to provide reasonable advance notice to aircraft operators consistent with the safety of the national airspace system and the needs of law enforcement and national security.

(E) The setting and character of any covered facility or asset, including whether it is located in a populated area or near other structures, whether the facility is open to the public, whether the facility is also used for nongovernmental functions, and

any potential for interference with wireless communications or for injury or damage to persons or property.

(F) The setting, character, timeframe, and national airspace system impacts of launch services and reentry services.

(G) Potential consequences to national security, public safety, or law enforcement if threats posed by unmanned aircraft systems are not detected, identified, monitored, and tracked.

(7) The terms "unmanned aircraft" and "unmanned aircraft system" have the meanings given those terms in section 44801 of title 49.

Sectional Analysis:

Executive Summary: This legislative proposal would authorize NASA to detect, identify, monitor and track unmanned aircraft systems (UAS) that threaten certain critical facilities and assets. NASA is not seeking authority to mitigate or "counter" a UAS-based credible threat at this time.

Background: UAS technology offers tremendous benefits to our economy and society, promising to transform the delivery of goods and services. UAS can also improve the safety and efficiency of countless activities, from the provision of medical services to the safe inspection of critical infrastructure. The economic impact of the integration of UAS into the national airspace system is estimated to reach tens of billions of dollars.

- At the same time, the potential misuse or errant use of this technology poses unique safety and security challenges. Overseas, ISIS, other terrorist groups, and criminal organizations use commercially available UAS to drop explosive payloads, deliver harmful substances, and conduct reconnaissance. Domestically, criminals use UAS to deliver narcotics across the southern border, drop contraband inside prisons, conduct illicit surveillance, and interfere with law enforcement operations.

- While some UAS operators may be clueless or careless, the danger exists for nonstate actors to utilize UAS to commit espionage or to carry out catastrophic terrorist attacks on high-visibility NASA targets, specifically, launch operations involving highly combustible rocket fuels. For example, on October 27, 2019, two UAS were observed and heard by Kennedy Space Center Security Police Officers during the landing of the X-37B space

plane – a highly classified program. The UAS were operating within the landing zone and presented a safety hazard to the incoming spacecraft, as well as an intelligence concern due to the nature of the program.

- While some launchpads are located on U.S. Space Force property and, as such, DoD may seek to use its authority under 10 U.S.C. § 130i to use UAS detection and mitigation capabilities, others, like Pad 39B on NASA's property, are not. This creates a serious threat in that the Agency will be using Pad 39B for the Artemis program which begins April 2022 and will be taking humans to the Moon. There are many risks associated with the Agency lacking the authority to detect, identify, monitor and track an unauthorized UAS. The most obvious and significant risk associated with lacking this authority is the inability to gather key information regarding a potential catastrophic terrorist attack directed against multi-billion dollar assets during high-profile launch and reentry events. Detection, identification, monitoring and tracking capabilities would enable a quicker security police response in locating the operator, discerning their intent, and resolving the threat without utilizing technical mitigation measures. Lacking this authority also lowers the threshold at which the Agency's protective services component would decide to "no-go" a decision to launch, potentially at great cost to the Agency and taxpayers.

- Due in part to potential conflicts with certain federal laws, the federal government has limited authority to deploy technology to detect UAS-based threats. This legislative proposal would close this critical gap, enabling NASA to protect certain critical facilities and assets from this growing threat by monitoring and tracking such threats.

The National Aeronautics and Space Act assigns specific powers to the Agency in fulfilment of its mission. *See* 51 U.S.C. § 20113. The Act does establish that "[t]he Administrator shall establish such security requirements, restrictions, and safeguard as the Administrator deems necessary." *See* 51 U.S.C. § 20132. The Act also grants specific authority to carry firearms and make arrests. *See* 51 U.S.C. §§ 20133-20134. None of these provisions specifically considers the detection, identification, monitoring, and tracking of a UAS that has entered the area surrounding a NASA facility.

Section XXX. Unmanned Aircraft System Detection and Mitigation Enforcement Authority

(a) In General.—Chapter 448 of title 49, is amended by adding at the end the following:

"§44811. Unmanned Aircraft System Detection and Mitigation Enforcement.

"(a) In General.—

"(1) No person may operate a system or technology to detect, identify, monitor, track, or mitigate an unmanned aircraft or unmanned aircraft system in a manner that adversely impacts or interferes with safe airport operations, navigation, or air traffic services, or the safe and efficient operation of the national airspace system.

"(2) The Administrator may take such action as may be necessary to address the adverse impacts or interference of operations that violate paragraph (1).

"(b) Penalties.—A person who operates a system or technology referred to in subsection (a)(1) in a manner that adversely impacts or interferes with safe airport operations, navigation, or air traffic services, or the safe and efficient operation of the national airspace system, is liable to the United States Government for a civil penalty of not more than $25,000 per violation.

"(c) Rule of Construction.—the word "person" as used in this section does not include—

"(A) the government of the United States of America or any bureau, department, instrumentality or other agency of the federal government; or

"(B) an officer, employee, or contractor of the government of the United States of America or any bureau, department, instrumentality or other agency of the federal

government if the officer, employee, or contractor is authorized by the government of the United States of America or any bureau, department, instrumentality or other agency of the federal government to operate a system or technology referred to in subsection (a)(1).".

(b) Conforming Amendment.—the table of contents for chapter 448 is amended by inserting at the end the following:

"44811. Unmanned Aircraft System Detection and Mitigation Enforcement."

Sectional Analysis

As provided in 49 U.S.C. 44810(a), the Administrator of the Federal Aviation Administration (FAA) shall work with the Secretary of Defense, the Secretary of Homeland Security, and the heads of other relevant Federal departments and agencies for the purpose of ensuring that technologies or systems that are developed, tested, or deployed by Federal departments and agencies to detect and mitigate potential risks posed by errant or hostile UAS operations do not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system (NAS). Currently, four federal departments have been expressly authorized by Congress to use UAS detection and/or mitigation systems and technologies with relief from federal criminal laws to address UAS-based threats against specified covered facilities and assets in the United States. The FAA has established coordination procedures with its federal security partners that enable the review and analysis by FAA of proposed UAS detection and/or mitigation research, testing, training, evaluation and deployment activities in order to evaluate any potential adverse impacts or interferences of these systems and technologies on the NAS and to identify any necessary FAA mitigations to address such secondary impacts or interference.

As UAS detection and mitigation authorities proliferate among non-federal entities, such as owners and operators of airports, state, local, territorial, and tribal law enforcement entities as well as owners and operators of critical infrastructure, the technology used by these entities poses a growing risk to the safe operations of lawful users of the national airspace (NAS), as well as other land or sea-based transportation entities or systems and persons and property on the ground.

Many UAS mitigation or "C-UAS" systems, as well as certain UAS detection systems, use technology that interfere with the signals between an operator and a drone. Depending upon the system, this can include interference with a drone's ability to communicate with other communications or navigation systems such as the Global Positioning System (GPS). Potential interference is not limited to drones, however. A system can also interfere with other air, land, or sea-based navigation or communications systems. In addition, once mitigated, a UAS may introduce adverse secondary effects to other aircraft in flight or persons and property on the ground.

Further, since some products feature both UAS detection and mitigation capabilities integrated into a single system, operators authorized to use detection-only technology may acquire and activate the mitigation technology either intentionally or unintentionally. As use of these technologies proliferate, the risk increases that users of UAS detection systems may intentionally or unintentionally disrupt lawful air, land, or sea operations, as well as persons or property on the ground, compromising the safety and efficiency of both the NAS and other components of the national transportation system.

For these reasons the FAA has proposed that the Administrator be provided with authority to take such action as may be necessary to protect the safety and efficiency of the NAS and to levy civil penalties against entities that misuse detection or mitigation systems. This authority would permit the Administrator of the FAA to initiate a civil enforcement action against any non-federal entity that uses (for any purpose) a UAS detection or mitigation system without express relief from federal criminal laws from Congress, or inconsistent with the authority granted by Congress, and causes an adverse impact on, or interference with, the safe and efficient operation of the NAS. This authority would further permit the Administrator of the FAA to initiate a civil enforcement action against any non-federal entity or person that otherwise uses (for any purpose) a UAS detection or mitigation system inconsistent with specified parameters for use established by the federal government, and causes an adverse impact on, or interference with, the safe and efficient operation of the NAS including but not limited to restrictions for use established in a list of authorized equipment maintained by a federal department or agency.