# Department of Justice
# Justice Management Division

**Privacy Impact Assessment Addendum**
for the
Justice Security Tracking and Adjudication Record System (JSTARS): iReport Module

Issued by:
Arthur E. Gary
JMD General Counsel and Senior Component Official for Privacy

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

Date Approved: [May 7, 2018]

# EXECUTIVE SUMMARY

iReport is a module within the Justice Security Tracking and Adjudication Record System (JSTARS). iReport will allow the Department of Justice (DOJ or the Department) to meet its personnel security reporting requirements mandated by the Department Security Officer and the Director of National Intelligence in his capacity as the Security Executive Agent. The initial JSTARS Privacy Impact Assessment (PIA) was approved on May 2, 2008,[1] and amended on April 14, 2010[2] and December 17, 2011.[3] This PIA addendum has been prepared because the iReport module will provide a new mechanism for individuals to provide information in identifiable form into JSTARS.[4]

## 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 used by personnel security staff to process personnel security information and transactions on employees, contractors, and other personnel processed for fitness, suitability, and eligibility for a security clearance, and/or eligibility to occupy a sensitive position.

Personnel security tasks accomplished within JSTARS include, but are not limited to: processing pre-employment waivers of prerequisite investigations; processing reciprocity requests; adjudicating initial background investigations and re-investigations for fitness, suitability and/or eligibility to occupy a sensitive position; and processing National Security Information clearances, Sensitive Compartmented Information access requests, and clearance certifications. JSTARS is currently used by all components of the Department.

## Section 2: Description of iReport and what Information it Collects

iReport is a module within JSTARS that will enable the DOJ workforce to self-report as mandated by DOJ Policy Statement 1700.04 *Department Personnel Security Reporting Requirements* signed by the Department Security Officer on April 16, 2018. [redacted]

[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] Unless otherwise indicated in this PIA Addendum, the iReport module incorporates the documented assessments conducted and published in the JSTARS PIA and its addenda.

Individuals who have undergone ther prerequisite security vetting to work in the Department will will access iReport through a webpage placed on DOJ components' respective intranet sites.

Upon clicking on the iReport webpage link, users will be asked to provide their last name, the last five digits of their Social Security Account Number (SSN), and their date of birth. This information is required in order for JSTARS to upload the self-report into the correct JSTARS security case file relating to the reporting individual. Individuals submitting a report will need to enter this information for themselves whether they are self-reporting or reporting on someone else. They will not be required to report any personally identifiable information on individuals for whom they may report.

iReport 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; SSN; citizenship status; date and place of birth; educational records; medical history; criminal history; employment history; and credit history.

Users will utilize the system to submit self-reports online instead of emailing or otherwise sending a report to their Security Programs Manager.

## Section 3: How iReport Information will be Used and Shared

**Self-reported information:** The information required to be self reported depends on the individual's position sensitivity level. All information is entered into the system by the indivudial filing the report. They may also upload supporting documents to their submittal. All the information received will be reviewed by trained personnel security specialists and the adjudicative guidelines[5] will be applied. Additional investigations may be needed to properly address issues that may develop based on the received information. 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, or eligibility to occupy, a sensitive position. Any other information sharing will be in accordance with the Privacy Act. Information reporting will be retain in accordance with the Department's System of Records Notice, included but not limited to 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).

**Third party information:** If there is information in the individual's report submission that pertains to other covered personnel, such information will be evaluated and could possibly be incorporated into the other covered individual's security file, as appropriate.

[5] Security Executive Agent Directive 4, National Security Adjudicative Guidelines issued December 10, 2016, provides the single, common adjudicative criteria for all covered individual who require initial or continued eleigibility for access to classified information or elgibility to hold a sensitive position. It supersedes all previously issued national security adjudicative criteria or guidelines.

Information received from an iReport may be shared with entities as described in the JSTARS PIA and its addendums. Such entities include, but are not limited to, the Office of Personnel Management 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

- Department of Justice Policy Statement 1700.04 *Department Personnel Security Reporting Requirements*, April 16, 2018.
- Security Executive Agent Directive (SEAD) 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*, issued December 14, 2016.
- Intelligence Community Standard (ICS) 703-02, *Reporting Requirements for Individuals with Access to SCI*, issued August 11, 2016;

## 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 iReport will result in a new medium of collecting information from individuals regarding their background investigations, and additional information being received and added to the security file of these same individuals. The information received will be safeguarded in JSTARS on these individuals by the same procedures outlined in the existing JSTARS PIA and its addenda. Consistent with the JSTAR 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 (2012). 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 explains how the information is used. In addition, notice is provided to the public of the existing of this system through System of Records Notices, included but not limited to 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 iReport into JSTARS will likely have no further significant adverse privacy risks.