



PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.

All entries must be Times New Roman, 12pt, and start on the next line.

If you need further assistance, contact your LPO. A listing of the LPOs can be found here:

https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO Roster.docx

System Name: Multimedia Division (MD)		System Owner: Jini Ryan	
Preparer: Anthony Singleton		Office: AO-OEA-MD	
Date: 07/24/2026		Phone: 202-564-2293	
Reason for Submittal:			
New: ☐	Revised: ☒	Annual Review: ☐	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: ☒	Rescindment/Decommission: ☐		
Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f). The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).			

Provide a general description/overview and purpose of the system:

EPA's Multimedia Division (MD) is the full-service multimedia production unit. Through broadcasting, livestreaming, photography, audio, and graphics, MD helps keep EPA staff and the general public informed and up to date on the latest Agency activities and messages.

All multimedia produced in EPA's video studios (Studio One) is captured or created, edited, encoded, and broadcast for public distribution. MD keeps a database of all captured or created media for a period of five years, after which the content is sent to the National Archives for permanent storage per records keeping regulations.

Cybersecurity implementation is designed with a multi-faceted defense approach. MD utilizes CrowdStrike Falcon EPS and Tenable Nessus vulnerability scanning separate from EPA OFA security solutions due to the nature of the office. These software packages provide the MD ISSO with the ability to utilize End-Point Security, Antivirus, Virtual Firewall, audit logging and STIG vulnerability scanning. MD also employs YubiKey for multi-factor authentication.

Section 1. Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

Video and audio data often transferred to MD or collected by MD will be the interview subject's name, workplace, and job titles. Business phone numbers are collected via email for communications purposes only.

In accordance with OMB Circular No. A-123, Section VII(A) and 44 U.S.C. § 3501 note. Section 208(b); MD system is designed not to collect any additional PII type. All multimedia content generated by MD is in the public domain and falls under "unrestricted" access and distribution and does not contain non-public information.

IAC w/ NIST SP 800-122 the only PII collected is the person's name. Business phone numbers, workplace, and job titles are not considered PII.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have, or will the system be issued an Authorization-to-Operate? When does the ATO expire?

MD does have an SSP published in Xacta. MD has a current ATO due to expire on August 28, 2027.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

N/A

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FEDRAMP approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes, limited multimedia content (photos, video and graphics) is temporarily stored through FEDRAMP certified provider Box.com in order to transfer multimedia material to agency stakeholders. All multimedia content generated by MD is in the public domain and falls under "unrestricted" access and distribution and does not contain non-public information. Only assigned/authorized personnel have access to the Box.com account. The content is provided to

specific stakeholders with a restricted access link that expires after 5 days.

Section 2. Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

Video and audio data often transferred to MD or collected by MD will be the interview subject's name, workplace, and job titles. Business phone numbers are collected via email for communications purposes only.

The system collects raw analog or digital video/audio from various camera/microphone input devices in conjunction with digital recording devices. Digital photography is also taken for record. This data is then manipulated for storytelling or information distribution purposes. The final dissemination of the product is used to transmit the intent of EPA's mission to the public and EPA employees on behalf of the Office of the Administrator. The format of the product could take the form of any or all of the following: video/audio broadcasting via satellite, closed circuit television, live broadcast television, webcasting, press announcements, public educational films, social media or internal EPA training media. All multimedia content generated by MD is in the public domain and falls under "unrestricted" access and distribution and does not contain non-public information.

2.2 What are the sources of the information and how is the information collected for the system?

The source of the information varies depending on the topic of the content and ranges from internal EPA personnel and federal/state/tribal partners to stakeholders and stock content sites. The content is dependent on the type of multimedia product that is needed, for example: B-roll video footage, radio or video interviews, live footage, educational films, training videos, webcasting, web meeting, photographs, graphics, podcasting, music, stock footage, historic maps, etc.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

In the course of content creation, MD sometimes relies on commercially available materials like interview footage from contractors, other federal/state/tribal partners, or EPA stakeholders etc. that is obtained directly from each source. Non-public information obtained from specific individuals or entities (stakeholders) is used only with express permission from the copyright owner through an EPA consent form or licensing agreement. This material is stored only for use in the multimedia content under production and is not transferred to the National Archives as they are not official EPA records and the copyright remains with the source of the material.

2.4 Discuss how accuracy of the data is ensured.

The data is retained on an off-network Digital Asset Management System that resides only

within MD. Reliance of data accuracy is high as only assigned/authorized personnel have access to this data.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included

Privacy Risk:

All MD-generated content is in the public domain and falls under “unrestricted” access and distribution and does not contain non-public information. The system collects raw digital video/audio from various camera/microphone input devices in conjunction with digital recording devices. Digital photography is also taken for record. This data is then produced into multimedia content to include public service announcements, feature stories, infographics, photo slideshows, audio podcasts, social media clips, etc., to disseminate agency messages to EPA employees, stakeholders, and the public. The format of the product can also take one or more of the following forms: video/audio broadcasting via satellite, closed circuit television, live broadcast television, webcasting, press announcements, public educational films, social media, or internal EPA training media. MD does not remediate the data in any way. At the time of recording one-on-one content with individuals, MD obtains signed consent from the subject using documentation, reviewed and approved by the Office of General Counsel, to use their name, likeness and voice. Any media procured from an individual or entity for use in an EPA multimedia product, (example photos, video clips, etc.), is also obtained using a signed license agreement form, also approved by the Office of General Counsel, granting the agency permission to use the material.

Mitigation:

At the time of recording one-on-one content with individuals, MD obtains signed consent from the subject using documentation reviewed and approved by the Office of General Counsel to use their name, likeness and voice. Any media procured from an individual or entity for use in an EPA multimedia product, (example photos, video clips, etc.), is obtained using a signed license agreement form, also approved by the Office of General Counsel, granting the agency permission to use the material.

Section 3. Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don’t have a need to know? If so, what control levels have been put in place? If no controls are in place, why have they been omitted?

MD production systems will not have access control levels installed beyond two factor authentication due to the operational requirement of multimedia transfers and editing software needing full administrator access for proper use, as well as multimedia production requirements in support of the agency. All personnel will have the ability to access the data stores with the Chief Engineer as the system administrator.

3.2 What policy/procedure are the access controls identified in 3.1, documented?

04 OM POLICY - Identification and Authentication Procedure (IA) 2025

3.3 Are there other components with assigned roles and responsibilities within the system?

None

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Only MD government-employed personnel and authorized OM ORISE Fellow or OM interns will have explicit access to the data.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Record schedule class 722 has been established for multimedia content. MD maintains digital signatures, audit, network traffic logs, system logs, and deliberative product, final product, video footage, audio/photo/graphics files for five (5) years, per records keeping protocols. Completed products and raw MD-captured content considered an official agency record is transferred to the National Archives for historical preservation, which is researchable and obtainable via a media/public query, a FOIA request or contacting NARA directly.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system

Privacy Risk:

MD maintenance of digital signatures, audit, network traffic logs, system logs, and deliberative and final product, video footage, audio/photo/graphics files for a storage period of five years is secured physically behind a keyed main door and a crypto key access door. The data store is further secured by maintaining an off-network enclave designed with a multi-faceted defense approach. The data store also employs YubiKey multi-factor authentication for secure access. MD content, considered official agency records, is stored for a period of five years then transferred to the National Archives for historical preservation.

Mitigation:

MD data is secured physically behind a keyed main door and a crypto key access door. The data store is further secured by maintaining an off-network enclave designed with a multi-faceted defense approach. The data store also employs YubiKey multi-factor authentication for secure access.

Section 4. Information Sharing

CUI//ISVI
For Official Use Only (FOUO)

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local governments, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Yes, information is created to be shared outside of EPA as part of normal agency operations through the Office of External Affairs. All MD-captured and generated content is considered public domain and “unrestricted,” and is readily available to the public upon request. The data is public information and available to other federal agencies, state/tribal, and local governments, EPA stakeholders and the general public through the EPA website, news sites, social media channels and web-based hosts, a media query or through a FOIA (Freedom of Information Act) request. Other federal agencies, state/tribal, or local governments and EPA stakeholders do not have direct access to EPA’s Box, a FEDRAMP cloud SaaS system, only a download link for the specific content they’ve requested.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

All multimedia produced by MD is captured or created, edited, encoded, and broadcast for public distribution. Multimedia data is shared with external sources and is also released to entities with an approved FOIA (Freedom of Information Act) request. The data shared is considered public domain and “unrestricted,” and available for external use through media queries or content requests from the public.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

MD system does not conduct any information sharing beyond a formal FOIA, media query or public content request.

4.4 Does the agreement place limitations on re-dissemination?

All MD-captured and generated content is considered public domain and “unrestricted,” and readily available to the public upon request.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

4.6 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

MD system does not conduct any information sharing beyond a formal FOIA, media query or public content request.

4.7 Does the agreement place limitations on re-dissemination?

All MD-captured and generated content is considered public domain and “unrestricted,” and readily available to the public upon request.

4.8 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

All MD-captured and generated content is considered public domain and “unrestricted,” and readily available to the public upon request. MD-generated content considered an official agency record is transferred every five (5) years to the National Archives for historic preservation and is readily available upon request by any individual or entity. Privacy risk is at the lowest level and does not need to be remediated.

Mitigation:

At the time of recording one-on-one content with individuals, MD obtains signed consent from the subject using documentation, reviewed and approved by the Office of General Counsel, to use their name, likeness and voice. Any media procured from an individual or entity for use in an EPA multimedia product, (example photos, video clips, etc.), is also obtained using a signed license agreement form, also approved by the Office of General Counsel, granting the agency permission to use the material.

Section 5. Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

The system collects raw analog or digital video, audio, graphics and photo assets from a variety of sources. The acquired data is used to inform EPA employees, stakeholders and the public about the agency's mission and priorities. All multimedia content generated by MD is in the public domain and "unrestricted." Content is stored on secure GFE systems and used in conjunction with specific projects and agency messaging needs. This content is collected, edited, and produced separately and isolated from the EPA LAN, and thus has no capability to be audited via established enterprise methods. MD uses a date-based/topic-based naming convention for all captured content. MD producers, in conjunction with the MD director, manage each production data set.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

MD enforces the mandatory agencywide Information Security and Privacy Awareness training. MD Director provides verbal/written instructions on obtaining consent and license agreement forms.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

MD loses track of multimedia created in the office.

Mitigation:

The collected, edited, and produced data is separate from the EPA LAN, and thus has no capability to be audited via established enterprise methods. MD tasks individual producers to manage each production data set. Each producer is held responsible for data integrity and for ensuring backups are in place on the MD archive. The MD archivist verifies media via visual checks and meta data tagging for records keeping purposes.

Section 6. Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

The data acquired is used for outreach and communications purposes to inform EPA employees, stakeholders and the general public about the agency's mission and priorities via audiovisual content to produce educational, training, public information, interviews, social media and specialty features.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: ☐ No: ☒ If yes, what identifier(s) will be used.

A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.

Information is retrieved by date of event, project, or program.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

Prior to collection of multimedia assets, project team leaders in EPA programs and regions are required to obtain signed agency consent forms and/or content license agreements from individuals, to include EPA employees, who will be participating in the multimedia project via interviews, footage, photos, graphics and audio actualities. Assigned MD producers maintain and access the data to create multimedia content to disseminate agency messages. The media assets collected are considered public domain and "unrestricted" and those interviewed by MD have no reasonable expectation of privacy by signing the consent form. MD limits access to its data to only authorized users of the MD system, however, MD responds to content requests received through the FOIA process, media enquiries to the Office of External Affairs, or direct requests from the public, and releases only relevant materials in relation to those requests.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

MD employees could misuse images of individuals.

Mitigation:

MD has a limited number of audiovisual producers and support staff who are all federal employees. They must be cleared by the MD director/system owner to have access to various key and keypad locked studios. They are all mandated to take annual agency training for cybersecurity and ethics. MD personnel are required to sign a rule of behavior statement annually. Individuals who are not part of the

MD team do not have access to MD studios without an escort.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required.
If so, the following additional sections will be required.

Section 7. Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt-out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information.

Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Mitigation:

Section 8. Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card,

employee badge or identification card). Additional identity verification procedures may be required, as warranted.

Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and Freedom of Information Act (FOIA).

Privacy Risk:

Mitigation:

I attest as the Agency Privacy Officer that **Multimedia Division (MD)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt. Branch
EPA/OFA