



Privacy Impact Assessment  
for

# FEMA Response Use of Unmanned Aircraft System (UAS) Derived Imagery

**DHS/FEMA/PIA-055**

**May 27, 2020**

**Contact Point**

**Christopher Vaughan  
Office of Response and Recovery  
Response Directorate  
(202) 212-1739**

**Reviewing Official**

**Dena Kozanas  
Chief Privacy Officer  
Department of Homeland Security  
(202) 343-1717**



## Abstract

The Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Office of Response and Recovery (ORR), Response Directorate (RD) uses imagery from Unmanned Aircraft Systems (UAS) to assist FEMA in fulfilling disaster response requirements with less cost, less environmental impact, and enhanced safety when compared to other conventional methods. FEMA RD does not own or operate UAS; instead FEMA RD uses mission assignment of other federal agencies (e.g., Civil Air Patrol, U.S. Customs and Border Protection) to obtain UAS-derived imagery. UAS-derived imagery enhances the common operational picture and supports FEMA situational awareness and decision-making. FEMA RD will not use the data provided by UAS operations to identify individuals, monitor an individual or group's movement, or intentionally gather personally identifiable information (PII); any PII collected is incidental and will be obfuscated or deleted prior to use or storage. DHS/FEMA is conducting this PIA to evaluate the privacy impact of the use of UAS-derived imagery.

## Introduction

The Department of Homeland Security (DHS), Federal Emergency Management Agency's (FEMA) mission is to support our citizens and first responders to ensure that as a nation, we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.<sup>1</sup> Specifically, FEMA Response Directorate (RD) is responsible for leading and coordinating efforts to maintain capabilities necessary to respond to and stabilize effects of presidentially declared disasters. Following a disaster declaration, FEMA RD may mission assign another federal agency to gather imagery using an Unmanned Aircraft System (UAS) to assist in fulfilling FEMA RD mission requirements including damage assessment, search and rescue, situational awareness, and assessment (e.g., route planning for emergency responders). UAS are equipped with video, radar, and/or other imaging technologies that allow FEMA RD to fulfill these missions with less cost, less environmental impact, and enhanced safety when compared to other conventional methods. UAS allow ground personnel to safely view disaster areas from above and gather images of the disaster without exposing emergency responders to potentially dangerous hazards and situations. UAS are particularly useful for emergency responders performing rapid response, search and rescue, and information gathering or situational awareness missions.

Mission assigned UAS range in size (depending on the provider) and are flown by operators on the ground using wireless ground control stations. The aircraft are equipped with cameras or imaging sensors that can capture images or video. UAS can transmit data to the ground stations through live streams or store them on removable media for retrieval upon landing.

---

<sup>1</sup> FEMA's responsibilities related to disaster response are outlined in the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, available at <https://www.fema.gov/media-library-data/1519395888776-af5f95a1a9237302af7e3fd5b0d07d71/StaffordAct.pdf>.



FEMA RD does not own or operate its own UAS aircraft. FEMA RD leverages UAS owned and operated by other federal agencies (e.g., Civil Air Patrol, U.S. Customs and Border Protection). Through mission assignments, FEMA RD designates specific areas or regions over which the assigned agency should operate UAS to capture images or videos relevant to FEMA's responsibilities. FEMA RD may also be granted access to UAS-derived imagery (i.e., photos and video) through information sharing agreements for UAS data acquired by other federal, state, local, tribal or territorial or organizations. FEMA RD does not mission assign UAS to conduct surveillance on individuals; however, the aircraft are equipped with technology that could capture images or video that can be associated with persons whom FEMA encounters. In addition to mission assignments, FEMA occasionally gets UAS-derived imagery from State, Local, Tribal and Territorial (SLTT) partners. These partners own and/or operate their own UAS technology and obtain the imagery without direction from FEMA. Any UAS-derived imagery obtained from SLTT partners will be handled in a manner identical to UAS-derived imagery received from FEMA mission assignments.

UAS-derived images are initially stored by the mission-assigned agency. When necessary for efficient or time-sensitive interagency disaster response, UAS-derived imagery may be delivered directly to FEMA field organizations and stored on approved FEMA Information Technology systems (e.g., Joint Field Office Geospatial Information System (GIS) servers, Local Area Network (LAN) servers, or approved and accredited cloud-based storage devices). All of these systems employ approved access control measures that require individual user accounts/passwords, which will be provided to FEMA RD employees and any other FEMA employees whom FEMA RD leadership determines has a need-to-know during disaster response and recovery. FEMA employees can then use approved computer and mobile devices to access the UAS-acquired images and videos, further process them into background maps, or derive disaster-specific information such as search and rescue plans or preliminary damage assessment products.

FEMA RD will review all UAS-derived imagery for PII elements. Any PII that is discovered in the imagery will be obfuscated or removed. Obfuscation methods include irreversible pixel blurring, pixel blocking by overlaying symbols or shapes, or permanent cropping of the PII element so it no longer exists in the image. For UAS-derived videos that contain PII, reviewers may also simply edit out ("cut" or "delete") that portion of the video (individual video frames) containing PII data. Once these edited versions of previously-PII-containing files are received by FEMA, FEMA RD will delete/destroy the corresponding, original, PII-containing images and videos.

The Geospatial Data Act of 2018 (GDA)<sup>2</sup> directed the Federal Geographic Data Committee (FGDC) to "operate an electronic service that provides access to geospatial data and metadata for geospatial data to the general public, to be known as the GeoPlatform." In keeping with open data

---

<sup>2</sup> Geospatial Data Act of 2018 (GDA), (Pub. L. 115-254), H.R. 302, Subtitle F, Sections 751-759, *available at* <https://www.fgdc.gov/gda/geospatial-data-act-of-2018.pdf>.



and data transparency best business practices and U.S government open data directives, FEMA's Response Geospatial Office (RGO) employs the Department of Interior's GeoPlatform as the primary means for sharing disaster response and recovery-related geospatial and remotely-sensed data (to include UAS-derived imagery and videos) and derived products with Whole of Community (federal, state, local, tribal, territorial, and private sector) emergency managers, disaster survivors, and the general public.

FEMA RD uses a secure space on the Department of the Interior's (DOI) GeoPlatform to store UAS-derived imagery. Any UAS-derived imagery delivered directly to FEMA field organizations will be uploaded and stored by FEMA RD on to GeoPlatform. Data on GeoPlatform can be configured as either "public" data, meaning anyone can view or access it, or "controlled" data, meaning it can only be viewed or accessed by appropriately credentialed and authorized users. The UAS-derived imagery received by FEMA RD will initially be stored in password-protected folders within the secure section of GeoPlatform that can only be accessed by FEMA-approved users for the express purpose of reviewing the data for PII. No UAS-derived imagery will be released to public GeoPlatform users or operationalized until it has undergone a PII review and all PII elements have been redacted, deleted, or blurred. Once this review is complete, and the UAS-derived imagery is moved to the public section of GeoPlatform, the data will be removed from the secure section. This imagery may also then be transferred to the FEMA Enterprise Network.<sup>3</sup>

### Response Directorate Uses of UAS Derived Imagery

FEMA RD uses mission assigned UAS to provide FEMA, and those directly involved with incident-specific disaster response or recovery duties, with imagery or video data for situational awareness and assessment regarding the impacts of disasters. Specifically, FEMA RD uses UAS-derived imagery during disaster response to determine the presence or extent of damage such as debris fields, flood inundation extents, fire lines, etc.; to conduct rapid, preliminary inspections of key facilities like dams, bridges, power generation plants, etc.; to enumerate and assess damages to the housing sector in order to validate a Governor's request for a Presidential disaster declaration; or to otherwise provide information to support life-sustaining and community lifeline stabilization activities.

Infrared imagery or Infrared video may also be requested to indicate heat emanating from animals, people, or impacted facilities or power generation and transmission lines, which can help determine damage, danger, or potential cascading effects from power surges or outages. Video may be requested to detect time-sensitive, near-real-time movements of groups of people along evacuation or other routes and help focus the delivery of critical life-sustaining commodities or transportation. In such uses, FEMA RD is only interested in the presence and whereabouts of the

---

<sup>3</sup> The imagery is initially stored on GeoPlatform instead of the FEMA Enterprise Network because of the cost efficiencies, ability to store large quantities of data, and the tools available for redaction purposes.



group to deliver lifesaving or sustaining services and will not use the video footage or images to identify any individuals or for any other purposes.

Additionally, aerial imagery and multi-spectral imagery collected by UAS operations under a FEMA RD mission assignment may be processed and converted into high-quality background maps. Or, the data may be visibly or automatically analyzed using computer-aided technologies and damage detection algorithms to classify damages and extract imagery-derived geospatial layers, such as flood or damage extents, by comparing pre-event imagery and post-event data. Such damage maps will be integrated into impact or situation maps or used to validate damage and impact models. Infrared sensors aboard UAS help detect water and can be used to map floods or changes in shorelines. Multispectral or hyperspectral sensors may be used by mission-assigned UAS to identify specific materials in debris fields, such as asbestos or other hazardous materials, or to assess the health of crops and vegetation, such as differentiating between living and dead trees.

## Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.<sup>4</sup>

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.<sup>5</sup> The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208<sup>6</sup> and the Homeland Security Act of 2002 Section 222.<sup>7</sup> Given that FEMA's use of unmanned aircraft systems is a privacy sensitive technology rather than a particular information technology system, this PIA is conducted as it

---

<sup>4</sup> 6 U.S.C. § 142(a)(2).

<sup>5</sup> See Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>6</sup> 44 U.S.C. § 3501 note.

<sup>7</sup> 6 U.S.C. § 142.



relates to the DHS construct of FIPPs. This PIA examines the privacy impact of UAS operations as it relates to the FIPPs.

## 1. Principle of Transparency

*Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.*

FEMA is publishing this PIA to provide notice and transparency to the public about the FEMA Response Directorate's current use of UAS-derived imagery to support its operations. FEMA does not intend to collect PII with UAS-derived imagery; however, there is the possibility of unintended PII being collected. Any PII that is discovered in the imagery will be obfuscated or removed prior to being shared by FEMA.

**Privacy Risk:** There is a risk that a member of the public will not know that mission assigned UAS may be collecting photos, videos, or other information on behalf of FEMA.

**Mitigation:** This risk is partially mitigated. FEMA provides notice of its use of UAS-derived imagery through the publication of this PIA. However, the risk cannot be fully mitigated as FEMA's use of UAS-derived imagery is directly related to disaster response and requires immediate deployment to be effective. Notice is not always possible, but the imagery is obtained by flights through areas where FEMA has a responsibility to respond (e.g., disaster areas). In addition, FEMA cannot guarantee the branding on the mission assigned aircraft because they are operated by different agencies.

## 2. Principle of Individual Participation

*Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

FEMA RD will not link UAS-collected imagery to an individual. Any collection of images related to individuals is incidental and will not be used by FEMA in any agency processes or for operational purposes. Any PII that is discovered in the imagery will be obfuscated or removed prior to being shared by FEMA. FEMA is unable to obtain individual consent prior to the collection, use, dissemination, and maintenance of UAS-derived imagery as it would interfere with FEMA's ability to obtain timely information critical to the execution of its mission. Additionally, for certain operations such as search and rescue, the intention is to locate individuals that may need to be rescued. In such cases, FEMA would not be able to obtain consent beforehand.



Any individual may seek notification of and access to any FEMA record pursuant to procedures provided by FOIA and can do so by visiting <https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form>, or by mailing a request to:

FEMA Disclosure Branch  
Federal Emergency Management Agency  
Department of Homeland Security  
500 C Street, SW  
Washington D.C. 20742

The request should include the name of the requester, nature of the record(s) sought, and the required verification of identity.

**Privacy Risk:** There is a risk that individuals are unable to provide consent to being recorded in UAS-derived imagery.

**Mitigation:** This risk is not mitigated. Through the publication of this PIA individuals are provided notice of this possible collection; however, consent is not possible due to the nature of FEMA's mission and the requirement to obtain timely information. FEMA determined it does not require PII to complete this mission. Although consent may not be obtained, there is minimal impact to individuals because FEMA does not retain any PII through the measures outlined above.

### 3. Principle of Purpose Specification

*Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

FEMA RD uses UAS-derived video and imagery pursuant to Stafford Act disaster declarations to gain situational awareness and to support lifesaving and life-sustaining decisions by emergency responders and emergency managers. FEMA RD will not link UAS-derived imagery to an individual. Any PII that is discovered in the imagery will be obfuscated or removed prior to being saved or shared by FEMA.

FEMA RD mission assigns UAS to assist FEMA in fulfilling mission requirements with less cost, less environmental impact, and enhanced safety when compared to other conventional methods. UAS also promote safety and reduce risks to employees engaging in potentially dangerous operations, particularly for emergency responders during rapid response and situational awareness missions. The purpose of UAS use aligns with FEMA's overall mission under the Stafford Act to support the public and first responders to ensure FEMA builds, sustains, and improves its capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

**Privacy Risk:** There is a risk that FEMA will use UAS-derived imagery for purposes other than those articulated in this PIA.



**Mitigation:** This risk is mitigated. Documented procedures for the use and sanitization of UAS-derived imagery are communicated within FEMA RD. This sanitization occurs upon receipt of any imagery. Once the UAS-derived imagery is verified to be free of PII it is made publicly available via the GeoPlatform.

## 4. Principle of Data Minimization

*Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

FEMA RD seeks to minimize the amount of UAS imagery collected and retains only to the amount necessary and relevant to carry out FEMA RD missions. When FEMA RD mission assigns an agency to provide UAS services, an exact description of what data FEMA needs the UAS to collect will be provided to that agency. Any PII that is discovered in the imagery will be obfuscated or removed prior to being shared by FEMA.

**Privacy Risk:** There is an over-collection risk associated with the fact that FEMA does not control the UAS technology used to collect imagery.

**Mitigation:** This risk is mitigated. FEMA minimizes over-collection risk through the obfuscation and/or removal of PII as described previously. Obfuscation methods include irreversible pixel blurring, pixel blocking by overlaying symbols or shapes, or permanent cropping of the PII element so it no longer exists in the image. For UAS-derived videos that contain PII, reviewers may edit out (“cut” or “delete”) that portion of the video (individual video frames) containing PII data.

## 5. Principle of Use Limitation

*Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

FEMA RD collects UAS-derived imagery to support various aspects of its mission as outlined in the introduction of this PIA. FEMA RD will not use any images captured that are related to individuals beyond the scope of FEMA RD operations, as outlined in this PIA. If UAS data is provided to FEMA with information about individuals or activities that are beyond the scope of FEMA’s authorities, it will be referred to the appropriate agency or organization, or destroyed, as applicable. Any PII that is discovered in the imagery will be obfuscated or removed prior to being shared by FEMA.



**Privacy Risk:** There is a risk that UAS-derived imagery may contain information about individual activities that are beyond the scope of FEMA’s authorities. For example, UAS cameras may capture individuals entering places or engaging in lawful activities as they relate to their daily lives. Although unlikely during normal operations, there is a possibility that a UAS may collect video images, photographs, radio frequency emissions, and location information of an individual entering a doctor’s office, attending public rallies, social events, meetings, or associating with other individuals.

**Mitigation:** This risk is mitigated. FEMA minimizes this through the obfuscation and/or removal of PII as described previously in this PIA. Obfuscation methods include irreversible pixel blurring, pixel blocking by overlaying symbols or shapes, or permanent cropping of the PII element so it no longer exists in the image. For UAS-derived videos that contain PII, reviewers may also simply edit out (“cut” or “delete”) that portion of the video (individual video frames) containing PII data.

## 6. Principle of Data Quality and Integrity

*Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

FEMA does not control the technology used to collect the UAS-derived imagery; FEMA relies on the agency providing the data for assurance of data quality and integrity.

**Privacy Risk:** There is a risk that UAS-derived imagery will contain data that is not accurate, relevant, timely and complete. This risk is escalated because FEMA does not control the technology that will be used to collect the data.

**Mitigation:** This risk is partially mitigated. FEMA will outline specific data requirements for all mission assignments and when receiving UAS-derived imagery from SLTT partners, FEMA will verify the accuracy as possible. However, FEMA will rely on the source agency for accuracy and integrity. Additionally, FEMA RD does not use UAS-derived imagery to make benefit determinations or take action against individuals. Any inaccurate information would not have an impact on the privacy of an individual.

## 7. Principle of Security

*Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

FEMA RD relies on the source agency to protect video and imagery data captured during UAS activities. If the data was collected solely for FEMA (i.e., mission assignments), FEMA RD will request that the source agency verify that it has destroyed their copy of the data. Once FEMA



has accepted the data it will be stored on a secure section of the GeoPlatform while undergoing the process for purging PII as described above. Access to this area on the GeoPlatform will be limited to FEMA RD employees.

**Privacy Risk:** There is a risk that the agency collecting UAS-derived imagery does not provide appropriate security safeguards.

**Mitigation:** This risk is partially mitigated. Mission assigned federal agencies are expected to be knowledgeable and compliant with required security protocols. FEMA does not have a way to mitigate this risk when it concerns SLTT partners who provide UAS-derived imagery obtained separate of FEMA missions.

**Privacy Risk:** There is a risk that FEMA maintains imagery on a non-DHS accredited system.

**Mitigation:** This risk is mitigated. Only FEMA personnel and authorized contractors will have access to FEMA's secure section of the system. Additionally, GeoPlatform has gone through the accreditation and authorization process and received its Authority to Operate from the DOI. While the system was not accredited by DHS, it is a FedRAMP-approved system

## 8. Principle of Accountability and Auditing

*Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

FEMA RD will not use UAS-derived imagery that contains PII as part of its mission; however, all FEMA employees are required to complete annual DHS privacy training regarding the safe handling and protection of PII.

UAS-derived imagery will only be accessible to select FEMA RD employees while it undergoes the review for potential PII. Once all PII has been obfuscated or destroyed, the imagery will be posted to the public portion of the GeoPlatform as described previously in this PIA.



## Conclusion

FEMA RD incorporates UAS-derived imagery from mission assigned federal partners or SLTT partners into disaster response operations. FEMA RD will not request or mission assign UAS that might carry feature or facial recognition technologies that could identify individuals. FEMA RD will also not request UAS to collect PII on individuals. Any PII incidentally collected by UAS and shared with RD officials will be obfuscated or destroyed as necessary.

## Responsible Officials

William H. Holzerland  
Senior Director for Information Management  
Office of the Chief Administrative Officer  
Federal Emergency Management Agency  
Department of Homeland Security

## Approval Signature

Original, signed copy on file with the DHS Privacy Office.

---

Dena Kozanas  
Chief Privacy Officer  
Department of Homeland Security