

Page 01

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Page 05

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act





**U.S. Department of Homeland Security**

**Best Practices for**

**Protecting Privacy, Civil Rights & Civil Liberties**

**In**

**Unmanned Aircraft Systems Programs**

**U.S. Department of Homeland Security**  
**Privacy, Civil Rights & Civil Liberties**  
**Unmanned Aircraft Systems Working Group**

**December 18, 2015**

## Joint Statement

### Co-Chairs

#### **Department of Homeland Security Privacy, Civil Rights & Civil Liberties Unmanned Aircraft Systems Working Group**

As co-chairs of the Department of Homeland Security's (DHS) Privacy, Civil Rights & Civil Liberties Unmanned Aircraft Systems Working Group (DHS Working Group), we are pleased to present these best practices, which reflect DHS' experiences in building unmanned aircraft system programs founded on strong privacy, civil rights, and civil liberties protections. Unmanned aircraft systems are an essential tool in DHS's border security mission and present a great deal of promise for assisting first responders and improving situational awareness.

These best practices represent an optimal approach to protecting individual rights that is influenced by U.S. Customs and Border Protection's (CBP) ten years of experience using unmanned aircraft systems as a tool in protecting and securing the Nation's borders. We are sharing these reflections broadly, recognizing that government entities (including CBP) have various limitations based upon their respective missions, operating characteristics, and legal authorities, and that many of the considerations that apply to our agency may not be applicable or appropriate for other entities. The DHS Working Group neither proposes nor intends that this document regulate any other government entity. Our goal, rather, is simply to share the best practices we have identified as helping to sustain privacy, civil rights, and civil liberties throughout the lifecycle of an unmanned aircraft systems program.<sup>1</sup>

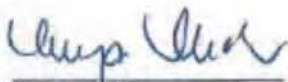
We provide these best practices to share DHS's view of how to protect individual rights in this evolving technology-driven field. The rapid changes in technology compel legal, privacy, and civil rights and civil liberties experts to continually review and update implementing documents (e.g., best practices, standard operating procedures, and policies) to properly reflect changes in the law, as well as advances in the technology and new applications of the technology. It is important for government entities to ensure that technology is not used in a manner that erodes or violates an individual's statutory or constitutional rights.

---

<sup>1</sup> This guidance is intended for first responders (e.g., emergency management, emergency medical service, fire departments, and security professionals responding to disasters and other emergencies), and does not seek to provide guidance in regard to investigative use of unmanned aircraft systems. DHS's primary experience with UAS operations, which serves as the basis for these best practices, has come in the context of general border surveillance operations.

Finally, even though these best practices are intended for DHS and our local, state, and federal government partners and grantees, the private sector may also find these recommendations valuable and instructive in creating their unmanned aircraft system programs.

Sincerely,



Megan H. Mack  
Officer for Civil Rights  
and Civil Liberties



Karen Neuman  
Chief Privacy Officer



Edward E. Young  
Deputy Assistant Commissioner  
U.S. Customs and Border Protection



# U.S. Department of Homeland Security

## Best Practices for

### Protecting Privacy, Civil Rights & Civil Liberties In Unmanned Aircraft Systems Programs

#### Overview

The term “unmanned aircraft systems” is used to define an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot or system operator in command to operate safely and efficiently in the national airspace system.<sup>1</sup> In the past, unmanned aircraft were referred to as “unmanned aerial vehicles,” but today they are simply referred to as unmanned aircraft.

Unmanned aircraft systems offer a variety of benefits for protecting our borders; supporting law enforcement; assisting in search and rescue operations; locating forest fire hot spots; evaluating dangerous environments (e.g., post-chemical spill and radiological exposure); conducting forensic imagery; inspecting pipeline and utilities; monitoring evacuation routes; and relaying telecommunication signals.<sup>2</sup>

The development of a new technology, significant improvement of a current technology, or the new application of an existing technology often results in concerns about the impact on individual privacy, civil rights, and civil liberties. For instance, the integration of government and commercial unmanned aircraft systems into the National Airspace System by 2015, as required by the *Federal Aviation Administration Modernization and Reform Act of 2012*, has prompted questions about how this might impact individual rights.<sup>3</sup>

In this regard, the Acting Officer for Civil Rights and Civil Liberties, the Acting Chief Privacy Officer, and the Assistant Commissioner for U.S. Customs and Border Protection, Office of Air and Marine jointly established the DHS *Unmanned Aircraft Systems Privacy, Civil Rights and Civil Liberties Working Group* (DHS Working Group) in September 2012 to “provide leadership to the homeland security enterprise by clarifying the privacy, civil rights, and civil liberties legal and policy issues surrounding government use of [Unmanned Aircraft Systems].”<sup>4</sup>

---

<sup>1</sup> *FAA Modernization and Reform Act of 2012*, Pub. L. No. 112-95.

<sup>2</sup> Government Accountability Office, *Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*, p. 10, GAO-12-981 (September 2012).

<sup>3</sup> *Id.* at 2-3, 32-36.

<sup>4</sup> *Memorandum for the Secretary, Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department’s Use and Support of Unmanned Aerial Systems (UAS)*, from Tamara J. Kessler, Acting Officer, Office for Civil Rights and Civil Liberties; and Jonathan R. Cantor, Acting Chief Privacy Officer (September 12, 2012). The DHS *Unmanned Aircraft Systems Privacy, Civil Rights and Civil Liberties Working Group*, co-chaired by the DHS Office for Civil Rights & Civil Liberties, DHS Privacy Office and U.S. Customs and Border Protection, is comprised of policy and operational subject matter experts from across DHS including the U.S. Coast Guard, Office of Intelligence and Analysis, Office of the General Counsel, Office of Policy, National Protection and Programs

The DHS Working Group publishes these best practices to inform DHS and our local, state, and federal government partners and grantees that want to establish unmanned aircraft programs based on policies and procedures that are respectful of privacy, civil rights, and civil liberties. These best practices are also consistent with the February 15, 2015 Presidential Memorandum: *Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*.<sup>5</sup>

Unmanned aircraft systems programs are encouraged to incorporate principles of transparency and accountability, while not revealing information that could reasonably be expected to compromise law enforcement or national security, and consider the issues that DHS has encountered in the context of developing its own policies and programs.

These best practices are not prescriptive, but rather are provided to share the Department's considerable experience operating unmanned aircraft systems in securing the Nation's borders and supporting communities during natural disasters and emergencies, and to provide unmanned aircraft system operators with privacy, civil rights, and civil liberties practices to consider before initiating an unmanned aircraft program. The applicability or advisability of implementing each recommended practice to a particular unmanned aircraft program will vary based upon each individual agency's legal authorities, purpose of the mission, mission of the agency, type of unmanned aircraft system, type of payload onboard, operating characteristics, and flight profiles. Therefore, each agency is encouraged to consult with its legal counsel to ensure compliance with its agency's own particular legal requirements

Although the intended audience is DHS and other government agencies, the private sector may also find these practices instructive in creating or operating unmanned aircraft programs.

It is important that agencies work closely with legal, privacy, civil rights, and civil liberties experts to ensure compliance with applicable local, state, and federal laws and regulations when developing an unmanned aircraft program.

---

Directorate, Science & Technology Directorate, Federal Emergency Management Agency and the Office of Operations Coordination and Planning.

<sup>5</sup> Presidential Memorandum, *Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* (2015). <http://wh.gov/ibmmj>.



## **Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Aircraft Systems Programs**

### **1. Consult Your Legal Counsel, Privacy, Civil Rights, and Civil Liberties Experts to Ensure Legal Authority and Compliance**

Prior to establishing an unmanned aircraft program, work closely with your legal counsel to confirm there is legal authority to operate unmanned aircraft systems for the intended purpose and whether it is permissible to fly unmanned aircraft in the desired area. Involve legal, privacy, civil rights, and civil liberties experts at every stage of formulation, operation, and review of an unmanned aircraft program to ensure compliance with applicable laws and policies.

### **2. Clearly State the Purpose of the Unmanned Aircraft Program**

Clearly articulate the primary purpose for establishing the unmanned aircraft systems program.

#### *Considerations:*

- The public may better understand and appreciate an agency's reasons for establishing an unmanned aircraft program with a clearly stated and plainly worded purpose.
- Identify the challenge that prompted your agency to create an unmanned aircraft program and how unmanned aircraft systems will assist in addressing that challenge.
- Determine the appropriate payload(s) (e.g., infrared camera, video, radar) for each stated purpose.
- Describe the primary purpose(s) of your unmanned aircraft program online and/or make this information publicly accessible, while not revealing information that could reasonably be expected to compromise law enforcement or national security.

### **3. Stay Focused on the Purpose of the Unmanned Aircraft Program**

Recognizing that the purpose and utility of a UAS program may evolve over time, certain changes to the unmanned aircraft program's stated purpose that may impact individual rights should be reviewed by an agency's legal, privacy, civil rights and civil liberties experts.

#### *Consideration:*

- Changes to the unmanned aircraft program's primary purposes should be reflected in documents readily available to the public prior to implementing those changes (if feasible).

### **4. Designate an Individual Responsible for Privacy, Civil Rights, and Civil Liberties Compliance**

This should be a senior level individual within the organization, preferably in the office(s) responsible for privacy, civil rights and civil liberties (if one exists), with working knowledge of the relevant privacy, civil rights, and civil liberties laws and regulations. The senior level individual should have a "direct line" to the person who has overall responsibility for the unmanned aircraft program.

### **5. Stay Involved from Conception Throughout Deployment and Thereafter**



Program managers, technical staff, and operations staff should consult with legal, privacy, civil rights, and civil liberties experts throughout the lifecycle of the unmanned aircraft program.

Considerations:

- Establish and make publicly available clear policies and procedures to ensure respect for privacy, civil rights, and civil liberties while also making it clear that some information may not be able to be made publicly available based upon other legal, investigative or operational security reasons.
- Unmanned aircraft program managers should consult with legal, privacy, civil rights, and civil liberties experts when formulating concepts of operations, standard operating procedures, agreements, procurement contracts, and other underlying unmanned aircraft system documents.
- Establish a routine program review process to assess whether the program's purpose is being met and whether modifications are required. For example, the Presidential Memorandum: *Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* requires federal agencies to perform such an assessment at least every three years and before new UAS programs are developed.

**6. Conduct a Privacy Impact Assessment and Document Privacy Compliance**

Agencies should conduct an analysis of potential privacy, civil rights, and civil liberties concerns before using unmanned aircraft systems. The Presidential Memorandum (referenced above) requires that Federal agencies examine their existing UAS policies and procedures relating to the collection, use, retention, and dissemination of information obtained by UAS at least every three years, to ensure that privacy, civil rights, and civil liberties are protected. Although not required for all agencies, DHS found it useful to use a Privacy Impact Assessment (PIA) format for its examination—similar to that required for federal government information technologies under the *E-Government Act of 2002*. Privacy assessments are beneficial in evaluating an agency's compliance with applicable legal, regulatory, and policy requirements. The decision as to when such an assessment is appropriate will be a contextual decision for agencies to make based on their expertise, and the facts and circumstances involved. Any privacy assessment should identify potential risks to privacy, as well as steps an agency will take to mitigate any potential privacy risks. DHS has also found the PIA format useful for public notification of its UAS activities. For more information on the PIA format used by DHS (and to consult DHS PIAs that cover both unmanned aircraft systems and the use of sensors by aircraft) please visit the DHS Privacy Office webpage, available at [http://www.dhs.gov/privacy-compliance\\_](http://www.dhs.gov/privacy-compliance_)

Considerations:

- Some agencies conduct a brief Privacy Threshold Analysis to determine whether any Personally Identifiable Information<sup>2</sup> is to be collected or whether an unmanned

---

<sup>2</sup> DHS defines "Personally Identifiable Information" as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.



aircraft program raises privacy sensitivities before initiating a Privacy Impact Assessment.

- Consult state, local, and tribal or territorial laws to decide if any public notice is required regarding the system used to store, use, or share information acquired through unmanned aircraft systems. Federal agencies should consult the Privacy Act of 1974, as it may be applicable.

## 7. Limit Collection, Use, Dissemination, and Retention of Unmanned Aircraft System-Recorded Data

Collection, use, dissemination, and retention of unmanned aircraft system-recorded data should be limited to data legally acquired and relevant to the entity's operations. *See Best Practice #3.*

### Considerations:

- Recorded images of individuals should not be retained beyond a reasonable period as defined by existing agency/departmental policy unless there is authorization based on a legal, policy or operational purpose.
- Collection, use, dissemination, or retention of unmanned aircraft system-recorded data should not be based solely on individual characteristics (e.g., race, ethnicity, national origin, sexual orientation, gender identity, religion, age, or gender), which is a violation of the law.
- The users of unmanned aircraft system-recorded data are responsible for ensuring dissemination of data is authorized and consistent with the recipients' legitimate need to know and authority to receive such data; any further dissemination by a data recipient should require the data owner's prior consent, which should only be provided upon the advice of the entity's legal counsel.
- Federal agencies need to establish whether their systems collect and store PII, and if so, whether there is an applicable System of Records Notice. Additionally, if their system does collect and store PII, agencies should consider whether they should limit the collection of personally identifiable information in accordance with OMB M 7-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.<sup>3</sup>
- Requests for unmanned aircraft system data by commercial entities, civil litigants, or Freedom of Information Act requesters should be reviewed by legal counsel to determine if such sharing is appropriate and permissible under applicable laws or regulations.
- Unmanned aircraft program managers should employ reasonable technological or administrative safeguards to ensure that images of people incidentally recorded who are not relevant to an operation are not disseminated or viewed unnecessarily to protect individual rights. This is especially important for recordings that include images of minors not relevant to an operation.
- Follow and clarify (if necessary) existing procedures for identifying, disseminating, retaining, indexing, and storing relevant and necessary unmanned aircraft system-recorded data in a retrievable manner.

---

<sup>3</sup> OMB M 7-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (2007). <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>



- Establish or comply with an approved records retention schedule that systematically eliminates stored data after they are no longer legally required or operationally useful. If not already present, this schedule should be periodically reviewed and updated. Ensure retention periods are compatible with the type of data retained and needs of the unmanned aircraft program. Data collected that does not pertain to an authorized purpose should not be retained beyond 180 days.

**8. Respect Constitutionally Protected Activities**

At times, government agencies may find it necessary to deploy unmanned aircraft systems to protect the public safety or respond to emergencies while other constitutionally protected activities may be taking place at the same location.

*Considerations:*

- Incidental images of identifiable individuals that are recorded, but not needed for legal compliance or law enforcement purposes, should be deleted according to established procedures and within 180 days.
- Be attuned to the potential privacy risks or legal ramifications arising from inadvertently capturing images of individuals engaging in constitutionally protected activities, and establish appropriate guidelines and administrative controls to anonymize, destroy, safeguard or prevent the misuse of such data, consistent with applicable law.
- Unmanned aircraft system-recorded data should not be collected, disseminated or retained solely for the purpose of monitoring activities protected by the U.S. Constitution, such as the First Amendment's protections of religion, speech, press, assembly, and redress of grievances (e.g., protests, demonstrations).

**9. Have a Redress Program for Individuals that Covers Unmanned Aircraft System Activities**

A robust and streamlined redress program is essential for permitting challenges to alleged inappropriate capture of personally identifiable information. Ensure that adequate procedures are in place to receive, investigate, and address, as appropriate, privacy, civil rights, and civil liberties complaints.

*Considerations:*

- Where an administrative process is used, the process for resolving complaints should promote resolution within a reasonable amount of time.
- When circumstances permit, and while not revealing information that could reasonably be expected to compromise law enforcement or national security, individuals should be provided information regarding the factual basis for redress determinations.
- Information on how an individual requests redress should be succinct, straightforward, and readily available to the public.

**10. Ensure Accountability in Management of Unmanned Aircraft Program**

Accountability is a key element to a successful unmanned aircraft program. A program that properly records access and use of unmanned aircraft system-recorded data is better prepared to identify and resolve problems, and is more responsive to the public and regulatory bodies.



Considerations:

- Establish or confirm that existing oversight procedures (including audits or assessments) ensure compliance with policies and regulations; this may also serve as another layer of security and improve the overall integrity of the program.
- Provide adequate supervision of personnel and a process for personnel to report suspected cases of misuse or abuse.
- Impose penalties for misuse and non-compliance with policies and procedures.
- Establish policies and procedures for documenting individuals accessing or requesting access to unmanned aircraft system-recorded data.
- Institute a schedule of regularly submitted reports to agency legal, privacy, civil rights, and civil liberties experts documenting all unmanned aircraft system activities and complaints received during the prior reporting period. Reports should be submitted at least annually.
- Determine whether there is a need for new data sharing agreements, and establish appropriate record management policies before sharing data with other agencies.

11. **Properly Secure and Store Unmanned Aircraft System-Recorded Data**

An unmanned aircraft program should be designed with appropriate security safeguards to prevent or mitigate data loss, unauthorized access, use and disclosure of data.

Considerations:

- Ensure access to unmanned aircraft system-recorded data is controlled by using appropriate physical, personnel or technical security measures as appropriate (e.g., digital watermarks, encryption, or other security and authentication techniques) to protect the data.
- Apply appropriate handling and safeguarding procedures to unmanned aircraft system-recorded data that may be linked to individuals, or to sensitive information that is not otherwise personally identifiable (e.g., sensitive government or business proprietary information).
- Ensure the unmanned aircraft program authenticates and establishes a chain-of-custody that preserves the integrity of all data stored in the event that the data are produced in litigation.
- Develop procedures to ensure the system and its stored data are used only as authorized.
- Security measures should be layered to avoid reliance on any single security measure; employ several measures that functionally overlap to create redundancy in the security of data and the overall program.
- Protect the physical security of the communication links, and operational and data storage centers.
- Individuals with access to unmanned aircraft systems should receive background checks in accordance with an agency's regulations.

12. **Review Agency Procurement Solicitations**

Agencies should consult their legal, privacy, civil rights, and civil liberties experts when reviewing unmanned aircraft system sensor technology procurement solicitations to determine if the technology impacts individual rights (e.g., capable of observing non-public activities).

Considerations:

- Work with unmanned aircraft system vendors, payload vendors, and field operators to ensure that only equipment capabilities needed to support a specified purpose are used.
- Prior to any acquisition, ensure that the prospective sensor aligns with and furthers the purpose of the unmanned aircraft program, while minimizing the potential risk upon use to privacy, civil rights, or civil liberties.

**13. Transparency and Outreach**

Public support is essential for an unmanned aircraft program's success. A program that is not transparent according to applicable laws, agency policies, and best practices may quickly lose support and create misperceptions about the program's intended mission(s).

Considerations:

- When organizing initial outreach efforts, consider using the best practices listed in this guide that are operationally and legally feasible for your agency as a starting point, and periodically engage the public to keep them informed about the program and proposed significant changes.
- Outreach efforts should consider how to include persons with limited English proficiency and persons with disabilities.
- When circumstances permit, and while not revealing information that could reasonably be expected to compromise law enforcement or national security, provide notice to the public as to where unmanned aircraft routinely operate (e.g., a description of the general operating area on websites, public documents, or through use of public signs).

**14. Train Personnel**

Require that personnel receive training regarding privacy and civil liberties policies that may apply to unmanned aircraft system operations. The agency's office(s) generally responsible for privacy, civil rights, and civil liberties should participate in developing and conducting the annual training.

Considerations:

- Individuals with access to stored data should receive training designed for the specific software and hardware employed by the agency's unmanned aircraft program.
- Those personnel responsible for handling unmanned aircraft systems support requests from other agencies should receive additional training on the agency's standard operating procedures for handling such requests.
- Staff should be instructed not to use any unmanned aircraft systems-acquired data for personal use.

**15. Develop Procedures to Handle Unmanned Aircraft Systems Support Requests**

The desirability and versatility of unmanned aircraft may prompt requests by outside organizations seeking unmanned aircraft systems support from an agency.



Considerations:

- Unmanned aircraft system assets used within the National Airspace System in support of an outside agency's request should only be operated by the agency authorized to operate unmanned aircraft by the Federal Aviation Administration.
- Establish and publish guidelines for agencies making unmanned aircraft systems support requests so that each requesting agency is aware of existing support limitations, and exactly what information they must provide to the unmanned aircraft systems operator.
- Ask sufficient questions of the requesting agency to ensure the scope and breadth of the request is understood so an appropriate payload and asset, which may be other than an unmanned aircraft (e.g., manned rotary- or fixed-wing aircraft), is provided to support the requesting agency.
- Agencies should create standard operating procedures for handling requests during both exigent and non-exigent circumstances.
- Standard operating procedures should (at a minimum) be reviewed by agency legal, privacy, civil rights, and civil liberties experts on an annual basis.
- It may be beneficial to have a memorandum of understanding or a similar written agreement that identifies each agency's roles and responsibilities in fulfilling a request. This agreement may include identifying which agency will exercise ownership, retention, and dissemination rights over any recorded data. It is best to create a template for support agreements that is then tailored to reflect each new request.
- If a request is received from other government agencies, there should be an understanding and respect for each agency's authorities and jurisdiction in fulfilling the request. If feasible, include an accounting of support requests received by, and responses from, the unmanned aircraft program (e.g., granted, denied, or asset other than an unmanned aircraft provided) when meeting periodic reporting requirements. *See Best Practice #10.*



**U.S. Department of Homeland Security**

**Best Practices for**

**Protecting Privacy, Civil Rights & Civil Liberties**

**In**

**Unmanned Aircraft Systems Programs**

**U.S. Department of Homeland Security**  
**Privacy, Civil Rights & Civil Liberties**  
**Unmanned Aircraft Systems Working Group**

**December 18, 2015**

## **Joint Statement**

### **Co-Chairs**

#### **Department of Homeland Security Privacy, Civil Rights & Civil Liberties Unmanned Aircraft Systems Working Group**

As co-chairs of the Department of Homeland Security's (DHS) Privacy, Civil Rights & Civil Liberties Unmanned Aircraft Systems Working Group (DHS Working Group), we are pleased to present these best practices, which reflect DHS' experiences in building unmanned aircraft system programs founded on strong privacy, civil rights, and civil liberties protections. Unmanned aircraft systems are an essential tool in DHS's border security mission and present a great deal of promise for assisting first responders and improving situational awareness.

These best practices represent an optimal approach to protecting individual rights that is influenced by U.S. Customs and Border Protection's (CBP) ten years of experience using unmanned aircraft systems as a tool in protecting and securing the Nation's borders. We are sharing these reflections broadly, recognizing that government entities (including CBP) have various limitations based upon their respective missions, operating characteristics, and legal authorities, and that many of the considerations that apply to our agency may not be applicable or appropriate for other entities. The DHS Working Group neither proposes nor intends that this document regulate any other government entity. Our goal, rather, is simply to share the best practices we have identified as helping to sustain privacy, civil rights, and civil liberties throughout the lifecycle of an unmanned aircraft systems program.<sup>1</sup>

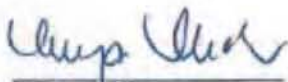
We provide these best practices to share DHS's view of how to protect individual rights in this evolving technology-driven field. The rapid changes in technology compel legal, privacy, and civil rights and civil liberties experts to continually review and update implementing documents (e.g., best practices, standard operating procedures, and policies) to properly reflect changes in the law, as well as advances in the technology and new applications of the technology. It is important for government entities to ensure that technology is not used in a manner that erodes or violates an individual's statutory or constitutional rights.

---

<sup>1</sup> This guidance is intended for first responders (e.g., emergency management, emergency medical service, fire departments, and security professionals responding to disasters and other emergencies), and does not seek to provide guidance in regard to investigative use of unmanned aircraft systems. DHS's primary experience with UAS operations, which serves as the basis for these best practices, has come in the context of general border surveillance operations.

Finally, even though these best practices are intended for DHS and our local, state, and federal government partners and grantees, the private sector may also find these recommendations valuable and instructive in creating their unmanned aircraft system programs.

Sincerely,



Megan H. Mack  
Officer for Civil Rights  
and Civil Liberties



Karen Neuman  
Chief Privacy Officer



Edward E. Young  
Deputy Assistant Commissioner  
U.S. Customs and Border Protection



# U.S. Department of Homeland Security

## Best Practices for

### Protecting Privacy, Civil Rights & Civil Liberties In Unmanned Aircraft Systems Programs

#### Overview

The term “unmanned aircraft systems” is used to define an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot or system operator in command to operate safely and efficiently in the national airspace system.<sup>1</sup> In the past, unmanned aircraft were referred to as “unmanned aerial vehicles,” but today they are simply referred to as unmanned aircraft.

Unmanned aircraft systems offer a variety of benefits for protecting our borders; supporting law enforcement; assisting in search and rescue operations; locating forest fire hot spots; evaluating dangerous environments (e.g., post-chemical spill and radiological exposure); conducting forensic imagery; inspecting pipeline and utilities; monitoring evacuation routes; and relaying telecommunication signals.<sup>2</sup>

The development of a new technology, significant improvement of a current technology, or the new application of an existing technology often results in concerns about the impact on individual privacy, civil rights, and civil liberties. For instance, the integration of government and commercial unmanned aircraft systems into the National Airspace System by 2015, as required by the *Federal Aviation Administration Modernization and Reform Act of 2012*, has prompted questions about how this might impact individual rights.<sup>3</sup>

In this regard, the Acting Officer for Civil Rights and Civil Liberties, the Acting Chief Privacy Officer, and the Assistant Commissioner for U.S. Customs and Border Protection, Office of Air and Marine jointly established the DHS *Unmanned Aircraft Systems Privacy, Civil Rights and Civil Liberties Working Group* (DHS Working Group) in September 2012 to “provide leadership to the homeland security enterprise by clarifying the privacy, civil rights, and civil liberties legal and policy issues surrounding government use of [Unmanned Aircraft Systems].”<sup>4</sup>

---

<sup>1</sup> *FAA Modernization and Reform Act of 2012*, Pub. L. No. 112-95.

<sup>2</sup> Government Accountability Office, *Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*, p. 10, GAO-12-981 (September 2012).

<sup>3</sup> *Id.* at 2-3, 32-36.

<sup>4</sup> *Memorandum for the Secretary, Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department's Use and Support of Unmanned Aerial Systems (UAS)*, from Tamara J. Kessler, Acting Officer, Office for Civil Rights and Civil Liberties; and Jonathan R. Cantor, Acting Chief Privacy Officer (September 12, 2012). The DHS *Unmanned Aircraft Systems Privacy, Civil Rights and Civil Liberties Working Group*, co-chaired by the DHS Office for Civil Rights & Civil Liberties, DHS Privacy Office and U.S. Customs and Border Protection, is comprised of policy and operational subject matter experts from across DHS including the U.S. Coast Guard, Office of Intelligence and Analysis, Office of the General Counsel, Office of Policy, National Protection and Programs



The DHS Working Group publishes these best practices to inform DHS and our local, state, and federal government partners and grantees that want to establish unmanned aircraft programs based on policies and procedures that are respectful of privacy, civil rights, and civil liberties. These best practices are also consistent with the February 15, 2015 Presidential Memorandum: *Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*.<sup>5</sup>

Unmanned aircraft systems programs are encouraged to incorporate principles of transparency and accountability, while not revealing information that could reasonably be expected to compromise law enforcement or national security, and consider the issues that DHS has encountered in the context of developing its own policies and programs.

These best practices are not prescriptive, but rather are provided to share the Department's considerable experience operating unmanned aircraft systems in securing the Nation's borders and supporting communities during natural disasters and emergencies, and to provide unmanned aircraft system operators with privacy, civil rights, and civil liberties practices to consider before initiating an unmanned aircraft program. The applicability or advisability of implementing each recommended practice to a particular unmanned aircraft program will vary based upon each individual agency's legal authorities, purpose of the mission, mission of the agency, type of unmanned aircraft system, type of payload onboard, operating characteristics, and flight profiles. Therefore, each agency is encouraged to consult with its legal counsel to ensure compliance with its agency's own particular legal requirements

Although the intended audience is DHS and other government agencies, the private sector may also find these practices instructive in creating or operating unmanned aircraft programs.

It is important that agencies work closely with legal, privacy, civil rights, and civil liberties experts to ensure compliance with applicable local, state, and federal laws and regulations when developing an unmanned aircraft program.

---

Directorate, Science & Technology Directorate, Federal Emergency Management Agency and the Office of Operations Coordination and Planning.

<sup>5</sup> Presidential Memorandum, *Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* (2015). <http://wh.gov/ibmmj>.

## **Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Aircraft Systems Programs**

### **1. Consult Your Legal Counsel, Privacy, Civil Rights, and Civil Liberties Experts to Ensure Legal Authority and Compliance**

Prior to establishing an unmanned aircraft program, work closely with your legal counsel to confirm there is legal authority to operate unmanned aircraft systems for the intended purpose and whether it is permissible to fly unmanned aircraft in the desired area. Involve legal, privacy, civil rights, and civil liberties experts at every stage of formulation, operation, and review of an unmanned aircraft program to ensure compliance with applicable laws and policies.

### **2. Clearly State the Purpose of the Unmanned Aircraft Program**

Clearly articulate the primary purpose for establishing the unmanned aircraft systems program.

#### *Considerations:*

- The public may better understand and appreciate an agency's reasons for establishing an unmanned aircraft program with a clearly stated and plainly worded purpose.
- Identify the challenge that prompted your agency to create an unmanned aircraft program and how unmanned aircraft systems will assist in addressing that challenge.
- Determine the appropriate payload(s) (e.g., infrared camera, video, radar) for each stated purpose.
- Describe the primary purpose(s) of your unmanned aircraft program online and/or make this information publicly accessible, while not revealing information that could reasonably be expected to compromise law enforcement or national security.

### **3. Stay Focused on the Purpose of the Unmanned Aircraft Program**

Recognizing that the purpose and utility of a UAS program may evolve over time, certain changes to the unmanned aircraft program's stated purpose that may impact individual rights should be reviewed by an agency's legal, privacy, civil rights and civil liberties experts.

#### *Consideration:*

- Changes to the unmanned aircraft program's primary purposes should be reflected in documents readily available to the public prior to implementing those changes (if feasible).

### **4. Designate an Individual Responsible for Privacy, Civil Rights, and Civil Liberties Compliance**

This should be a senior level individual within the organization, preferably in the office(s) responsible for privacy, civil rights and civil liberties (if one exists), with working knowledge of the relevant privacy, civil rights, and civil liberties laws and regulations. The senior level individual should have a "direct line" to the person who has overall responsibility for the unmanned aircraft program.

### **5. Stay Involved from Conception Throughout Deployment and Thereafter**



Program managers, technical staff, and operations staff should consult with legal, privacy, civil rights, and civil liberties experts throughout the lifecycle of the unmanned aircraft program.

Considerations:

- Establish and make publicly available clear policies and procedures to ensure respect for privacy, civil rights, and civil liberties while also making it clear that some information may not be able to be made publicly available based upon other legal, investigative or operational security reasons.
- Unmanned aircraft program managers should consult with legal, privacy, civil rights, and civil liberties experts when formulating concepts of operations, standard operating procedures, agreements, procurement contracts, and other underlying unmanned aircraft system documents.
- Establish a routine program review process to assess whether the program's purpose is being met and whether modifications are required. For example, the Presidential Memorandum: *Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* requires federal agencies to perform such an assessment at least every three years and before new UAS programs are developed.

**6. Conduct a Privacy Impact Assessment and Document Privacy Compliance**

Agencies should conduct an analysis of potential privacy, civil rights, and civil liberties concerns before using unmanned aircraft systems. The Presidential Memorandum (referenced above) requires that Federal agencies examine their existing UAS policies and procedures relating to the collection, use, retention, and dissemination of information obtained by UAS at least every three years, to ensure that privacy, civil rights, and civil liberties are protected. Although not required for all agencies, DHS found it useful to use a Privacy Impact Assessment (PIA) format for its examination—similar to that required for federal government information technologies under the *E-Government Act of 2002*. Privacy assessments are beneficial in evaluating an agency's compliance with applicable legal, regulatory, and policy requirements. The decision as to when such an assessment is appropriate will be a contextual decision for agencies to make based on their expertise, and the facts and circumstances involved. Any privacy assessment should identify potential risks to privacy, as well as steps an agency will take to mitigate any potential privacy risks. DHS has also found the PIA format useful for public notification of its UAS activities. For more information on the PIA format used by DHS (and to consult DHS PIAs that cover both unmanned aircraft systems and the use of sensors by aircraft) please visit the DHS Privacy Office webpage, available at [http://www.dhs.gov/privacy-compliance\\_](http://www.dhs.gov/privacy-compliance_)

Considerations:

- Some agencies conduct a brief Privacy Threshold Analysis to determine whether any Personally Identifiable Information<sup>2</sup> is to be collected or whether an unmanned

---

<sup>2</sup> DHS defines "Personally Identifiable Information" as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.



aircraft program raises privacy sensitivities before initiating a Privacy Impact Assessment.

- Consult state, local, and tribal or territorial laws to decide if any public notice is required regarding the system used to store, use, or share information acquired through unmanned aircraft systems. Federal agencies should consult the Privacy Act of 1974, as it may be applicable.

7. **Limit Collection, Use, Dissemination, and Retention of Unmanned Aircraft System-Recorded Data**

Collection, use, dissemination, and retention of unmanned aircraft system-recorded data should be limited to data legally acquired and relevant to the entity's operations. *See Best Practice #3.*

Considerations:

- Recorded images of individuals should not be retained beyond a reasonable period as defined by existing agency/departmental policy unless there is authorization based on a legal, policy or operational purpose.
- Collection, use, dissemination, or retention of unmanned aircraft system-recorded data should not be based solely on individual characteristics (e.g., race, ethnicity, national origin, sexual orientation, gender identity, religion, age, or gender), which is a violation of the law.
- The users of unmanned aircraft system-recorded data are responsible for ensuring dissemination of data is authorized and consistent with the recipients' legitimate need to know and authority to receive such data; any further dissemination by a data recipient should require the data owner's prior consent, which should only be provided upon the advice of the entity's legal counsel.
- Federal agencies need to establish whether their systems collect and store PII, and if so, whether there is an applicable System of Records Notice. Additionally, if their system does collect and store PII, agencies should consider whether they should limit the collection of personally identifiable information in accordance with OMB M 7-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.<sup>3</sup>
- Requests for unmanned aircraft system data by commercial entities, civil litigants, or Freedom of Information Act requesters should be reviewed by legal counsel to determine if such sharing is appropriate and permissible under applicable laws or regulations.
- Unmanned aircraft program managers should employ reasonable technological or administrative safeguards to ensure that images of people incidentally recorded who are not relevant to an operation are not disseminated or viewed unnecessarily to protect individual rights. This is especially important for recordings that include images of minors not relevant to an operation.
- Follow and clarify (if necessary) existing procedures for identifying, disseminating, retaining, indexing, and storing relevant and necessary unmanned aircraft system-recorded data in a retrievable manner.

---

<sup>3</sup> OMB M 7-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (2007). <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>



- Establish or comply with an approved records retention schedule that systematically eliminates stored data after they are no longer legally required or operationally useful. If not already present, this schedule should be periodically reviewed and updated. Ensure retention periods are compatible with the type of data retained and needs of the unmanned aircraft program. Data collected that does not pertain to an authorized purpose should not be retained beyond 180 days.

#### 8. **Respect Constitutionally Protected Activities**

At times, government agencies may find it necessary to deploy unmanned aircraft systems to protect the public safety or respond to emergencies while other constitutionally protected activities may be taking place at the same location.

##### *Considerations:*

- Incidental images of identifiable individuals that are recorded, but not needed for legal compliance or law enforcement purposes, should be deleted according to established procedures and within 180 days.
- Be attuned to the potential privacy risks or legal ramifications arising from inadvertently capturing images of individuals engaging in constitutionally protected activities, and establish appropriate guidelines and administrative controls to anonymize, destroy, safeguard or prevent the misuse of such data, consistent with applicable law.
- Unmanned aircraft system-recorded data should not be collected, disseminated or retained solely for the purpose of monitoring activities protected by the U.S. Constitution, such as the First Amendment's protections of religion, speech, press, assembly, and redress of grievances (e.g., protests, demonstrations).

#### 9. **Have a Redress Program for Individuals that Covers Unmanned Aircraft System Activities**

A robust and streamlined redress program is essential for permitting challenges to alleged inappropriate capture of personally identifiable information. Ensure that adequate procedures are in place to receive, investigate, and address, as appropriate, privacy, civil rights, and civil liberties complaints.

##### *Considerations:*

- Where an administrative process is used, the process for resolving complaints should promote resolution within a reasonable amount of time.
- When circumstances permit, and while not revealing information that could reasonably be expected to compromise law enforcement or national security, individuals should be provided information regarding the factual basis for redress determinations.
- Information on how an individual requests redress should be succinct, straightforward, and readily available to the public.

#### 10. **Ensure Accountability in Management of Unmanned Aircraft Program**

Accountability is a key element to a successful unmanned aircraft program. A program that properly records access and use of unmanned aircraft system-recorded data is better prepared to identify and resolve problems, and is more responsive to the public and regulatory bodies.



Considerations:

- Establish or confirm that existing oversight procedures (including audits or assessments) ensure compliance with policies and regulations; this may also serve as another layer of security and improve the overall integrity of the program.
- Provide adequate supervision of personnel and a process for personnel to report suspected cases of misuse or abuse.
- Impose penalties for misuse and non-compliance with policies and procedures.
- Establish policies and procedures for documenting individuals accessing or requesting access to unmanned aircraft system-recorded data.
- Institute a schedule of regularly submitted reports to agency legal, privacy, civil rights, and civil liberties experts documenting all unmanned aircraft system activities and complaints received during the prior reporting period. Reports should be submitted at least annually.
- Determine whether there is a need for new data sharing agreements, and establish appropriate record management policies before sharing data with other agencies.

11. **Properly Secure and Store Unmanned Aircraft System-Recorded Data**

An unmanned aircraft program should be designed with appropriate security safeguards to prevent or mitigate data loss, unauthorized access, use and disclosure of data.

Considerations:

- Ensure access to unmanned aircraft system-recorded data is controlled by using appropriate physical, personnel or technical security measures as appropriate (e.g., digital watermarks, encryption, or other security and authentication techniques) to protect the data.
- Apply appropriate handling and safeguarding procedures to unmanned aircraft system-recorded data that may be linked to individuals, or to sensitive information that is not otherwise personally identifiable (e.g., sensitive government or business proprietary information).
- Ensure the unmanned aircraft program authenticates and establishes a chain-of-custody that preserves the integrity of all data stored in the event that the data are produced in litigation.
- Develop procedures to ensure the system and its stored data are used only as authorized.
- Security measures should be layered to avoid reliance on any single security measure; employ several measures that functionally overlap to create redundancy in the security of data and the overall program.
- Protect the physical security of the communication links, and operational and data storage centers.
- Individuals with access to unmanned aircraft systems should receive background checks in accordance with an agency's regulations.

12. **Review Agency Procurement Solicitations**

Agencies should consult their legal, privacy, civil rights, and civil liberties experts when reviewing unmanned aircraft system sensor technology procurement solicitations to determine if the technology impacts individual rights (e.g., capable of observing non-public activities).

Considerations:

- Work with unmanned aircraft system vendors, payload vendors, and field operators to ensure that only equipment capabilities needed to support a specified purpose are used.
- Prior to any acquisition, ensure that the prospective sensor aligns with and furthers the purpose of the unmanned aircraft program, while minimizing the potential risk upon use to privacy, civil rights, or civil liberties.

**13. Transparency and Outreach**

Public support is essential for an unmanned aircraft program's success. A program that is not transparent according to applicable laws, agency policies, and best practices may quickly lose support and create misperceptions about the program's intended mission(s).

Considerations:

- When organizing initial outreach efforts, consider using the best practices listed in this guide that are operationally and legally feasible for your agency as a starting point, and periodically engage the public to keep them informed about the program and proposed significant changes.
- Outreach efforts should consider how to include persons with limited English proficiency and persons with disabilities.
- When circumstances permit, and while not revealing information that could reasonably be expected to compromise law enforcement or national security, provide notice to the public as to where unmanned aircraft routinely operate (e.g., a description of the general operating area on websites, public documents, or through use of public signs).

**14. Train Personnel**

Require that personnel receive training regarding privacy and civil liberties policies that may apply to unmanned aircraft system operations. The agency's office(s) generally responsible for privacy, civil rights, and civil liberties should participate in developing and conducting the annual training.

Considerations:

- Individuals with access to stored data should receive training designed for the specific software and hardware employed by the agency's unmanned aircraft program.
- Those personnel responsible for handling unmanned aircraft systems support requests from other agencies should receive additional training on the agency's standard operating procedures for handling such requests.
- Staff should be instructed not to use any unmanned aircraft systems-acquired data for personal use.

**15. Develop Procedures to Handle Unmanned Aircraft Systems Support Requests**

The desirability and versatility of unmanned aircraft may prompt requests by outside organizations seeking unmanned aircraft systems support from an agency.



Considerations:

- Unmanned aircraft system assets used within the National Airspace System in support of an outside agency's request should only be operated by the agency authorized to operate unmanned aircraft by the Federal Aviation Administration.
- Establish and publish guidelines for agencies making unmanned aircraft systems support requests so that each requesting agency is aware of existing support limitations, and exactly what information they must provide to the unmanned aircraft systems operator.
- Ask sufficient questions of the requesting agency to ensure the scope and breadth of the request is understood so an appropriate payload and asset, which may be other than an unmanned aircraft (e.g., manned rotary- or fixed-wing aircraft), is provided to support the requesting agency.
- Agencies should create standard operating procedures for handling requests during both exigent and non-exigent circumstances.
- Standard operating procedures should (at a minimum) be reviewed by agency legal, privacy, civil rights, and civil liberties experts on an annual basis.
- It may be beneficial to have a memorandum of understanding or a similar written agreement that identifies each agency's roles and responsibilities in fulfilling a request. This agreement may include identifying which agency will exercise ownership, retention, and dissemination rights over any recorded data. It is best to create a template for support agreements that is then tailored to reflect each new request.
- If a request is received from other government agencies, there should be an understanding and respect for each agency's authorities and jurisdiction in fulfilling the request. If feasible, include an accounting of support requests received by, and responses from, the unmanned aircraft program (e.g., granted, denied, or asset other than an unmanned aircraft provided) when meeting periodic reporting requirements. *See Best Practice #10.*





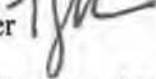
Homeland  
Security

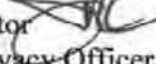
September 14, 2012

INFORMATION

MEMORANDUM FOR THE SECRETARY

FROM:

Tamara J. Kessler   
Acting Officer  
Office for Civil Rights and Civil Liberties

Jonathan R. Cantor   
Acting Chief Privacy Officer

SUBJECT:

Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department's Use and Support of Unmanned Aerial Systems (UAS)

Purpose

The Office for Civil Rights and Civil Liberties (CRCL) and the Privacy Office (PRIV) would like to assist DHS to provide leadership to the homeland security enterprise by clarifying the privacy, civil rights, and civil liberties (P/CRCL) legal and policy issues surrounding government use of UASs. To accomplish this goal, we plan to establish a Department-wide working group, led by CRCL, PRIV and Customs and Border Protection (CBP). As the use of UASs by federal, state, and local entities expands, DHS will have an increasingly public-facing role; establishing a group on this issue would signal that DHS recognizes the importance of protecting privacy, civil rights, and civil liberties in the use of UASs. The working group will serve to support all DHS mission areas and, in particular, PRIV and CRCL's mandate to ensure that privacy, civil rights, and civil liberties are not diminished by efforts, activities, and programs aimed at securing the homeland.

Background

This issue has attracted significant attention from Congress and the media, including technology-focused media. Earlier this year Congress required the Federal Aviation Administration (FAA) to speed up the process by which it authorizes government agencies to operate UASs, relax requirements for state and local agency use of UASs, and mandated regulations for testing and

~~DELIBERATIVE PROCESS PRIVILEGE // PRE-DECISIONAL // FOR OFFICIAL USE ONLY~~

licensing of private and commercial UASs. These actions have led to expressions of concern by the public and stakeholders regarding the P/CRCL implications of UAS use.

A working group chaired by CRCL, PRIV, and CBP presents a unique opportunity to clarify any misunderstandings that exist regarding DHS's UAS program and to mitigate and address any outstanding P/CRCL concerns with DHS programs. We think that the working group will serve a similar purpose with respect to the UAS Joint Program Office. It will demonstrate that DHS intends to take a proactive leadership role in ensuring that privacy, civil rights, and civil liberties are safeguarded by the lawful use of UASs by DHS components and grant recipients.

### Discussion

CRCL and PRIV are aware of three current uses of UASs to support DHS's mission:

- 1.
- 2.
- 3.



We do not believe that DHS has any other active UAS programs, but realize that there may be additional proposals for the use of UASs by the Department over time. Therefore, we think that a working group should examine all active and planned DHS uses of UASs, as well as DHS support to state and local partners in their use of UASs.

The overarching goal of the working group is to determine what policies and procedures are needed to ensure that protections for privacy, civil rights, and civil liberties are designed into DHS and DHS-funded UAS programs while fully supporting the appropriate use of UASs to achieve homeland security enterprise mission objectives. Working group participants will include representatives from CRCL, PRIV, OGC, each component that either uses or plans to use UASs, and other relevant parties from within DHS. CBP, the Coast Guard, S&T, IGA, MGMT, PLCY, OPA, OLA, and OGC have all concurred with this plan. The working group will have four objectives:

1. Establish a forum for DHS headquarters and components to discuss P/CRCL issues related to the Department's use and support of UASs;
2. Ensure that P/CRCL guidance and policies are reflected within the different CONOPS for UAS uses by the Department;
3. Identify potential privacy, civil rights, and civil liberties concerns with respect to the various current or planned uses of UASs by the Department; and
4. Promote DHS best practices for safeguarding privacy, civil rights, and civil liberties in the use of UASs by DHS partners and grant recipients.

cc:

Jane Holl Lute  
Deputy Secretary

Ivan Fong  
General Counsel

David V. Aguilar  
Acting Commissioner  
U.S. Customs and Border Protection

General Michael C. Kostelnik  
Assistant Commissioner  
CBP Office of Air and Marine

Admiral Robert J. Papp  
Commandant  
U.S. Coast Guard

Dr. Tara O'Toole  
Under Secretary  
Science and Technology

~~DELIBERATIVE PROCESS PRIVILEGE // PRE-DECISIONAL // FOR OFFICIAL USE ONLY~~

3





**U.S. Department of Homeland Security**

**Status Report  
As Directed in the**

**Presidential Memorandum:  
*Promoting Economic Competitiveness While Safeguarding  
Privacy, Civil Rights, and Civil Liberties in Domestic Use of  
Unmanned Aircraft Systems (February 15, 2015)***

**Submitted by:**

**Office for Civil Rights and Civil Liberties**

**Privacy Office**

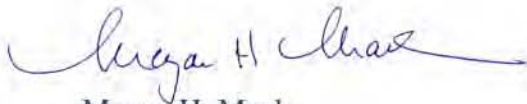
**August 6, 2015**



FOR OFFICIAL USE ONLY

## Forward

The U.S. Department of Homeland Security (DHS) Office for Civil Rights and Civil Liberties (CRCL) and the DHS Privacy Office (Privacy Office) are pleased to provide this status report on its implementation of privacy, civil rights, and civil liberties protections in the collection, use, retention, and dissemination of information captured by unmanned aircraft systems, as required by Section 1(e) of the Presidential Memorandum, *Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (February 15, 2015)* (Presidential Memorandum).



Megan H. Mack  
Officer  
Office for Civil Rights and Civil Liberties



Karen Neuman  
Chief Privacy Officer  
Privacy Office

FOR OFFICIAL USE ONLY

## Presidential Memorandum

### Section 1 Language

Section 1 sets forth the following requirements for unmanned aircraft systems (UAS):

*UAS Policies and Procedures for Federal Government Use. The Federal Government currently operates UAS in the United States for several purposes, including to manage Federal lands, monitor wildfires, conduct scientific research, monitor our borders, support law enforcement, and effectively train our military. As with information collected by the Federal Government using any technology, where UAS is the platform for collection, information must be collected, used, retained, and disseminated consistent with the Constitution, Federal law, and other applicable regulations and policies. Agencies must, for example, comply with the Privacy Act of 1974 (5 U.S.C. 552a) (the "Privacy Act"), which, among other things, restricts the collection and dissemination of individuals' information that is maintained in systems of records, including personally identifiable information (PII), and permits individuals to seek access to and amendment of records.*

*(a) Privacy Protections Particularly in light of the diverse potential uses of UAS in the NAS [National Airspace System], expected advancements in UAS technologies, and the anticipated increase in UAS use in the future, the Federal Government shall take steps to ensure that privacy protections and policies relative to UAS continue to keep pace with these developments. Accordingly, agencies shall, prior to deployment of new UAS technology and at least every 3 years, examine their existing UAS policies and procedures relating to the collection, use, retention, and dissemination of information obtained by UAS, to ensure that privacy, civil rights, and civil liberties are protected. Agencies shall update their policies and procedures, or issue new policies and procedures, as necessary. In addition to requiring compliance with the Privacy Act in applicable circumstances, agencies that collect information through UAS in the NAS shall ensure that their policies and procedures with respect to such information incorporate the following requirements:*

*(i) Collection and Use. Agencies shall only collect information using UAS, or use UAS-collected information, to the extent that such collection or use is consistent with and relevant to an authorized purpose.*

*(ii) Retention. Information collected using UAS that may contain PII shall not be retained for more than 180 days unless retention of the information is determined to be necessary to an authorized mission of the retaining agency, is maintained in a system of records covered by the Privacy Act, or is required to be retained for a longer period by any other applicable law or regulation.*

*(iii) Dissemination. UAS-collected information that is not maintained in a system of records covered by the Privacy Act shall not be disseminated outside of the agency unless dissemination is required by law, or fulfills an authorized purpose and complies with agency requirements.*

*(b) Civil Rights and Civil Liberties Protections. To protect civil rights and civil liberties, agencies shall:*



## FOR OFFICIAL USE ONLY

- (i) ensure that policies are in place to prohibit the collection, use, retention, or dissemination of data in any manner that would violate the First Amendment or in any manner that would discriminate against persons based upon their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity, in violation of law;*
- (ii) ensure that UAS activities are performed in a manner consistent with the Constitution and applicable laws, Executive Orders, and other Presidential directives; and*
- (iii) ensure that adequate procedures are in place to receive, investigate, and address, as appropriate, privacy, civil rights, and civil liberties complaints.*

*(c) Accountability. To provide for effective oversight, agencies shall:*

- (i) ensure that oversight procedures for agencies' UAS use, including audits or assessments, comply with existing agency policies and regulations;*
- (ii) verify the existence of rules of conduct and training for Federal Government personnel and contractors who work on UAS programs, and procedures for reporting suspected cases of misuse or abuse of UAS technologies;*
- (iii) establish policies and procedures, or confirm that policies and procedures are in place, that provide meaningful oversight of individuals who have access to sensitive information (including any PII) collected using UAS;*
- (iv) ensure that any data-sharing agreements or policies, data use policies, and record management policies applicable to UAS conform to applicable laws, regulations, and policies;*
- (v) establish policies and procedures, or confirm that policies and procedures are in place, to authorize the use of UAS in response to a request for UAS assistance in support of Federal, State, local, tribal, or territorial government operations; and*
- (vi) require that State, local, tribal, and territorial government recipients of Federal grant funding for the purchase or use of UAS for their own operations have in place policies and procedures to safeguard individuals' privacy, civil rights, and civil liberties prior to expending such funds.*

*(d) Transparency. To promote transparency about their UAS activities within the NAS, agencies that use UAS shall, while not revealing information that could reasonably be expected to compromise law enforcement or national security:*

- (i) provide notice to the public regarding where the agency's UAS are authorized to operate in the NAS;*
- (ii) keep the public informed about the agency's UAS program as well as changes that would significantly affect privacy, civil rights, or civil liberties; and*
- (iii) make available to the public, on an annual basis, a general summary of the agency's UAS operations during the previous fiscal year, to include a brief description of types or categories of missions flown, and the number of times the agency provided assistance to other agencies, or to State, local, tribal, or territorial governments.*

*(e) Reports. Within 180 days of the date of this memorandum, agencies shall provide the President with a status report on the implementation of this section. Within 1 year of the date of this memorandum, agencies shall publish information on how to access their publicly available policies and procedures implementing this section.*



FOR OFFICIAL USE ONLY

## Background

### *U.S. Customs and Border Protection's Use of Unmanned Aircraft Systems*

DHS's U.S. Customs and Border Protection (CBP), Office of Air and Marine, is the only component in the Department with an operational unmanned aircraft system (UAS) program.<sup>1</sup> With a decade of experience operating UAS, CBP has established policies and procedures concerning proper data use, minimization, retention, data quality and integrity, and data security, as well as a decision-making process for determining when it is appropriate to use a DHS UAS in support of other requesting agencies.

CBP is responsible for protecting nearly 7,000 miles of land border the United States shares with Canada and Mexico and 2,000 miles of coastal waters surrounding the Florida peninsula and off the coast of Southern California. The agency also protects 95,000 miles of maritime border in partnership with the United States Coast Guard (USCG). To achieve these missions, CBP employs several types of aircraft, including manned helicopters and manned fixed-wing aircraft. These aircraft assist CBP in patrolling the border. Surveillance aircraft may be used to: (1) patrol the border; (2) conduct surveillance for investigative operations; (3) conduct damage assessment and consequence management in disaster situations; and (4) respond to emergencies. Although infrequent, CBP also flies its unmanned aircraft in response to disaster situations as they are equipped with (b)(7)(E) unmanned aircraft can also map critical infrastructure before and after hurricanes, which allows the Federal Emergency Management Agency (FEMA) to track storm damage and note changes to the topography.

CBP owns and operates (b)(7)(E) that allow it to conduct missions in areas that are remote, too rugged for ground access, or otherwise considered too high-risk for manned aircraft or ground personnel. The aircraft are stationed and principally controlled at (b)(7)(E)

(b)(7)(E)

CBP's UAS operate in the National Airspace in accordance with Federal Aviation Administration (FAA) regulations and within designated special use airspace as published and/or authorized through the FAA Certificate of Authorization process.

In order to collect data and to assist the pilot during take-off and landing, (b)(7)(E)

(b)(7)(E)

<sup>1</sup> Although CBP, Office of Air and Marine, is the focus of this Status Report, other DHS entities, such as the Science and Technology Directorate, U.S. Border Patrol, U.S. Coast Guard, and U.S. Secret Service are involved in testing UAS capabilities or countermeasures.



FOR OFFICIAL USE ONLY

CBP conducts its UAS missions at altitudes (b)(7)(E)

(b)(7)(E)

### *DHS Privacy Office and Office for Civil Rights and Civil Liberties*

The Homeland Security Act of 2002, Section 222, provides the Chief Privacy Officer with primary responsibility for assuring that “the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information.” Based on this authority, in June, 2010, the Privacy Office requested CBP complete a Privacy Threshold Analysis on its use of aerial surveillance systems, including UAS.

Following submission of the Privacy Threshold Analysis, and in consultation with CBP, the Privacy Office determined that CBP’s use of sensors onboard its aircraft—manned and unmanned—could implicate the privacy of persons with whom CBP encounters. With CBP’s agreement, the Privacy Office directed CBP to prepare a Privacy Impact Assessment of all aircraft sensors. This Aircraft Systems Privacy Impact Assessment (September 9, 2013) and may be found at <http://www.dhs.gov/publication/dhscbppia-018-aircraft-systems>. Consistent with DHS policy, the Aircraft Systems Privacy Impact Assessment will be reviewed every three (3) years and updated as necessary. However, if CBP employs new, different, or updated technologies, or if operating environments change, or the Federal Government or DHS create new policies before three years have passed, CBP and the Privacy Office will update and amend the Privacy Impact Assessment to reflect these changes.

Although individuals cannot participate in the initial decision by CBP to collect information on them, they may contest or seek redress through any resulting proceedings brought against them by contacting CBP, CRCL, and/or the Privacy Office.

### *DHS Unmanned Aircraft Systems Privacy, Civil Rights, and Civil Liberties Working Group*

In recognizing the increased public and congressional concern over the government’s use of UAS, CRCL and the Privacy Office jointly established a Department-wide working group in September 2012.

The *DHS Unmanned Aircraft Systems Privacy, Civil Rights, and Civil Liberties Working Group* (the Unmanned Aircraft Systems Working Group), chaired by CRCL, Privacy, and CBP’s Office of Air and Marine (OAM) is responsible for “provid[ing] leadership to the homeland security enterprise by clarifying the privacy, civil rights, and civil liberties legal and policy issues surrounding government use of unmanned aircraft systems.”<sup>2</sup> The goal for this body is to serve

<sup>2</sup> *Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department’s Use and Support of Unmanned Aerial Systems (UAS), Memorandum for the Secretary*, from Tamara J. Kessler, Acting Officer, Office for Civil Rights and Civil Liberties; and Jonathan R. Cantor, Acting Chief Privacy Officer (*Working Group Memo*)

**FOR OFFICIAL USE ONLY**

as a collaborative forum for components and offices to identify, discuss, and address unmanned aircraft system issues potentially impacting privacy, civil rights, and civil liberties.

---

(September 12, 2012). [Http://www.dhs.gov/sites/default/files/publications/foia/working-group-to-safeguard-privacy-civil-rights-and-civil-liberties-in-the-departments-use-and-support-of-unmanned-aerial-systems-uas-sl-information-memorandum-09142012.pdf](http://www.dhs.gov/sites/default/files/publications/foia/working-group-to-safeguard-privacy-civil-rights-and-civil-liberties-in-the-departments-use-and-support-of-unmanned-aerial-systems-uas-sl-information-memorandum-09142012.pdf).



FOR OFFICIAL USE ONLY

## DHS Status Report on Section 1 Implementation

- I. Privacy Protections (Section 1(a)(i-iii)):** *In addition to requiring compliance with the Privacy Act in applicable circumstances, agencies that collect information through UAS in the NAS shall ensure that their policies and procedures with respect to such information incorporate the following requirements:*

*(i) Collection and Use. Agencies shall only collect information using UAS, or use UAS-collected information, to the extent that such collection or use is consistent with and relevant to an authorized purpose.*

*(ii) Retention. Information collected using UAS that may contain PII shall not be retained for more than 180 days unless retention of the information is determined to be necessary to an authorized mission of the retaining agency, is maintained in a system of records covered by the Privacy Act, or is required to be retained for a longer period by any other applicable law or regulation.*

*(iii) Dissemination. UAS-collected information that is not maintained in a system of records covered by the Privacy Act shall not be disseminated outside of the agency unless dissemination is required by law, or fulfills an authorized purpose and complies with agency requirements.*

### Status:

#### Privacy Protections:

**Collection and Use (Section 1(a)(i)):** *Agencies shall only collect information using UAS, or use UAS-collected information, to the extent that such collection or use is consistent with and relevant to an authorized purpose.*

CBP's UAS only collect video and/or radar images pursuant to its law enforcement authority, as part of its border security mission, or when flying a mission in support of another agency when that other agency's authority covers the mission either through delegation of authority or direct control of the information collected. CBP has a broad mandate to determine the admissibility of persons and to ensure goods brought into the country comply with United States law.<sup>3</sup>

CBP's OAM is authorized under current and past appropriations to provide UAS support to other Federal, State, and local agencies. Reflecting similar language in past appropriations, in 2015 Congress directed OAM to use appropriated funds, in part,

<sup>3</sup> 8 USC §§ 1225, 1357, other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1595a(d), and other pertinent provisions of customs laws and regulations.



## FOR OFFICIAL USE ONLY

[f]or . . . necessary expenses for the operations, maintenance, and procurement of marine vessels, aircraft, unmanned aircraft systems, the Air and Marine Operations Center, and other related equipment of the air and marine program . . . the operations of which include the following: the interdiction of narcotics and other goods; the provision of support to Federal, State, and local agencies in the enforcement or administration of laws enforced by the Department of Homeland Security; and, at the discretion of the Secretary of Homeland Security, the provision of assistance to Federal, State, and local agencies in other law enforcement and emergency humanitarian efforts.<sup>4</sup>

Together, these authorities allow CBP to obtain information in support of border interdiction of narcotics and other contraband, the prevention of the illegal entry of aliens into the United States, the security of airspace for high-risk areas or National Special Security Events, and in support of Federal, State, and local law enforcement, counterterrorism, and emergency humanitarian efforts.

CBP may use video, still images, and/or radar images, obtained from aircraft, to apprehend individuals and to provide evidence of an illegal border crossing or other violation of law. Consistent with applicable laws and System of Record Notices, the information may be shared with other State, local, Federal, tribal, and foreign law enforcement agencies in furtherance of enforcement of their laws.<sup>5</sup>

Although CBP's use of UAS is not limited to areas along the border, CBP is currently limited to operations consistent with Federal law and is limited by Certificates of Authorization and internally by CBP's own policies and procedures. In response to exigent circumstances, UAS may be used outside existing Certificates of Authorization, with authorization by the FAA, to assist in natural disasters and in support of State, local, and other Federal law enforcement operations. CBP's UAS are always operated by CBP FAA-certified pilots and CBP-contracted FAA-certified pilots. In a joint program with the USCG, some USCG pilots and sensor operators serve as crewmembers in the operation of CBP UAS. In addition, the FAA has granted CBP Certificates of Authorization to ferry UAS between the different operational areas and airfields. Should the FAA change the requirement for Certificates of Authorization, CBP will operate its UAS in accordance with the same policies and procedures that apply to CBP manned aircraft.

CBP's 2013 Privacy Impact Assessment on Aircraft Systems found that it remained true to its mission when using UAS. While the information obtained by UAS sensors alone are insufficient to identify a person, the images or information may be associated with an individual from context within the image, circumstances surrounding the activity occurring in the image, or additional information obtained directly from the person by an officer or agent. Importantly, images or information are only associated with an individual if the individual is apprehended or if the images are taken as part of an ongoing law enforcement investigation.

<sup>4</sup> *Department of Homeland Security Appropriations Act, 2015*, Public Law 114-4, 129 STAT. 39, 42.

<sup>5</sup> *Id.*



## FOR OFFICIAL USE ONLY

There are also internal controls in place to ensure UAS are not used for unauthorized purposes. Any changes or expansion to the program that might impact individual rights will be reviewed by CRCL and the Privacy Office in close consultation with CBP's operations personnel and component privacy personnel.

**Retention** (Section 1(a)(ii)). *Information collected using UAS that may contain PII shall not be retained for more than 180 days unless retention of the information is determined to be necessary to an authorized mission of the retaining agency, is maintained in a system of records covered by the Privacy Act, or is required to be retained for a longer period by any other applicable law or regulation.*

CBP seeks to minimize the collection and retention of video and radar to that which is necessary and relevant to carry out CBP's mission. Accordingly, when aircraft are flown to patrol the border, they are authorized to fly within the designated border surveillance mission area to ensure they are only capturing images and information necessary to detect, identify, apprehend, and remove persons and their possessions illegally entering the United States at and between Ports of Entry.

When aircraft are flown for investigative operations, officer safety incidents, or natural disasters, CBP approves and defines the specific mission that is authorized and works with the FAA to construct a Certificate of Authority to establish airspace for that specific operation. Video not associated with a case (b)(7)(E)

(b)(7)(E)

Live video captured by the (b)(7)(E) on UAS is transmitted through the DHS firewall to (b)(7)(E)

(b)(7)(E)

If an individual is apprehended by CBP as a result of observation by aircraft or subsequent association from the presence of CBP assets, CBP may have video of that individual's apprehension associated with his or her enforcement case file. That video is retained according to the retention schedule of the System of Records Notice of the corresponding case management system.



FOR OFFICIAL USE ONLY

Video and radar images obtained from UAS border patrols are also provided to (b)(7)(E)

(b)(7)(E)

Therefore, video not associated with a case remains on the digital video recorder until it is

(b)(7)(E)

**Dissemination** (Section 1(a)(iii)). *UAS-collected information that is not maintained in a system of records covered by the Privacy Act shall not be disseminated outside of the agency unless dissemination is required by law, or fulfills an authorized purpose and complies with agency requirements.*

The data collected by DHS's UAS is not subject to the Privacy Act unless it is retrieved by using an individual's name or other unique identifier. As stated above, data collected that are not associated with a case reside on a digital video recorder until it is over-written by new data, after (b)(7)(E) consequently this unassociated data is not maintained in a system of records. However, persons who are apprehended and who were recorded by an unmanned aircraft may have video of their crossing and/or apprehension associated with a case file that contains their personally identifiable information.

CBP has procedures and processes in place for sharing any data collected by aircraft, including when that information becomes associated with a case and is used as evidence against an apprehended individual. In addition, all requests for aerial surveillance for intelligence gathering purposes must receive prior approval by the Executive Director or Deputy of CBP National Air Security Operations, before the air asset can conduct the flight. Similarly, requests for analytical products incorporating historical analysis of the border topography must also be approved by the Executive Director or Deputy of CBP National Air Security Operations.

Once the images or videos are cross-referenced with, and included within records relating to an ongoing investigation or case, they become covered by the system of records for that particular case file system and subject to the Privacy Act requirements of that system.

**II. Civil Rights and Civil Liberties Protections** (Section 1(b)(i-iii)). *To protect civil rights and civil liberties, agencies shall:*

*(i) ensure that policies are in place to prohibit the collection, use, retention, or dissemination of data in any manner that would violate the First Amendment or in any manner that would discriminate against persons based upon their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity, in violation of law;*



## FOR OFFICIAL USE ONLY

*(ii) ensure that UAS activities are performed in a manner consistent with the Constitution and applicable laws, Executive Orders, and other Presidential directives; and*

*(iii) ensure that adequate procedures are in place to receive, investigate, and address, as appropriate, privacy, civil rights, and civil liberties complaints.*

**Status:**

*(i) ensure that policies are in place to prohibit the collection, use, retention, or dissemination of data in any manner that would violate the First Amendment or in any manner that would discriminate against persons based upon their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity, in violation of law;*

CBP's UAS, pursuant to the Certificate of Authorization approved by the FAA, operate primarily at an altitude (b)(7)(E) from that height. CBP's Certificates of Authorization also place limits on its UAS operations, such as from flying over major cities.

The UAS do not physically intrude upon or interfere with the use of private property. The cameras on the UAS are not intended, nor do they have the capability, (b)(7)(E)

(b)(7)(E)

*(ii) ensure that UAS activities are performed in a manner consistent with the Constitution and applicable laws, Executive Orders, and other Presidential directives;*

CBP's UAS are flown by sworn Federal law enforcement officers, who are guided by the Constitution, applicable US Code, DHS policy, and CBP OAM's evidence collection/retention policy.

In addition to CRCL and the Privacy Office's Department-wide oversight functions, CBP also has its own privacy officer and staff, which was reorganized in 2013 into the Privacy and Diversity Office under the CBP Commissioner to strengthen its ability to provide immediate on-site guidance and oversight of all CBP systems and programs.

As technology improves, operating environments change, laws evolve, and policies adapt, the Privacy Office and CBP staff will update or amend the Privacy Impact Assessment to refresh the analysis of these changes on the privacy of persons. CBP remains committed to involving legal, privacy, civil rights, and civil liberties experts throughout the life cycle of future projects involving sensor technologies used on UAS. In addition, CRCL and the Privacy Office's statutory authorities provide the means by which privacy and civil rights and civil liberties experts will remain involved from conception through deployment and thereafter.

The Privacy Office also conducts Privacy Compliance Reviews, which are designed to improve a program's ability to comply with assurances made in privacy compliance documentation



## FOR OFFICIAL USE ONLY

including Privacy Impact Assessments, System of Records Notices, and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreement. Privacy Compliance Reviews are performed at the discretion of the Chief Privacy Officer at any time during a program's life cycle.

*(iii) ensure that adequate procedures are in place to receive, investigate, and address, as appropriate, privacy, civil rights, and civil liberties complaints.*

CRCL's Compliance Branch investigates and resolves civil rights and civil liberties complaints filed by the public regarding DHS policies or activities. Complaints may be initiated by members of the public, Federal agencies or agency personnel, non-governmental organizations, media reports, and other sources through submissions to CRCL via mail, e-mail, fax, or telephone. Once a complaint is opened, CRCL staff determines whether to refer the complaint to the appropriate component for fact-investigating or to retain the complaint for investigation by CRCL (unless the Department's Office of Inspector General decides to investigate the allegations). If referred, the component is required to report its findings to CRCL. If the complaint is retained, CRCL staff conducts an investigation to determine if the factual allegations in the complaint can be verified. Whether a fact investigation is conducted by CRCL or a component, CRCL may recommend steps to be taken by the component to address policy issues of concern.

The Privacy Office is responsible for ensuring that the Department has procedures in place to receive, investigate, respond to, and provide redress for complaints from individuals who allege that the DHS has violated their privacy, or that DHS has not complied with privacy compliance requirements. U.S. citizens, Lawful Permanent Residents, visitors to the United States, and aliens may submit privacy complaints to the Privacy Office. Between June 1, 2013 and May 31, 2014, the DHS received 3,627 privacy complaints and closed 3,714.

As of the writing of this report, no correspondence or formal complaints regarding CBP's use of unmanned aircraft systems have been received by CBP, CRCL, or the Privacy Office.

**III. Accountability (Section 1(c)(i-vi).** *To provide for effective oversight, agencies shall:*

*(i) ensure that oversight procedures for agencies' UAS use, including audits or assessments, comply with existing agency policies and regulations;*

*(ii) verify the existence of rules of conduct and training for Federal Government personnel and contractors who work on UAS programs, and procedures for reporting suspected cases of misuse or abuse of UAS technologies;*

*(iii) establish policies and procedures, or confirm that policies and procedures are in place, that provide meaningful oversight of individuals who have access to sensitive information (including any PII) collected using UAS;*

*(iv) ensure that any data-sharing agreements or policies, data use policies, and record management policies applicable to UAS conform to applicable laws, regulations, and policies;*



## FOR OFFICIAL USE ONLY

*(v) establish policies and procedures, or confirm that policies and procedures are in place, to authorize the use of UAS in response to a request for UAS assistance in support of Federal, State, local, tribal, or territorial government operations; and*

*(vi) require that State, local, tribal, and territorial government recipients of Federal grant funding for the purchase or use of UAS for their own operations have in place policies and procedures to safeguard individuals' privacy, civil rights, and civil liberties prior to expending such funds.*

**Status:**

*(i) ensure that oversight procedures for agencies' UAS use, including audits or assessments, comply with existing agency policies and regulations;*

In order to hold personnel accountable for their use of data obtained by UAS, CBP has an established process for restricting the dissemination of video, still images, and radar images and keeps a log of disclosures. CBP complies with established privacy policies, practices, and procedures for associated recording systems. All Aviation Support Requests and chain of custody with regard to evidence are kept by OAM. Requests for Information are kept by OI; discrepancies discovered in the logs initially are addressed by holding component. Incidents involving inappropriate use, disclosures, or breaches involving data acquired by UAS are covered by the DHS *Privacy Incident Handling Guide*, which includes a process for assessing responsibility for incidents as well as mitigation strategies. CBP is also held accountable for redacting law enforcement sensitive information, personally identifiable information, and other sensitive related data unless the requestor has a valid need to know.

CRCL and the Privacy Office are granted broad oversight authority over all DHS components to ensure accountability. For instance, the Officer for Civil Rights and Civil Liberties is charged with “oversee[ing] compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by the programs and activities of the Department.”<sup>6</sup> Both officers for CRCL and the Privacy Office are required to coordinate efforts to ensure that “programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner.”<sup>7</sup> In the context of UAS, this coordination is clearly exhibited by the two offices’ joint creation of the Unmanned Aircraft Systems Working Group, and close collaboration in drafting UAS best practices to protect privacy, civil rights, and civil liberties.

CRCL and the Privacy Office both have statutory authority to investigate DHS components. As previously discussed, CRCL is empowered to “investigate complaints and information indicating possible abuses of civil rights or civil liberties, unless the Inspector General of the Department determines that any such complaint or information should be investigated by the Inspector

<sup>6</sup> 6 U.S.C. §345(a)(4).

<sup>7</sup> 6 U.S.C. §345(a)(5); *see also* 6 U.S.C. §142(a)(5)(A) (parallel responsibility for the DHS Chief Privacy Officer).



## FOR OFFICIAL USE ONLY

General.”<sup>8</sup> This authority empowers CRCL to investigate complaints related to CBP’s use of UAS.

Similarly, the Privacy Office is authorized to “make such investigations and reports relating to the administration of the programs and operations of the Department as are, in the senior official’s judgment, necessary or desirable;”<sup>9</sup> and, subject to coordination with the Inspector General for investigations of possible violations or abuse, subpoena necessary documentary evidence and administer to, or take from any person, an oath, affirmation, or affidavit. The Unmanned Aircraft Systems Working Group also provides a forum where issues of concern may be brought to the attention of the members, which in turn can be raised to the Secretary for resolution, if necessary.

Finally, as previously mentioned, the DHS Chief Privacy Officer has the discretion to direct a Privacy Compliance Review of a program to ensure compliance with assurances made in privacy compliance documentation and formal agreements.

*(ii) verify the existence of rules of conduct and training for Federal Government personnel and contractors who work on UAS programs, and procedures for reporting suspected cases of misuse or abuse of UAS technologies;*

All CBP employees are required to complete annual privacy awareness in addition to ethics and CBP Code of Conduct training. Access controls, both physical and technological, are in place to ensure only authorized access to the aircraft systems and the collected data/images. CBP also requires its employees to successfully complete training on techniques to copy recorded evidence to portable digital media, which requires them to follow procedures to ensure that such evidence is not co-mingled with data from other investigations. Employees are also trained to follow procedures to maintain an adequate chain of custody in the event that the information is used as evidence.

*(iii) establish policies and procedures, or confirm that policies and procedures are in place, that provide meaningful oversight of individuals who have access to sensitive information (including any PII) collected using UAS;*

The Privacy Office Privacy Compliance Reviews, as discussed, provide meaningful oversight of Departmental projects as the discretion of the Chief Privacy Officer. CBP’s OI also has a process for restricting the dissemination of video, still images, and radar images and keeps a log of the disclosures. OI redacts law enforcement sensitive information, personally identifiable information, and other sensitive related data unless the requestor has a valid need-to-know. Separately, CBP periodically reviews the logs or disclosure records to ensure compliance with established privacy policies, practices, and procedures for associated systems.

---

<sup>8</sup> 6 U.S.C. §345(a)(6).

<sup>9</sup> 6 U.S.C. §142(b).



## FOR OFFICIAL USE ONLY

*(iv) ensure that any data-sharing agreements or policies, data use policies, and record management policies applicable to UAS conform to applicable laws, regulations, and policies;*

As discussed earlier, the Privacy Office and CBP privacy staff will update or amend the Privacy Impact Assessment to reflect changes that may impact individual privacy. CBP remains committed to involving legal, privacy, and civil rights and civil liberties experts throughout the life cycle of future projects involving sensor technologies used on unmanned aircraft. In addition, the statutory authorities for CRCL and the Privacy Office provide both offices with the means to ensure individual rights are sustained throughout a UAS program's life cycle.

The DHS Unmanned Aircraft Systems Working Group may also serve as a forum for learning about UAS initiatives and identifying potential issues.

*(v) establish policies and procedures, or confirm that policies and procedures are in place, to authorize the use of UAS in response to a request for UAS assistance in support of Federal, State, local, tribal, or territorial government operations;*

CBP has existing policies and procedures for handling requests for UAS support. All requests for CBP UAS support must be coordinated through the National Command Duty Officer. Prior to a mission launch, requests for CBP UAS support must be coordinated in accordance with the current OAM *Aviation Support Request Policy*, through the Executive Director or Deputy of CBP National Air Security Operations. Each request for information follows a standard process that is reviewed and considered based on the requesting agencies' authorities to receive the sought after information, CBP's own authority to lend assistance, and CBP's ability to integrate the information collection into its mission.

OAM determines the availability of aircraft type and the integration of the requested activity into its flight operations. Typical support missions include overhead observation of persons, specified locations, and particular conveyances for enhanced situational awareness and increased officer safety. For example, a UAS could conduct surveillance over a building to inform ground units of the general external layout of the building or provide the location of vehicles or individuals outside the building. When flying a UAS in support of another component or government agency for an investigative operation, CBP may provide the other agency (b)(7)(E) (b)(7)(E) in whole or in part, based on the request.

The deployment of a CBP UAS must be conducted on a priority basis; however, this commitment will not preclude the use of other CBP aviation resources in support of additional authorized CBP mission and/or investigation. The following mission sets are listed in order of priority: 1. National CBP Missions; 2. CBP Missions; and 3. Other Federal/State/Local Missions (Resources Permitting)

Specific missions listed in order of priority include: 1. CBP law enforcement officer needs assistance; 2. Any other persons need assistance in life-threatening situations; 3. Reported crimes



## FOR OFFICIAL USE ONLY

in progress; 4. Investigative or other air support missions; 5. Routine mission support; and 6. Maintenance test flights.

*(vi) require that State, local, tribal, and territorial government recipients of Federal grant funding for the purchase or use of UAS for their own operations have in place policies and procedures to safeguard individuals' privacy, civil rights, and civil liberties prior to expending such funds.*

DHS's Federal Emergency Management Agency (FEMA) is responsible for reviewing and approving grants to State, local, tribal, and territorial governments. As a condition of accepting an award under the various preparedness grant programs, all recipients are required to execute and submit a fully completed Standard Form 424B ("SF-424B"), titled "Assurances for Non-Construction Programs." Assurance Number 6 in the SF-424B requires recipients to affirm that they will comply with all Federal non-discrimination statutes, including Title VI of the Civil Rights Act of 1964, which prohibits discrimination on the basis of race, color, or national origin. This assurance serves as a prohibition of the use of grant funds for any illegal discriminatory practices. Assurance Number 18 places a blanket requirement on recipients to comply with all Federal laws, executive orders, and regulations and policies governing the program. So by accepting an award, the recipients is acknowledging and certifying that any equipment purchased with grant funds, including UAS, will be employed and operated in compliance with all applicable laws and regulations.

Beyond these legal assurances, FEMA is currently working on an Information Bulletin/FEMA Policy to inform recipients that any requests to use grant funds for the purchase of a UAS must be accompanied by the recipients' civil rights, civil liberties, and privacy policies. In addition, the *Recommendations Pursuant to Executive Order 13688 Federal Support for Local Law Enforcement Equipment Acquisition Law* ( May 2015), listed UAS under the controlled equipment category and placed additional requirements on the purchase thereof. These requirements must also be incorporated into the Information Bulletin/FEMA Policy, as well as future Notices of Funding Opportunity. In the meantime, FEMA is not approving any requests for purchase of UAS with grant funding until such time as these requirements are finalized, which is anticipated to be for the FY 2016 grant funding cycle.

**IV. Transparency** (Section 1(d)(i-iii). *To promote transparency about their UAS activities within the NAS, agencies that use UAS shall, while not revealing information that could reasonably be expected to compromise law enforcement or national security:*

*(i) provide notice to the public regarding where the agency's UAS are authorized to operate in the NAS;*

*(ii) keep the public informed about the agency's UAS program as well as changes that would significantly affect privacy, civil rights, or civil liberties; and*

*(iii) make available to the public, on an annual basis, a general summary of the agency's UAS operations during the previous fiscal year, to include a brief description of types or categories of missions flown, and the number of times the agency provided assistance to other agencies, or to State, local, tribal, or territorial governments.*



## FOR OFFICIAL USE ONLY

**Status:**

*(i) provide notice to the public regarding where the agency's UAS are authorized to operate in the NAS;*

The privacy impact assessment published in September 2013 on CBP's aircraft systems provides transparency to the public about the current surveillance programs undertaken by CBP. Also, the video images associated with an individual's case file are covered by the appropriate law enforcement case management's system of records notice, which maintains the case file. All DHS privacy impact assessments, which are posted on DHS's website, are reviewed and updated, as necessary, every three (3) years. CBP will periodically re-assess the means by which the images from the aircraft are retrieved to determine whether the requirement for a system of records notice is triggered.

*(ii) keep the public informed about the agency's UAS program as well as changes that would significantly affect privacy, civil rights, or civil liberties;*

CBP provides a UAS Fact Sheet accessible on its website

[http://www.cbp.gov/sites/default/files/documents/FS\\_2014\\_UAS.pdf](http://www.cbp.gov/sites/default/files/documents/FS_2014_UAS.pdf) describing the Predator B UAS, its capabilities and its area of operations. In addition, periodic briefings by CBP, CRCL, and the Privacy Office to Members of Congress and their staffs, regular meetings with advocacy groups, and publication of privacy documentation on DHS's website provide a measure of transparency. Documents have already been released to the public under the Freedom of Information Act. The Privacy Office and CBP privacy staff will continue to update or amend the currently posted aircraft privacy impact assessment to reflect changes that may impact individual privacy.

*(iii) make available to the public, on an annual basis, a general summary of the agency's UAS operations during the previous fiscal year, to include a brief description of types or categories of missions flown, and the number of times the agency provided assistance to other agencies, or to State, local, tribal, or territorial governments.*

CBP's website currently provides public access to summaries of its significant UAS accomplishments for Fiscal Years 2011- 2014, which includes flight hours, types and amount of drug seizures, and general locations flown. <http://www.cbp.gov/border-security/air-sea/milestones-and-achievements/fiscal-year-2014-unmanned-aircraft-systems-highlights>. CBP also provides aggregate statistics for UAS supported activities and hours flown for FY 2006-2014. [http://www.cbp.gov/sites/default/files/documents/Aggregate%20Stats\\_UAS%20Supported%20Results%20and%20Hours\\_022515\\_FINAL\\_0.pdf](http://www.cbp.gov/sites/default/files/documents/Aggregate%20Stats_UAS%20Supported%20Results%20and%20Hours_022515_FINAL_0.pdf). Summaries for FY 15 will be posted after the end of the fiscal year and once statistics are compiled.