Office of the Attorney General
Washington, D. C. 20530

April 13, 2020

MEMORANDUM FOR: HEADS OF THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES
THE DRUG ENFORCEMENT AGENCY
THE FEDERAL BUREAU OF INVESTIGATION
THE FEDERAL BUREAU OF PRISONS
THE UNITED STATES MARSHALS SERVICE
THE JUSTICE MANAGEMENT DIVISION
THE EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS

FROM: THE ATTORNEY GENERAL

SUBJECT: Guidance Regarding Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems

Law enforcement and security agencies play a crucial role in ensuring the safe and secure integration of drone technology into the airspace. As recognized in the Department's 2019 *Policy on the Use of Unmanned Aircraft Systems*, drone technology has transformative potential as a valuable law-enforcement and public-safety tool, including for use in crime scene investigations, search and rescue operations, and security assistance. As drones become more powerful and capable, however, they also become a more attractive tool for criminals, terrorists, and other bad actors to cause disruption and destruction. Unfortunately, the threat is not theoretical.

To assist the Department of Justice ("DOJ") and Department of Homeland Security ("DHS") in combatting these threats, Congress passed the Preventing Emerging Threats Act of 2018 (codified at 6 U.S.C. § 124n) ("the Act"). The Act provides DOJ and DHS with a tailored grant of authority for authorized Department components to take certain counter-drone actions, notwithstanding certain provisions of federal law that could potentially constrain necessary and appropriate actions to mitigate credible drone threats to designated facilities and assets.

Today, I have issued guidance under the Act entitled, *Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems* ("the Guidance"). As authorized components, your counter-drone activities conducted under the Act will be governed by the Guidance. The Guidance outlines the process by which your components may seek approval for the use of counter-drone technologies and request designation of facilities or assets for protection. As a general rule, not every facility or asset will qualify for protection. Only those considered "high risk and a potential target" for drone activity – and relate to one of the authorized DOJ missions enumerated in the Act and the Guidance – will qualify.

Additionally, the Guidance reflects the Department's commitment to working with the Federal Aviation Administration to address potential barriers to safe and secure operations in the National Airspace System. As required in the Act, the Guidance was developed in coordination with the Department of Transportation and contains a number of provisions designed to minimize any effect on aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, and the use of airspace.

Importantly, the Guidance contains explicit protections for privacy, civil rights, and civil liberties, including limitations on the retention and use of any data collected during the course of counter-drone operations. Component actions taken pursuant to the Act must be consistent with the First and Fourth Amendments, and the Guidance requires each component deploying counter-drone technologies to train personnel on privacy and civil liberties in the counter-drone context.

To fully effectuate the Guidance, components must develop component-level guidance and policies, and fulfill interagency and inter-department coordination standards and requirements for procurement, training, and testing.

Your counter-drone operations under the Act, consistent with this Guidance and your component-level guidance and policies, should serve as a model for responsible use of counter-drone authorities. Even as you seek to minimize the risk to the airspace and follow strict requirements to respect privacy and civil liberties, the Act and the Guidance should empower your components to take appropriate and lawful action against drones that threaten the safety of the skies, the public, or your missions.

In mitigating the threats posed by errant or malicious drone operators, your components will not only protect the Department's missions, but will also facilitate American drone innovation and integration into one of the most complex airspaces in the world.

cc: John C. Demers, Assistant Attorney General, National Security Division
Beth A. Williams, Assistant Attorney General, Office of Legal Policy
Brian A. Benczkowski, Assistant Attorney General, Criminal Division

Guidance from the Attorney General:

Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems

April 2020

I. Background

The Preventing Emerging Threats Act of 2018 (the "Act"), Pub. L. No. 115-254, Div. H, §§ 1601–03, 132 Stat. 3186, 3522–30, codified in relevant part at 6 U.S.C. § 124n, permits **authorized Department personnel** to take **protective measures** that are necessary 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**. The Act requires guidance from the Attorney General before the authority may be exercised. This Guidance implements that requirement. It instructs Department of Justice ("Department") components on the processes and standards for seeking the Department's designation of a facility or asset for protection, as well as the legal framework for exercising measures to protect those designated facilities and assets. It also instructs Department components on the coordination of **protective measures** with the Federal Aviation Administration ("FAA") and other entities to address the impact of these measures on the national airspace system and other activities.

As required by the Act, the Attorney General has coordinated this Guidance with the Administrator of the FAA and the Secretary of Transportation. In preparing this Guidance, the Department has also consulted with the Department of Homeland Security ("DHS").

Authorized Department components that seek to deploy **protective measures** under the authority of the Act will issue an appropriate component policy that conforms to the requirements set out in subsection VIII.B.

II. Scope and responsibilities

A. Applicability. This Guidance applies only to the exercise of authority pursuant to the Act. This includes the authority granted by the Act to take **protective measures** necessary to mitigate **credible threats** from **unmanned aircraft** or **unmanned aircraft systems** to the safety or security of **covered facilities or assets** notwithstanding certain provisions of law, namely 49 U.S.C. § 46502 (aircraft piracy), 18 U.S.C. § 32 (destruction of aircraft), 18 U.S.C. § 1030 (computer fraud), 18 U.S.C. § 1367 (interference with the operation of a satellite), and chapters 119 (interception of communications) and 206 (pen registers and trap and trace devices) of Title 18. This Guidance addresses how **authorized Department components** will exercise the authority granted by the Act. This Guidance does not confer any additional authorities, nor does it affect any existing authorities under separate provisions of law, including

authorities to deploy **protective measures** or other measures to mitigate threats from **unmanned aircraft** or **unmanned aircraft systems** consistent with the Constitution, applicable federal laws and regulations, and Department policy. This Guidance does not apply to, or authorize activity directed at, any aircraft or aircraft system operated with human pilots, crew, or passengers onboard.

B. Authorized Department components. The following components of the Department, through **authorized Department personnel**, may exercise the authorities granted to the Attorney General by the Act:

1. The Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF");
2. The Drug Enforcement Administration ("DEA");
3. The Federal Bureau of Investigation ("FBI");
4. The Federal Bureau of Prisons ("BOP");
5. The United States Marshals Service ("USMS");
6. The Justice Management Division ("JMD"); and
7. The Executive Office for United States Attorneys ("EOUSA").

C. Authorized Department personnel. Only officers or employees of the Department who are in an **authorized Department component** and whose assigned duties include the security or protection of people, facilities, or assets may exercise the authority to take **protective measures** granted by the Act. **Authorized Department personnel** must exercise such authority in a manner that is consistent with their other authorities and this Guidance.

III. Requests from components

A. General approval requirements

1. Requests. If an **authorized Department component** seeks to have a facility or asset designated as a **covered facility or asset** and to deploy **protective measures** at such a facility or asset, the component head[1] will submit a written request for approval to the Deputy Attorney General (the "Approving Official"), or, when authorized in paragraph 4, the component head may serve as the Approving Official. All requests will comply with the requirements of this section and include such other information as the Approving Official may require.

2. Modifications. If an **authorized Department component** wishes to make a significant change to a previously designated **covered facility or asset** or a previously authorized **protective measure**, it will submit a request to the Approving Official updating the information previously provided under this

[1] The Director of EOUSA will submit a request on behalf of a United States Attorney's Office.

section and using the same procedures applicable to initial designations and authorizations. Modifications covered by this paragraph include a change in the location of the facility or asset; an expansion of the area covered by a **protective measure**; the deployment of a new **protective measure**; and a significant change to a previously approved **protective measure**. Modifications to the system settings of a **protective measure** generally will not constitute a significant change, but the **authorized Department component** will need to evaluate any change, including modifications to system settings, on a case-by-case basis to determine whether it constitutes a significant change that requires the submission of a request to the Approving Official. All changes to system settings, however, must be coordinated in advance with the FAA and, when relevant, the National Telecommunications and Information Administration ("NTIA").

3. Timing. **Authorized Department components** will submit requests under this section to the Approving Official as soon as practicable and no fewer than 30 days before the date on which **protective measures** would be deployed or a modification to such measures would go into effect.

4. Exceptional circumstances. If the head of an **authorized Department component** determines that, due to exceptional circumstances, it is not reasonably possible to submit a written request to the Approving Official in accordance with paragraph 3, he or she may designate a facility or asset as a **covered facility or asset**, approve the deployment of **protective measures**, or approve a modification to a previously designated **covered facility or asset** or previously authorized **protective measure**. Such a designation or authorization must comply with all the requirements of the Act, including the requirement for a risk-based assessment as described in subsection F and advance coordination with the FAA as described in section V. It must also comply with all the requirements of this Guidance except that, to the extent necessary, the documentation required by this Guidance may be prepared as soon as practicable after the designation or authorization and, in any event, no later than five business days after the designation or authorization. The head of the **authorized Department component** will immediately notify the FAA, the Office of the Deputy Attorney General ("ODAG"), the Office of Legal Policy ("OLP"), and the National Security Division ("NSD") of the designation or authorization.

B. Description of facility or asset. The request will describe the facility or asset proposed for designation with specificity, including its nature and location; its surroundings, including proximity to air traffic, airports, air traffic control facilities, or other airspace features; whether it is stationary or mobile; and whether a significant portion of the facility or asset belongs to or is operated by any person or entity other than the Department. The facility or asset must be in the **United States**. For purposes of this Guidance, a facility or asset may include, among other things, (i) a conveyance, such as a vehicle transporting a witness that the USMS or FBI is protecting, or (ii) for a specified

timeframe, the location of an active federal law enforcement investigation, emergency response, or security function. For a mobile facility or asset, the request will describe as specifically as possible the anticipated locations of the facility or asset while it will be covered by the proposed **protective measures.**

C. Relationship to authorized mission. The request will describe how the facility or asset directly relates to one or more authorized missions of the Department (consistent with governing statutes, regulations, and orders issued by the Attorney General) that pertain to:

1. Personal protection operations by the FBI, as authorized by 28 U.S.C. § 533.

2. Personal protection operations by the USMS of federal jurists, court officers, witnesses, and other threatened persons in the interests of justice, as authorized by 28 U.S.C. § 566(e)(1)(A).

3. Provision of security by the USMS for federal courts, as authorized by 28 U.S.C. § 566(a).

4. Protection of penal, detention, and correctional facilities and operations conducted by the BOP.

5. Protection of buildings and grounds leased, owned, or operated by or for the Department.

6. Protection of a **National Special Security Event** and **Special Event Assessment Rating Event**.

7. Protection of an active federal law enforcement investigation, emergency response, or security function. A request involving any of these missions must describe how the protection being provided, including the use of **protective measures,** will be limited to a specified timeframe and location.

8. Provision of support to state, local, territorial, or tribal law enforcement to ensure the protection of people and property at mass gatherings requested in accordance with section IV by the chief executive officer of the State or territory.

D. Airspace restrictions. The request will describe whether the facility or asset is covered by airspace to which access is restricted, such as airspace subject to temporary flight restrictions imposed by the FAA in accordance with 14 C.F.R. § 99.7 or other applicable law, and will describe any such airspace restrictions. The requester will work with the FAA, which may determine that additional or modified airspace restrictions are needed to support enforcement efforts and to mitigate or eliminate risks posed by the **protective measures** to the airspace.

E. Protective measures. The request will describe:

1. The **protective measures** that the component seeks authority to use to protect the safety or security of the facility or asset, including:

a. The technology and equipment that the component plans to deploy, including its capabilities and specific technical characteristics;

b. Whether the Department's Unmanned Aircraft Systems Working Group ("UAS WG"),[2] or a designated subgroup thereof, or the FAA recommends the use of such technology and equipment and, if not, a justification for using the technology or equipment chosen; and

c. Any applicable policies or procedures relating to use of the **protective measures** at the facility or asset, including any relating to use of force and approvals for the use of the **protective measures**;

2. Whether the use of the **protective measures** is expected to result in the interception or acquisition of communications subject to the privacy protections of section VI and, if so, the nature of those communications;

3. The time period during which the **protective measures** will be used and the proposed area or airspace covered by the measures; and

4. Measures that will be employed using authorities other than the Act to mitigate the threat posed by an **unmanned aircraft** or **unmanned aircraft system**, if such measures will be used in conjunction with **protective measures** deployed or used under the authority of the Act.

F. Risk-based assessment. The request will:

1. Describe why there are reasonable grounds to believe, based on the totality of the circumstances, that the activities of **unmanned aircraft** or **unmanned aircraft systems** in the area or airspace covered by the proposed **protective measures** represent a **credible threat** to the safety or security of the facility or asset;

2. Describe why, based on the totality of the circumstances, including the results of the risk-based assessment required by the Act, the facility or asset (other than a

[2] Under the direction of the Deputy Attorney General, the Department-wide UAS WG provides a forum to coordinate and discuss matters relating to the Department's use of **unmanned aircraft** and **unmanned aircraft systems** and its use of **protective measures** to mitigate threats posed by **unmanned aircraft** and **unmanned aircraft systems**. The UAS WG is chaired by OLP and includes representatives from the FBI, DEA, USMS, ATF, BOP, ODAG, NSD, JMD, EOUSA, the Criminal Division, the Office of Justice Programs, the Office of Community Oriented Policing, the Office of Legislative Affairs ("OLA"), the Office of Privacy and Civil Liberties, and the JMD Office of the Chief Information Officer.

facility or asset identified in paragraph C.6) should be identified as high-risk and a potential target of the **unlawful activities** of **unmanned aircraft** or **unmanned aircraft systems**; and

3. Contain a risk-based assessment with respect to the potential impacts of **protective measures** on public safety, including the safety, efficiency, and use of the national airspace system, and the needs of law enforcement and national security at the facility or asset. The assessment will be coordinated with the FAA as described in section V and include an evaluation of the following factors:

a. The 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 a **protective measure**;

b. The options for mitigating any identified impacts to the national airspace system related to the use of any system or technology for carrying out a **protective measure**, including minimizing, when possible, the use of any technology that disrupts the transmission of radio or electronic signals;

c. The potential consequences of the impacts of a **protective measure** 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 the 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. If the facility or asset involves a **National Special Security Event** or **Special Event Assessment Rating Event**, the setting, character, timeframe, and national airspace system impact of the event; and

g. The potential consequences to national security, public safety, or law enforcement if threats posed by **unmanned aircraft** or **unmanned aircraft systems** are not mitigated or defeated, including any cybersecurity, espionage, intelligence, surveillance, reconnaissance, operational interference, criminal, chemical, biological, radiological, nuclear, or explosive-related risks.

G. Role of other entities. The request will describe whether (to the knowledge of the requesting **authorized Department component**) any other Department component, federal department or agency, or other entity also intends to deploy, under the authority of the Act or otherwise, technology or equipment to mitigate the threat posed by **unmanned aircraft** or **unmanned aircraft systems** to the same mission, facility, or asset.

H. Requests from States or territories. The request will state whether the chief executive officer of a State or territory has requested the **protective measures** in accordance with section IV.

I. Coordination. The request will describe the coordination that the component has conducted with the FAA as described in section V, including the risk-based assessment outlined in paragraphs F.2 and F.3 and the coordination described in subsection V.A, and the results of that coordination. The request will also describe any coordination or consultation that the component has conducted with the NTIA or other entities inside or outside the Department, and the results of such coordination or consultation.

J. Legal review. The request will include a summary of component counsel's legal assessment of the request.

K. Approval. If the Approving Official finds that (i) the request is consistent with the requirements of the Act, other applicable law, and this Guidance; and (ii) furthers the priorities and objectives of the Department, including consideration of resource constraints and priorities, the Approving Official may:

1. Designate the facility or asset as a **covered facility or asset** based on:

    a. A finding that the activities of **unmanned aircraft** or **unmanned aircraft systems** pose a **credible threat** to the facility or asset; and

    b. Identification of the facility or asset as high-risk and a potential target of the **unlawful activities** of such aircraft or systems, except that a facility or asset identified in paragraph C.6 may be presumed to be high-risk and a potential target for such **unlawful activities**;

2. Approve the deployment and use of some or all of the requested **protective measures** at the **covered facility or asset**; and

3. Specify any conditions for the deployment or use of **protective measures**, such as requirements for:

    a. Approval of operational plans or documents;

    b. Specific high-level or on-site approval for the use of some or all of the **protective measures**, such as the measures identified in paragraphs X.G.2 through 6; or

c. Specific operational and technical measures necessary to sufficiently mitigate impacts on aviation safety and the national airspace system.

IV. Requests to support state, local, territorial, or tribal law enforcement

A. Requests. An **authorized Department component** may request authorization to designate a facility or asset as a **covered facility or asset** and to deploy, or to deploy together with DHS, **protective measures** to support state, local, territorial, or tribal law enforcement to ensure protection of people and property at mass gatherings. The component may seek such authorization at the request of the chief executive officer of a State or territory, to the extent consistent with authorized missions of the Department.

B. Requirements. A request by an **authorized Department component** under this section will be made to the Approving Official and will:

1. Specifically describe the mass gathering, including its location and Special Event Assessment Rating, if applicable;

2. Specifically describe the threat to the mass gathering posed by **unmanned aircraft** or **unmanned aircraft systems**, including intelligence regarding the threat, any characteristics of the mass gathering relevant to assessing the threat, and any additional special security concerns;

3. Identify any airspace restrictions established by the FAA for the mass gathering (see subsection III.D);

4. Identify the specific time period for the support;

5. Comply with the requirements of this Guidance, including the timing, risk-based assessment, and other requirements of section III;

6. Describe how the component will provide the support within available resources;

7. Describe how the component will provide the support without delegating any authority under the Act to state, local, territorial, or tribal law enforcement;

8. Include the underlying request from the chief executive officer of the State or territory; and

9. Include such other information as the Approving Official may request.

C. Approval. The Approving Official may approve a request as provided in subsection III.K or, when applicable, paragraph III.A.4.

D. Reporting. Any Department component receiving a request for support involving the use of **protective measures** from the chief executive of a State or territory will promptly report the request to the Deputy Attorney General and the FAA, and otherwise as directed by the Deputy Attorney General, even if the component believes that it or the Department should not, or cannot consistent with the Act or available resources, provide such support.

V. Coordination

A. Department of Transportation

1. Coordination with the Secretary of Transportation. Pursuant to a delegation of authority from the Secretary of Transportation to the FAA, any coordination with the Secretary of Transportation required under the Act or this Guidance will be conducted through the FAA acting on behalf of the Secretary of Transportation. Any reference in the Guidance to coordination with the FAA includes coordination with the FAA acting on behalf of the Secretary of Transportation.

2. Actions pursuant to the Act. When an **authorized Department component** proposes to take any action under authority provided by the Act, including the deployment of **protective measures**, that might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace, the component will coordinate with the FAA. **Authorized Department components** will initiate such coordination as soon as practicable and, with the exception of measures approved for deployment or modification under paragraph III.A.4, no fewer than 30 days before the date on which the **protective measures** would be deployed or the modification would go into effect. In the case of protective measures approved for deployment or modification under paragraph III.A.4, the **authorized Department component** must coordinate with the FAA in advance, but such coordination may be initiated less than 30 days before deployment or modification. An **authorized Department component** proposing to issue policy or guidance implementing this Guidance (such as any guidance issued under section VIII) will coordinate the policy or guidance with the FAA.

3. Mobile deployments. In particular, any **authorized Department component** conducting, or requesting approval to deploy, mobile **protective measures** will coordinate those measures as far in advance as practicable with the FAA.

4. Advance requests. An **authorized Department component** may request a categorical determination from the FAA that a particular system used to implement **protective measures**, as a general matter or when used in identified circumstances, either does not have a negative impact, or has a level of impact that falls within acceptable limits, on the safety, efficiency, and use of the national airspace system. The impact of such a measure includes potential effects on manned and unmanned aircraft, aviation safety, airport operations and infrastructure, and air navigation services. This categorical determination does not relieve the component from spectrum coordination with the NTIA.

5. Unacceptable impacts. If the FAA determines that a proposed **protective measure** poses an unacceptable degree of risk to the safety, efficiency, or use of the national airspace system, the **authorized Department component** will coordinate with the FAA to identify potential steps that will both reduce the risk posed by the **protective measure** to an acceptable level and still adequately

address the threat posed by **unmanned aircraft** or **unmanned aircraft systems**. Such steps may include using a particular measure only in identified circumstances or imposing conditions or technical limitations on its use.

B. **Other entities.** To the extent feasible and appropriate, an **authorized Department component** will also coordinate with any other federal department or agency, or any state, local, tribal, territorial, or foreign governments, whose known interests or activities may be substantially affected by the component's proposed policy, guidance, or action, such as the deployment of **protective measures**, under the Act or this Guidance.

C. Internal coordination. OLP, in consultation with the Department's UAS WG and any appropriate subgroups to the extent appropriate and helpful, will direct and coordinate the following functions:

1. Facilitating and coordinating procurement and training in accordance with section VII;

2. Identifying recommended technologies and equipment for use by **authorized Department components**;

3. Promoting the sharing and accessibility of testing and evaluation data between components and with other federal departments and agencies;

4. Coordinating, prioritizing, and de-conflicting component requests to designate **covered facilities or assets** or to authorize **protective measures**, and making recommendations concerning such requests;

5. Reviewing the component-level policies required by section VIII and any other policies necessary to carry out the authorities granted by the Act;

6. Reviewing activities conducted under the Act by the Department or related activities conducted by others, and recommending changes or improvements; and

7. Ensuring that the Department, through OLA, complies with the congressional reporting requirements of the Act.

VI. Privacy protections

A. General. In exercising authority under the Act, an **authorized Department component** will consult as appropriate with the Senior Component Official for Privacy ("SCOP"). A component may only intercept, acquire, access, maintain, use, or disseminate communications in a manner consistent with the Constitution, including the First and Fourth Amendments; the Act; and other applicable federal laws, regulations, guidelines, and procedures, including the Privacy Act of 1974. A component may not deploy or use any **protective measure** under authority of the Act solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of rights secured by the Constitution or laws of the United States. A component should consider and be sensitive at all times to the potential impact **protective measures** may have on

legitimate activity by **unmanned aircraft** and **unmanned aircraft systems**, including systems operated by the press.

B. Retention. Department components may maintain records of communications to or from **unmanned aircraft** or **unmanned aircraft systems** intercepted or acquired under authority of the Act if, and for such period that, an authorized component official designated as specified in subparagraph VIII.B.1.n determines the maintenance of such records:

1. Is necessary to investigate or prosecute a violation of law;

2. Is necessary to directly support an ongoing security operation;

3. Is required under federal law; or

4. Is necessary for the purpose of litigation, including litigation that is reasonably foreseeable.

Department components may maintain records of any other communications to or from **unmanned aircraft** or **unmanned aircraft systems** intercepted or acquired under authority of the Act only for as long as necessary, and in no event for more than 180 days.

C. Dissemination. Department components may disseminate communications intercepted or acquired under authority of the Act outside the Department only if the dissemination is legally authorized and:

1. Is necessary to investigate or prosecute a violation of law;

2. Would support:

    a. the Department of Defense,

    b. a federal law enforcement agency, or

    c. 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 a **protective measure**;

3. Is to DHS in the course of a security or protection operation of either the Department or DHS or a joint operation of the Department and DHS; or

4. Is otherwise required by law.

D. Communications acquired by DHS. The requirements of subsections A through C also limit the retention and dissemination by the Department of communications that DHS acquires under authority of the Act and provides to the Department.

E. State or local law enforcement. Department components may, to the extent necessary, share threat information acquired under authority of the Act with state, local, territorial, or tribal law enforcement in the course of a security or protection operation. Threat information includes the location, altitude, speed, trajectory, track, make and model, registration number or other unique identifier, and payload of an **unmanned aircraft**, as well as the location of the operator as indicated by the position of the aircraft controller or ground control station. Threat information, however, does not include communications acquired under authority of the Act.

F. Searches and seizures. As in all circumstances, components will comply with the requirements of the Fourth Amendment and observe the policies of the Department with respect to searches and seizures. **Protective measures** taken under authority of the Act to mitigate a **credible threat** posed by an **unmanned aircraft** or **unmanned aircraft system** to the safety or security of a **covered facility or asset** are exempt from certain statutory requirements referenced in section II.A. All **protective measures**, however, must comply with any other statutory requirements applicable under the facts and circumstances and with the Fourth Amendment if the protective measures involve a search or seizure. The **protective measures** authorized by the Act, moreover, are limited to actions necessary to mitigate a **credible threat** posed by an **unmanned aircraft** or **unmanned aircraft system** to the safety or security of a **covered facility or asset**, and once that **credible threat** is mitigated or has otherwise ended, the exemptions under the Act no longer apply.

G. Recordkeeping. Department components will maintain records of how they access, maintain, use, and disseminate communications intercepted or acquired under authority of the Act.

VII. Procurement and training

A. Procurement. Before an **authorized Department component** acquires (for purposes other than testing and evaluation) technology or equipment (i.e., systems) to take **protective measures** under authority of the Act, it will:

1. Consider systems that minimize the risk of harm posed to bystanders, responders, and other persons;

2. Consider systems that minimize the risks to the safety, efficiency, and use of the national airspace system;

3. Consider systems that support the effective differentiation (including minimizing false positives and inaccurate location determinations) of legitimate, lawful **unmanned aircraft system** operations from activity that warrants further evaluation;

4. Consider systems that support the sharing of detection, tracking, identification, and interdiction data with government partners;

5. Consider the interoperability of the technology or equipment and whether the component will be able to share or transfer it within the Department or the Government;

6. Consider whether to purchase or lease the technology or equipment in light of the component's knowledge of its effectiveness and anticipated life expectancy;

7. Research, test, and evaluate the technology or equipment to determine its capability and utility, or review the results of similar research, testing, and evaluation conducted by other appropriate entities. (This requirement for testing and evaluation also applies to technology or equipment that a component may already possess.)

8. Before any testing or evaluation of the technology or equipment by the Department, the **authorized Department component** conducting the testing or evaluation will coordinate with the FAA if the activity might affect aviation safety, civilian aviation and aerospace operations, aircraft airworthiness, or the use of the airspace, and with the NTIA if the activity might affect the radio frequency spectrum;

9. Inform the Department's UAS WG about proposed testing and the results of testing and, where appropriate, similarly inform other Department components;

10. Submit any technology or equipment that is capable of processing, storing, or transmitting information to the information technology acquisition review and supply chain assessment processes, or obtain a waiver, if required by the Department-wide memorandum issued by the Assistant Attorney General for Administration on October 29, 2018 or by any subsequent Department policy; and

11. Ensure that any technology or equipment acquired or leased includes information-collection and reporting systems adequate to enable the Department to meet its reporting obligations on mission operations, cybersecurity, and supply chain issues, consistent with any guidance from the JMD Office of the Chief Information Officer.

B. Training Requirement for System Operators. An **authorized Department component** that acquires technology or equipment in order to take **protective measures** under authority of the Act will ensure that **authorized Department personnel** are properly trained on the use of the technology or equipment and on their responsibilities under this Guidance. Training will be conducted at regular intervals and include instruction on privacy and civil liberties, in consultation with the SCOP, as well as on all relevant federal legal standards applicable to the use of such **protective measures**.

VIII. Implementing policy

A. Use of force. If an **authorized Department component** intends to deploy **protective measures** to counter **unmanned aircraft** or **unmanned aircraft systems** that

may involve the use of force, it will review applicable use of force policies and training materials as they relate to **unmanned aircraft** and **unmanned aircraft systems** and, after coordination with the FAA, DHS, and other appropriate federal departments or agencies to the extent required by law, recommend any changes for approval by an official authorized to change such policies or training materials.

B. Component policy

1. The head of any **authorized Department component** that proposes to deploy **protective measures** under the authority of the Act will issue a component policy that addresses:

a. Prioritizing requests for **protective measures**.

b. Identifying the types of **protective measures** that may be authorized and the approvals required for their deployment and use.

c. Reviewing, by component legal counsel, requests for approval under sections III and IV.

d. Preparing risk-based assessments as required by the Act and subsection III.F.

e. Developing appropriate operational plans for the deployment and use of **protective measures** at any **covered facility or asset.**

f. Developing and implementing procedures and other measures in coordination with the FAA to address the safety and efficiency impacts of **protective measures** on the national airspace system.

g. Notifying appropriate persons or entities, including the FAA, of potentially concerning sightings of **unmanned aircraft** near a **covered facility or asset** or in or near airspace subject to relevant flight restrictions.

h. Conducting research, testing, training on, and evaluation of technology and equipment for taking **protective measures**, including internal approval requirements for any such activities and procedures to ensure that such activities are conducted consistent with applicable law. Such procedures will provide for preventing or minimizing the effect of such activities on third parties.

i. Coordinating the deployment and use of technology and equipment for taking **protective measures** with other appropriate government entities, including the FAA and NTIA, as well as with facilities or assets in an area where the component may use **protective measures**.

j. Notifying appropriate persons or entities, including the FAA, at the earliest operationally feasible opportunity after initiating the use of any **protective measures** and sharing post-incident data and analysis.

k. Treating a downed or otherwise captured **unmanned aircraft** or **unmanned aircraft system** as a potential explosive device or as posing chemical, biological, radiological, or nuclear risks.

l. Treating a downed or otherwise captured **unmanned aircraft** or **unmanned aircraft system** as potentially possessing evidentiary value, either as an instrumentality of a crime or as a device containing evidence of a crime, or both.

m. Seizing and seeking forfeiture of an **unmanned aircraft** or **unmanned aircraft system** in accordance with subsection IX.A and applicable Department procedures and federal law.

n. Identifying component officials who may approve the retention of communications beyond 180 days in accordance with subsection VI.B.

o. Documenting compliance with the requirements of this Guidance, including requirements to maintain detailed records of the deployment or use of **protective measures**.

p. Maintaining operational security, including, as needed, the use of proper classification and dissemination controls.

q. Conducting oversight of the use of **protective measures.**

r. Coordinating with the Department's Office of Public Affairs in advance of any new deployment of **protective measures**.

s. Notifying OLA and OLP at least seven days before deploying any new technology or equipment to carry out **protective measures**, so that the Department can notify appropriate congressional committees within 30 days of such deployment, as required by the Act.

t. Otherwise ensuring compliance with congressional reporting requirements.

2. The head of the **authorized Department component** will coordinate the development of such policy as required by section V.

3. An **authorized Department component** that has not issued such a component policy may, if necessary, submit a request to deploy **protective measures** consistent with this Guidance, including the requirements of section III.

4. The head of any **authorized Department component** that proposes to deploy **protective measures** under the authority of the Act to protect fixed sites under

paragraphs III.C.1–III.C.5 will issue criteria for ranking or categorizing for prioritization each fixed site for which **protective measures** are requested and will maintain a current list of ranked sites.

IX. General provisions

A. Forfeiture. Any **unmanned aircraft** or **unmanned aircraft system** that is seized through the use of a **protective measure** may be forfeited when consistent with federal law and Department policies, including the implementing policy required by section VIII.

B. Activities conducted with others. No Department personnel may participate in or request any person or entity to undertake any activity that is inconsistent with this Guidance.

C. Questions of interpretation. Authorized Department components and components participating in the Department's UAS WG will consult with NSD on significant questions regarding interpretations of the Act or this Guidance. To the extent written advice is provided, NSD, in consultation with OLP, will disseminate it to other entities, as appropriate.

D. Modifications, departures, and amendments

1. Modifications. If Department personnel identify a situation that they believe requires them to act inconsistently with this Guidance in order to protect the national security of the United States, enforce the criminal law, or protect life or property from serious harm, those personnel should immediately contact their legal counsel or other appropriate official in their component to request that this Guidance be modified. Any modification to this Guidance must comply with paragraph 2.

2. Amendments. The Deputy Attorney General may amend this Guidance or issue such further policies or guidance as may be necessary or appropriate to implement the Act. All substantive amendments and additional policies or guidance will be coordinated in accordance with section V.

3. Departures. If, in order to protect against an immediate or grave threat to human life, property, or national security, an **authorized Department component** determines that it must take action in apparent departure from this Guidance (but still in accordance with applicable federal law, including the Act and the Fourth Amendment to the Constitution) and that it is not feasible to obtain a timely modification of this Guidance, the component may take such action. Appropriate component personnel will report the action as quickly as reasonably practicable and in any event within three business days to the head of the component, OLP, NSD, and the FAA.

E. Congressional reporting. OLA, in consultation with the Department's UAS WG and component legislative affairs personnel, will prepare and submit all reports to

Congress required by the Act in a timely manner, and prepare and submit any other reports to Congress related to the Department's activities under the Act or this Guidance. Department components will comply with the standards and deadlines established by OLA for providing the information OLA needs to carry out these responsibilities.

F. No legal rights. This is internal guidance directed solely to Department components and employees. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. It also does not place any limitation on the otherwise lawful investigative, prosecutorial, or litigative prerogatives of the United States.

X. Definitions

A. Authorized Department component means a component identified in subsection II.B.

B. Authorized Department personnel means officers and employees of the Department who are identified in subsection II.C as authorized to take **protective measures** under the authority of the Act.

C. Covered facility or asset means a facility or asset designated in accordance with sections III or, where applicable, IV.

D. Credible threat means the reasonable belief, based on the totality of the circumstances, that the activity of an **unmanned aircraft** or **unmanned aircraft system** may, if unabated:

1. Cause physical harm to a person;

2. Damage property, assets, facilities, or systems;

3. Interfere with the mission of a **covered facility or asset**, including its movement, security, or protection;

4. Facilitate or constitute **unlawful activity**;

5. Interfere with the preparation or execution of an authorized government activity, including the authorized movement of persons;

6. Result in unauthorized surveillance or reconnaissance; or

7. Result in unauthorized access to, or disclosure of, classified, sensitive, or otherwise lawfully protected information.

E. Electronic communication, **intercept**, **oral communication**, and **wire communication** have the meanings given those terms at 18 U.S.C. § 2510.

F. National Special Security Event means a designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity.

G. Protective measures mean one or more of the following actions:

1. During the operation of an **unmanned aircraft** or **unmanned aircraft system**, the detection, identification, monitoring, and tracking of the **unmanned aircraft** or **unmanned aircraft system**, without prior consent, including by means of intercepting or otherwise accessing a **wire**, **oral**, or **electronic communication** used to control the **unmanned aircraft** or **unmanned aircraft system**.

2. Warning the operator of the **unmanned aircraft** or **unmanned aircraft system**, including by passive or active, and direct or indirect physical, electronic, radio, and electromagnetic means.

3. Disrupting control of the **unmanned aircraft** or **unmanned aircraft system**, without prior consent, including by disabling the **unmanned aircraft** or **unmanned aircraft system** by intercepting, interfering, or causing interference with **wire**, **oral**, **electronic**, or radio **communications** used to control the **unmanned aircraft** or **unmanned aircraft system**.

4. Seizing or exercising control of the **unmanned aircraft** or **unmanned aircraft system**.

5. Seizing or otherwise confiscating the **unmanned aircraft** or **unmanned aircraft system**.

6. Using reasonable force, if necessary, to disable, damage, or destroy the **unmanned aircraft** or **unmanned aircraft system**.

H. Special Event Assessment Rating Event means an event that is evaluated by the federal Special Events Working Group using a risk assessment methodology that considers the types of threats to the event, the vulnerabilities of the event, and the potential adverse consequences if a threat materializes. DHS and FBI co-chair the Working Group. Events are assigned a level 1 through 5 rating that is used in determining the level of federal support provided in securing the event. Level 1 is the highest rating and a level 1 event would receive the most federal support.

I. United States, when used in a geographic sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, any possession of the United States, and any waters within the jurisdiction of the United States.

J. Unlawful activity includes a violation of the laws or regulations governing the safe operation of **unmanned aircraft**. This includes violations of the Federal Aviation Regulations, such as unauthorized entry into FAA-designated restricted or special-use airspace, including prohibited or restricted airspace; national defense airspace; areas

subject to temporary flight restrictions; or warning, alert, military operations, national security, or controlled firing areas.

Unlawful activity also includes violations of other federal, state, local, territorial, or tribal laws, such as:

1. Laws prohibiting the provision of material support to terrorists or designated foreign terrorist organizations;

2. Laws protecting the safety of persons or property;

3. Laws prohibiting interference with law enforcement or public safety activities; and

4. State laws prohibiting nuisance activities.

K. Unmanned aircraft and **unmanned aircraft system** have the meanings given those terms at 49 U.S.C. § 44801.