PRIVACY IMPACT ASSESSMENT (PIA)

For the

Unified Video Dissemination System (UVDS)
Defense Information Systems Agency (DISA)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	14174
☒	**Yes, SIPRNET**	Enter SIPRNET Identification Number	14174
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes** ☒ **No**

If "Yes," enter UPI _____

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier K890.16 DoD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. _____

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

The authority allows Unified Video Dissemination System (UVDS) to collect the following data:

- 5 U.S.C. 301, Departmental Regulation;
- 10 U.S.C. chapter 8; DoD Directive 5105.19, Defense Information Systems Agency (DISA)
- DISA Memorandum for Principal Director for Network Services, Subject: Authorization to Operate for the Unified Video Dissemination System, Tracking Number 020571010, DITPR ID 14174, 16 October 2012
- DoDI 8510.01, Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

UVDS provides the framework for the integration and standardization of the Full Motion Video (FMV) within the Department of Defense (DoD). The UVDS consolidates FMV distribution architectures and establishes a standard approach for the back-haul, routing, storage, ingest, and dissemination of video and corresponding metadata. In addition, UVDS extends FMV dissemination capabilities through a suite of web-based applications, the UVDS Portal, to include live streaming video, archives and a fully integrated theater-wide FMV common operating picture.

The UVDS Portal application, accessible only on the SIPRNET network, is the only component of the UVDS involved in the collection of a limited number of the PII data elements. The UVDS Portal, a web-based application, includes an end-user self-registration web form. The form allows the UVDS Portal users to self-register for a UVDS Portal login account. During the self-registration, users are required to provide following PII information: First Name, Last Name, Office E-mail Address, Organization, Office Phone, and Location. Email addresses provided during the registration by the end-users are used to establish UVDS Portal User IDs. User ID is used to identify UVDS Portal users, enables UVDS Portal customization for each UVDS registered user, and allows UVDS data owners to control access to the restricted UVDS content.

The type of PII information collected by the UVDS is identified as a non-sensitive PII, releasable to the public IAW DoD 5400.11-R, Paragraph C4.2.2.5.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risk associated with the PII data collected by UVDS is determined as Low. The type of PII information collected by the UVDS is identified as non-sensitive PII, releasable to the public IAW DoD 5400.11-R, Paragraph C4.2.2.5.
Access to the type and an amount of data is governed by the privileges and access permissions implemented within UVDS application and its back-end components, i.e. UVDS database. The Defense-in-Depth methodology is used to protect UVDS data repository and system interconnections, including (but not limited to) Secure Sockets Layer/Transport Layer Security, access control lists, file system permissions, application permissions, intrusion detection and prevention systems and audit and log monitoring. These protections are implemented through shared responsibility between DISA DECCs and UVDS personnel. Access to UVDS information, including PII data, and information systems is restricted to and controlled by the certified and authorized personnel who are responsible for maintaining UVDS system integrity and data confidentiality.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☐ **Within the DoD Component.**

Specify.

☒ **Other DoD Components.**

Specify. DISA DECC System Administrators, UVDS System Administrators

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

The PII collected by UVDS is required to implement and operate UVDS. If these data elements were not available, UVDS would not be able to (1) properly identify authorized DoD Users (2) implement PKI/SIPRNet Token- based user authentication (currently in the process of being implemented).

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

These PII data are required to implement UVDS user authentication and properly identify authorized DoD users.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☒	**None**

Describe each applicable format.	UVDS does not provide information to an individual when asked to provide PII data during self-registration as the data collected is non-sensitive PII information and is considered releasable to the public per DoD 5400.11-R (paragraph C4.2.2.5).

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.