PRIVACY IMPACT ASSESSMENT (PIA)

	ICT A55	ESSMENT (FIA)	
PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Imp. (DoD) information systems or electronic collections of information (referred and/or disseminate personally identifiable information (PII) about members military facilities internationally. In the case where no PII is collected, the P system.	to as an "el of the publi	ectronic collection" for the purpose of c, Federal employees, contractors, or	f this form) that collect, maintain, use, foreign nationals employed at U.S.
1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:			
Automated Security Validation (ASV)			
2. DOD COMPONENT NAME:			3. PIA APPROVAL DATE:
Defense Information Systems Agency			10/18/24
SECTION 1: PII DESCRIPTIO	ON SUMMA	RY (FOR PUBLIC RELEASE)	
a. The PII is: (Check one. Note: Federal contractors, military family memb	bers, and fo	reign nationals are included in genera	al public.)
From members of the general public	x	From Federal employees	
from both members of the general public and Federal employees		Not Collected (if checked proceed to	o Section 4)
b. The PII is in a: (Check one.)			
New DoD Information System		New Electronic Collection	
X Existing DoD Information System		Existing Electronic Collection	
Significantly Modified DoD Information System			
 c. Describe the purpose of this DoD information system or electroni collected in the system. The ASV system is used to conduct breach and attack simulations ASV provides JFHQ-DODIN a central repository for multiple sim names, rank/grade is collected to create a user account on the AS' request for access. The types of personal information that is collected information. d. Why is the PII collected and/or what is the intended use of the PII' 	s to baselin nulations i V system. ected inclue	ne, assess and continuously monit results and reports across the DoE Security information is used to va des: Name(s), DoD ID Number, F	tor cyber defensive capabilities. D DAOs. User DOD ID number, ralidate and support the user's Rank/Grade, and Security
administrative use) PII is collected for verification, identification and authentication.			
 e. Do individuals have the opportunity to object to the collection of t (1) If "Yes," describe the method by which individuals can object to the c (2) If "No," state the reason why individuals cannot object to the collection 	collection of on of PII.		
Individuals can object to the collection of their PII by not comple	ting and s	ubmitting the information require	2d.
f. Do individuals have the opportunity to consent to the specific uses (1) If "Yes," describe the method by which individuals can give or withho (2) If "No," state the reason why individuals cannot give or withhold their Individuals can object to the specific uses of their PII by not complete for the specific uses of their PII by not complete for the specific uses of their PII by not complete for the specific uses of the specific uses of the specific uses for the specific uses of the specific uses uses of the specific uses uses uses used uses used uses used uses used uses uses	old their cons	sent.	uired.
g. When an individual is asked to provide PII, a Privacy Act Statemer	nt (PAS) an	d/or a Privacy Advisory must be pr	rovided. (Check as appropriate and
provide the actual wording.) X Privacy Act Statement Privacy Advisory	Г	Not Applicable	
	or Govern		w 00 171 the Computer Frend
AUTHORITY: Executive Orders 10450, Security requirements for and Abuse Act. PRINCIPAL PURPOSE(S): To collect names, signatures, and oth			-

PRINCIPAL PURPOSE(S): To collect names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

DD FORM 2930, JUN 2017

	UTINE USE(S): None CLOSURE: Voluntary; however, failure to provide the reques lest.	sted informa	tion may impede, delay or prevent further processing of this
h. V	Vith whom will the PII be shared through data/system exchange, b Check all that apply)	both within y	our DoD Component and outside your Component?
X	Within the DoD Component	Specify	DISA
	Other DoD Components (i.e. Army, Navy, Air Force)	Specify	
	Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)	Specify	
	State and Local Agencies	Specify	
	Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)	Specify	
	Other (e.g., commercial providers, colleges).	Specify	
i. So	ource of the PII collected is: (Check all that apply and list all information	tion systems i	applicable)
X	Individuals		Databases
	Existing DoD Information Systems		Commercial Systems
	Other Federal Information Systems		
j. Ho	w will the information be collected? (Check all that apply and list a		
	E-mail	X	Official Form (<i>Enter Form Number(s) in the box below</i>)
	In-Person Contact		Paper
	Fax		Telephone Interview
	Information Sharing - System to System		Website/E-Form
	Other (If Other, enter the information in the box below)		
DD	FORM 2875		
k. C	Does this DoD Information system or electronic collection require	a Privacy A	ct System of Records Notice (SORN)?
A Pi	rivacy Act SORN is required if the information system or electronic col etrieved by name or other unique identifier. PIA and Privacy Act SORN	llection contai	ns information about U.S. citizens or lawful permanent U.S. residents that
	Yes X No		
lf "Y	/es," enter SORN System Identifier		
	RN Identifier, not the Federal Register (FR) Citation. Consult the DoD /acy/SORNs/ or	Component I	Privacy Office for additional information or http://dpcld.defense.gov/
	SORN has not yet been published in the Federal Register, enter date ision (DPCLTD). Consult the DoD Component Privacy Office for this of		n for approval to Defense Privacy, Civil Liberties, and Transparency
lf "	No," explain why the SORN is not required in accordance with DoD Re	egulation 540	0.11-R: Department of Defense Privacy Program.
	date is being collected as DII is only used as a method of veri	fication ide	ntification and authentication purposes. As detailed in DoD

(1) NARA Job Number or General Records Schedule Authority.

DAA-GRS-2016-0016-0002

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.
Destroy when no longer needed for business use, or according to an agency predetermined time period or business rule.
m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.
 If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar. If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.
The authority below allows Automated Security Validation (ASV) to collect the following data:
10 U.S.C. Chapter 8-Defense Agencies and Department of Defense Field Activities;
DoD Directive (DoDD) 5105.19, Defense Information Systems Agency (DISA);
DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program;
DoD Enterprise User Data Management Plan for Persons and Personas;
DoD Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS);
DoDI 5200.46-DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC) DoDI 8520.03-Identity Authentication for Information Systems.
n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 X No Pending
 (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates. (2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections." (3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation. OMB approval is not required in accordance with DoD Manual 8910.01, Vol 2, "DoD Information Collections Manual: Procedure for DoD Public Information Collections. ASV is a pilot currently transitioning into a limited production environment while the final budgeting aspects are being established going forward.