Department of Justice
Justice Management Division

Privacy Impact Assessment Addendum
for the
Justice Security Tracking and Adjudication Record System (JSTARS): Next Generation (NextGen)

Issued by:
Morton J. Posner
JMD Senior Component Official for Privacy

Approved by: Jay Sinha
Senior Counsel,
Office of Privacy and Civil Liberties
United States Department of Justice

Date Approved: August 8, 2024

EXECUTIVE SUMMARY

The Justice Security Tracking and Adjudication Record System (JSTARS) Next Generation (NextGen) application will utilize a new version of the Entellitrak case management platform hosted in DOJ's AWS GovCloud. The data collected will remain the same as in the legacy JSTARS application, but the data model stored in the system will be modified. The data model used for the system has changed in that the JSTARS NextGen application utilizes a person base tracked object (BTO) vs. the legacy system which utilized a case base tracked object (BTO). The person tracked object is specific to a named individual, whereas a case tracked object relates to a specific case. Additionally, DOJ applicants will have the ability to directly upload documents into the application. In legacy JSTARS, applicants were required to email those documents to DOJ personnel security specialists, who would then upload the documents into JSTARS. The initial Privacy Impact Assessment (PIA) for JSTARS was approved on May 2, 2008[1], and amended on April 14, 2010[2], December 17, 2011[3], May 7, 2018[4], September 28, 2021[5] and April 28, 2022[6]. This PIA addendum has been prepared because the implementation of JSTARS NextGen will utilize different technology than legacy JSTARS. Unless otherwise indicated in this PIA Addendum, the addition of NextGen incorporates the documented assessments conducted and published in the JSTARS PIA and its addenda.

Section 1: JSTARS Background

JSTARS is a secure, web-based application accessible over the DOJ and public network via DOJ login, which automates the tracking of personnel security investigation activities for the DOJ. JSTARS is primarily used by personnel security staff to process personnel security information and security related requests on employees, contractors, and other personnel processed for fitness, suitability, and eligibility for a security clearance, and/or eligibility to occupy a sensitive position.

DOJ personnel security staff are able to access records within the JSTARS system to review the records and complete personnel security processes including but not limited to: processing pre-employment waivers of prerequisite background investigations; processing reciprocity requests; adjudicating initial background investigations and re-investigations for fitness, suitability and/or eligibility to occupy a sensitive position; and processing security clearances for access to classified national security information[7], sensitive compartmented information[8] access requests,

[1] The JSTARS PIA can be found at: https://www.justice.gov/sites/default/files/jmd/legacy/2014/02/24/pia-jstars-05022008.pdf.
[2] The April 2010 JSTARS PIA Addendum can be found at: https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/06/jstars-pia-addendum.pdf.
[3] The December 2011 JSTARS PIA Addendum can be found at: https://www.justice.gov/sites/default/files/jmd/legacy/2013/09/22/jstars-pia-addendum2.pdf.
[4] The May 2018 JSTARS PIA Addendum can be found at: https://www.justice.gov/JSTARS_iReport/download.
[5] The September 28, 2021 JSTARS PIA Addendum can be found at: https://www.justice.gov/d9/pages/attachments/2021/09/30/jstars_pia_modification_covid_vaccination_attestation_module_updated_v3_final.pdf.
[6] The April 28, 2022 JSTARS PIA Addendum can be found at: https://www.justice.gov/d9/2022-11/2022-04-20_-_jstars_pia_modification_ce_final.pdf.
[7] National security information is information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
[8] Sensitive compartmented information is classified information concerning or derived from intelligence sources, methods, or

and certifying security clearances to other agencies.

Section 2: Description of NextGen and what Information it Provides

JSTARS NextGen is a modernized Personnel Security system that is built on the latest version of Tyler Technology's Application Platform, formally known as Entellitrak. The modernized application will include single sign-on through DOJ Login (OKTA). In addition to single sign-on, access will be controlled through new optimized user roles and organizational hierarchy. The Applicant Portal will allow applicants to submit their PII information safely and securely through the eFile module. This feature provides for one-time data entry and review cycles. The modernized system contains new consolidated case management workflows that have been designed to meet the needs of all JSTARS NextGen users. JSTARS NextGen has many other new features, such as enhanced inboxes, case assignments, Rapid Search, editable correspondence templates, an updated iReport portal, and automated notifications. The JSTARS NextGen system has been designed with usability in mind. There are many new features to help the end user navigate the system and perform their daily tasks.

Section 3: How NextGen Information will be Used and Shared

Information obtained through NextGen will be used in the same manner as legacy JSTARS. JSTARS is a role-based system, in which users must be logged on to the DOJ network to access the system. Within DOJ, only JSTARS users authorized for access to the system and with the appropriate roles will have access to information received via NextGen. Generally, only personnel authorized to make an adjudicative determination on a case will be able to review data within the case. Additionally, authorized users with the appropriate need-to-know, such as background investigators (BI), may also access the information after completing an appropriate BI disclosure acknowledgement.

All the information received will be reviewed by trained personnel security specialists and the appropriate adjudicative guidelines[9] will be applied. Additional investigations or inquiries may be needed to properly address issues that may develop based on the information received. Information may also be disclosed to DOJ personnel with a need-to know to address such issues. The DOJ will follow the process mandated by Executive Order 12968, Access to Classified Information, as amended, or its successor, before any action is taken on an individual's eligibility for access to classified information, or eligibility to occupy a sensitive position. All information sharing will be conducted in accordance with the Privacy Act. Information reporting will be retained in accordance with the Department's System of Records Notice, JUSTICE/DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice, 67 Fed. Reg. 59864 (Sept. 24, 2002); 69 Fed. Reg. 65224 (Nov 10, 2004); and 82 Fed. Reg. 24147 (May 25, 2017).

Additionally, information received from NextGen may be shared with entities as described in the JSTARS PIA and its addenda and the applicable System of Records Notice. Such entities

analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

[9] For example, Security Executive Agent Directive 4, *National Security Adjudicative Guidelines* issued December 10, 2016, which provides the single, common adjudicative criteria for all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.

include, but are not limited to, the Office of Personnel Management or Defense Counterintelligence and Security Agency (DCSA) for clearance verification purposes; other U.S. Government Security offices and their authorized investigators who require investigation and clearance information to allow access to their respective facilities; and other authorized government investigative service providers (e.g., Secret Service, the Department of Homeland Security, the Department of Defense) to conduct requested background investigations.

Section 4: Legal Authorities, Policies, or Agreements

- Public Law 114-113, Title 5 U.S.C. § 11001, *Enhanced Personnel Security Programs (EPSP*), dated December 18, 2015, as amended.
- Continuous Evaluation Implementation Requirements for Fiscal Year 2020, dated December 6, 2019 (issued by ODNI).
- Security Executive Agent Directive (SEAD) 6, *Continuous Evaluation,* issued 12 January 2018.
- Executive Order 13467.
- Executive Order 12968.

Section 5: Privacy Impact

JSTARS currently maintains sensitive background investigation information including personally identifiable information on DOJ employees, contractors, volunteers, consultants, and other individuals whose background investigations are adjudicated by DOJ. The updated data model for NextGen will result in the JSTARS NextGen application utilizing a person based tracked object (BTO) vs. the legacy system which utilized a case based tracked object (BTO). The data collected and stored in the JSTARS NextGen System person based tracked objects include extremely sensitive personal information that is used to make security clearance and suitability determinations for granting and/or revoking a security clearances. This information can include but is not limited to: Full legal name, Social Security Number, Addresses (current and past), marital status, arrest records, legal records, foreign travel, and potentially derogatory personal information. To minimize the risk of unauthorized disclosure or misuse of this background investigation information, the information received will be safeguarded in JSTARS by the same procedures outlined in the existing JSTARS PIA and its addenda. Consistent with the JSTARS PIA and its addenda, in all cases, information will be collected, used, maintained, and disseminated in accordance with the Privacy Act, 5 U.S.C. § 552a.

Individuals will be provided with a Privacy Act Statement stating the reasons for collecting information, the consequences of failing to provide the requested information, and explaining how the information is used. In addition, notice is provided to the public of the existence of this system through System of Records Notices, JUSTICE/DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice, 67 Fed. Reg. 59864 (Sept. 24, 2002); 69 Fed. Reg. 65224 (Nov 10, 2004); and 82 Fed. Reg. 24147 (May 25, 2017).

The integration of NextGen into JSTARS is not expected to have any additional significant privacy risks.