Department of Justice
Justice Management Division

Privacy Impact Assessment Addendum
for the
Justice Security Tracking and Adjudication Record System (JSTARS): Continuous Evaluation (CE) Implementation

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

Approved by: Peter Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date Approved: [April 28, 2022]

EXECUTIVE SUMMARY

Continuous Evaluation (CE) is a personnel security investigative process that leverages technology to perform automated records checks of commercial databases, U.S. Government databases, and other information, in order to continuously review the background of individuals who have been determined eligible for access to classified information or eligibly to occupy a national security position. To meet the requirements of Security Executive Agent Directive (SEAD) 6, *Continuous Evaluation,* the Department is using the Director of National Intelligence's (DNI) Continuous Evaluation System (CES) and the Defense Counterintelligence and Security Agency's (DCSA) Trusted Workforce service. The initial Privacy Impact Assessment (PIA) for the Justice Security Tracking and Adjudication Record System (JSTARS) was approved on May 2, 2008[1], and amended on April 14, 2010[2], December 17, 2011[3], May 7, 2018[4], and August 12, 2021. This PIA addendum has been prepared because the implementation of CE will provide a new mechanism for information to be received into JSTARS[5] as well as additional data and data sources not previously included.

Section 1: JSTARS Background

JSTARS is a secure, web-based application accessible over the DOJ network, 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[6], sensitive compartmented information[7] access requests, and certifying security clearances to other agencies.

Section 2: Description of CE and what Information it Provides

[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] Unless otherwise indicated in this PIA Addendum, the addition of CE incorporates the documented assessments conducted and published in the JSTARS PIA and its addenda.
[6] 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.
[7] Sensitive compartmented information is classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

The Continuous Evaluation (CE) process provides more timely access to information that would typically be obtained during the background investigation process such as information obtained through annual credit checks, quarterly public record checks via commercial databases like Lexis Nexis/Thomson Reuters, daily criminal record checks, and monthly U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) checks. Most of the information received through CE is not new; however, the mechanism for receiving the information and the sending organization is new, and over time, more information will be received through CE than before its implementation. Through a system-to-system connection between the DNI CES[8] and JSTARS, JSTARS will send information for personnel in national security positions to the DNI CES for enrollment and unenrollment in CE. The DNI CES will send CE alerts and reports for enrolled personnel. The DNI CES will also send notification of changes to Scattered Castles records, discussed below, which would result in unenrollment.

In addition, there are some new sources of information that will be available through the CE that were not previously part of the DOJ background investigation process, namely:

- DHS advanced passenger information system (APIS) and border crossing information (BCI): APIS and BCI provide international travel related information for personnel, such as airport codes and dates of travel.

- Terrorist Identities Datamart Environment (TIDE) checks: These checks highlight cases for additional research in the DNI's TIDE system, the U.S. government's central database on known or suspected international terrorists.

- Scattered Castles checks: The Scattered Castles system is an Intelligence Community (IC) personnel security database maintained by the DNI that verifies personnel security access and visit certifications. Scattered Castles is used to perform a validation check for eligibility for enrollment. Currently, an individual must have an active record in Scattered Castles to be enrolled and remain enrolled in CE. When an active record no longer exists, the individual will automatically be un-enrolled from CE.

Additionally, to enroll individuals into the DNI CES, DOJ will import the following additional data elements from the National Finance Center (NFC), which handles DOJ payroll, benefits, and related personnel functions, into JSTARS for federal employees: home address, email address, and gender.

JSTARS may collect, maintain, use, and disseminate personnel security information as described in the JSTARS PIA and its addenda. Such information will include but is not limited to full name; Social Security number; citizenship status; date and place of birth; certain educational records and medical history information; criminal history; employment history; and credit history. JSTARS will also retain a copy of the reports received through CE as part of the individual's security file until the security file is purged.

Section 3: How CE Information will be Used and Shared

Information obtained through CE will be used to supplement the personnel security vetting process. 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 CE. Generally, only

[8] System to system connectivity with the DCSA Trusted Workforce service will be added once it is developed.

personnel authorized to make an adjudicative determination on a case will be able to review the CE 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 (9-24-2002); 69 Fed. Reg. 65224 (11-10-2004); and 82 Fed. Reg. 24147 (5-25-2017).

Additionally, information received from CE may be shared with entities as described in the JSTARS PIA and its addenda and the applicable System of Records Notice. Such entities 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
- ES 2016-00828: *Continuous Evaluation Phase implementation and options for Automated Records Checks*, dated 16 Dec 2016. This memo directed the phased implementation of CE starting in 2017.
- Joint Security and Suitability/Credentialing Executive Agents Executive Communication, *Transforming Federal Personnel Vetting: Continuous Vetting and Other Measures to Expedite Reform and Transition to Trusted Workforce 2.0*, dated January 15, 2021 (U//FOUO)
- Executive Order 13467

[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.

- 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 integration of CE will result in a new method of receiving information on individuals for the purpose of conducting their background investigations, and additional information being added to the security files of these same individuals. 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 (9-24-2002); 69 Fed. Reg. 65224 (11-10-2004); and 82 Fed. Reg. 24147 (5-25-2017).

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