Privacy Impact Assessment
for the

Justice Security Tracking and Adjudication Record System

May 2, 2008

Responsible Officials
David Todd
JSTARS Project Manager
Anna Harrison, Data Owner
Assistant Director Personnel Security Group
Dorianna Rice, User Representative
Chief of Operations Section, Personnel Security Group
(202) 514-2351

Reviewing Official
Vance Hitch
Chief Information Officer
Department of Justice
(202) 514-0507

Approving Official
Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer
Department of Justice
(202) 514-0208

INTRODUCTION

The Justice Security Tracking and Adjudication Record System (JSTARS) automates the tracking of personnel security investigation activities for the Department of Justice (DOJ). The purpose of JSTARS is to enable the DOJ Security and Emergency Planning Staff (SEPS), Personnel Security Group (PERSG) to store and manage DOJ personnel security information. In addition, JSTARS will allow PERSG to manage the integrated workflow process, management activities, caseloads, and reporting capabilities relating to personnel security investigations. Information contained within JSTARS includes: pre-employment waivers, background investigations (BIs), security clearances, SCI access, clearance receipts (reciprocity), reinvestigations, completion dates of various security checks, and adjudication status. Other information contained within JSTARS may include adjudication notes, decisions, employment records, education history, credit history, the subject's previous addresses, friends and associates, selective service records, military history, and citizenship.

Section 1
The Information Collected and Stored

What information is to be collected

The personally identifiable information (PII) collected consists of data elements necessary to identify the individual and to track completion of security related processes including background or other investigations concerning the individual. The system has been designed to closely align with PERSG's business practices.

JSTARS collects and maintains the following personally identifiable information which may be developed during the security investigation, including but is not limited to:

- Full Name
- Social Security No.
- Citizenship Status
- Date of Birth
- Place of Birth
- Educational Records
- Medical History
- Criminal History
- Mother's Maiden Name
- Employment History
- Credit History

JSTARS collects and maintains these essential data elements about each individual:

- Employee Type
- Organization
- Position Title
- Position Sensitivity
- Access Level
- SSN
- Granting Authority Contact

- Granting Authority Code
- Eligibility Level
- Record Type
- Eligibility Date / Adjudication Date
- Subject's Full Name
- Date of Birth
- Place of Birth (City / State / Country)
- Eligibility Exception (Conditions, Waivers, and Deviations)
- Clearance Type (Interim / Final)
- SCI Access Level (SCI, SAP, SCISAP, Not Eligible) & Approval Date
- Standard Code (indicating standard used to determine eligibility)
- Status Code (Status of the Clearance Eligibility)
- NSI Clearance Levels

From whom is the information collected?

Information is collected directly from DOJ applicants, employees, contractors, consultants, student interns, visitors, and others who require access to DOJ facilities and/or information systems. Several required forms are used to initiate the background investigation: Questionnaire for Non-Sensitive Positions Standard Form 85 (SF-85), Questionnaire for Public Trust Positions (SF-85P), Supplemental Questionnaire for Selected Positions (SF-85P-S), and Questionnaire for National Security Positions 86 (SF-86). Personally identifiable information is provided by the individual when completing the security form electronically through a system called e-QIP, a new system developed by the OPM to meet the Presidential Management Agenda for the e-Clearance module. It is an identical automated copy of the paper security forms. The SF 86, SF85P, and the SF85 are all available in e-QIP. At times the same PII may be collected from the individual through a paper security form identical to the e-QIP questionnaire. PERSG receives the information about the individual and enters it into JSTARS. The information collected in the security form is used by OPM and FBI investigators to conduct the necessary background investigations. Additional information may also be collected directly from the applicant by the investigator, or Security Program Manager/designee.

Section 2
Purpose of the System and the Information Collected

2.1 Why is the information being collected?

The basic personally identifiable information outlined above is used to create a record in JSTARS which tracks the ongoing security investigation and determination process. The information collected in

the security form is used by OPM and FBI investigators to conduct the necessary background investigations. Records are used to determine the loyalty, trustworthiness, suitability, eligibility and/or qualifications of employees for initial or continued employment in the Department of Justice, and for eligibility and continued eligibility for access to classified information. The records are also used to make similar suitability and security determinations regarding the employment of contractors to perform a service for the Department, to establish the trustworthiness for access to classified information of persons associated with and/or acting for the court or the defense during criminal proceedings, or in other specified cases where individuals employed by or performing services for the Federal Government require background investigations, including during Presidential transitions. Records in this system are also used by the Access Review Committee (ARC) when an appeal is made to the ARC to review a security clearance denial or revocation pursuant to E.O. 12968. Records in this system are also used to manage and track the status and types of investigations, the dates of clearances, and level of clearances.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

Depending on the type of investigation required, Executive Orders 10450, 10865, 12333, and 12968 provide the basis for collecting information regarding personnel security investigations for Positions of Public Trust, National Security Positions, and suitability.

Privacy Impact Analysis:

Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Collecting PII directly from the individual minimizes the risk of error. When possible, PII is entered by the individual when completing the required electronic security form through e-QIP, which is accessed through a secure portal hosted by the U.S. Office of Personnel Management. At times the same PII may be collected through a paper security form identical to the e-QIP questionnaire. PERSG receives the information about the individual and enters it into JSTARS. In order to minimize unauthorized access to or misuse of the information, access controls, training, and audit mechanisms have been put in place to ensure appropriate use of the information within the system.

In order to mitigate the risk of JSTARS and its information being improperly accessed or misused, the PERSG has put in place both technical safeguards and training. Access to the JSTARS system requires access to the DOJ internal network. JSTARS user accounts are individually approved by the Personnel Security Group Assistant Director (PERSG AD) or designee before any user is allowed to access the system. All users have received DOJ Computer Security training and have been vetted and cleared for access to PII, sensitive information. Access to JSTARS is role-based and data access for users of the system is limited to the minimum access needed to perform their respective functions. The capability to update information is restricted to those roles that specifically require this to perform their duties and record changes are tracked and audited through the use of transaction history tracking which provides information on data changes made and the specific user who made the change.

Section 3
Uses of the System and the Information

3.1 Describe all uses of the information.

The information collected in the security form is used by OPM and FBI investigators to conduct the necessary background investigations. The records in this system will be used for tracking all personnel security information related processes for the individual during his or her tenure with DOJ.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

No. This system is used to track security investigation information and related processes. There are no in-built data analysis functions to identify patterns or new areas of concern.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

As part of the application process, the individual is required to provide his or her PII and background information. PERSG receives the information about the individual and enters it into JSTARS. The individual's PII information is verified during the BI. Additionally, the individual's name and social security number is compared with information provided by the National Finance Center (NFC), the payroll processing center for the DOJ. If any PII differs in JSTARS from that within the BI then, that data is corrected.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

DOJ personnel security records relating to individuals are retained and disposed of in accordance with NARA General Records Schedule 18, item 22a and 22c, 23, 24 and 25.

Privacy Impact Analysis:

Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

All PERSG personnel are briefed on the use and protection of Privacy Act data as per the DOJ BI Disclosure Policy. Individual privacy data is only shared outside of the DOJ in accordance with DOJ Privacy Act routine use notification published in the Federal Register. Individual records are kept in

accordance with NARA General Records Schedule 18 as required. It should also be noted that system audit logs are frequently monitored for inappropriate user behavior.

Section 4
Internal Sharing and Disclosure of Information

4.1 With which internal components of the Department is the information shared?

The information is shared with the appropriate Department employees and contractors that require access to the information to facilitate the investigation and adjudication of personnel. This includes PERSG, all DOJ Component (Bureaus, Offices, Boards and Divisions), Security Program Managers (SPM) and DOJ Investigative Offices. PERSG personnel are, by law, bound by the Privacy Act. Specific information about an individual will be shared with Department employees and its contractors who have a "need to know".

4.2 For each recipient component or office, what information is shared and for what purpose?

Each DOJ Component Security Programs Manager and/or designee only has access to information pertaining to the personnel in their group. For example, components can only see data on those individuals working in their respective component. PERSG is the only office that has access to all the information contained within JSTARS and even then that view is constrained by the user's Role membership.

4.3 How is the information transmitted or disclosed?

Access to the information is via a secure authenticated web interface. Access control is based upon Role membership. Data is only accessible once the user has been approved for membership to a Role that has been granted access to the specific data types. Information presented on screens is based on specific roles and information required to facilitate those functions.

Privacy Impact Analysis:
Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

This information is shared with other parts of DOJ based on their need-to-know. The following are in place to mitigate the risk:

- Access to JSTARS requires an active DOJ domain account and that the user be logged into a DOJ domain accessible computer.
- All JSTARS users have received DOJ Computer Security training and have been vetted and cleared for access to sensitive and privacy information.

- Access to JSTARS is Role based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access.
- Write capability to system records is tracked and audited.
- A comprehensive set of Management, Operational, and Technical controls are documented in the System Security Plan and have been tested in conjunction with the FISMA Certification and Accreditation process.

Section 5
External Sharing and Disclosure

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Clearance information is uploaded to the OPM Clearance Verification System (CVS) data using OPM's "Extranet Service Portal" (ESP). ESP is maintained and hosted by OPM's Federal Investigative Services Division (FISD). This information is hosted in a secure facility approved for storage of secure government data. In addition, information is also shared with other U.S. Government Security offices and their authorized investigators who require investigation and clearance information to allow access to their respective facilities. Other authorized government investigators (e.g., Secret Service, DHS, Energy, OPM) may receive access to JSTARS records when conducting requested background investigations.

5.2 What information is shared and for what purpose?

JSTARS shares the following personally identifiable information:

- Employee Type
- Organization
- Position Title
- Position Sensitivity
- Access Level
- SSN
- Granting Authority Contact
- Granting Authority Code
- Eligibility Level / Adjudication Date
- Record Type
- Eligibility Date
- Subject's Full Name
- Date of Birth

- Place of Birth (City / State / Country)
- Eligibility Exception (Conditions, Waivers, and Deviations)
- Clearance Type (Interim / Final)
- SCI Access Level (SCI, SAP, SCISAP, Not Eligible) & Approval Date
- Standard (Code indicating standard used to determine eligibility)
- Status Code (Status of the Clearance Eligibility)
- Non-U.S. Immediate Family Member(s)
- NSI Clearance Levels

5.3 How is the information transmitted or disclosed?

Information is transmitted either through the secure OPM CVS Extranet Service Portal, by FAX or in person. OPM requires that each agency report adjudication decisions in a timely manor. PERSG personnel currently use OPM form OF 79a to report all adjudicative decisions. This form can be updated on line through the OPM Personnel Investigations Processing System (PIPS) via the OPM secure extranet service Portal.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

No, sharing of personnel security information is legally mandated under Executive Order 12958 (as amended) and is in accordance with appropriate routine uses under the Privacy Act.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

The Government requires personnel be trained in the handling of clearance and privacy data.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

No, there are no such provisions or agreements in place.

Privacy Impact Analysis:

Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The privacy risk is that PII and in particular a Social Security Number may be exposed and associated with an individual's name and date of birth as well as their clearance level and organization. The following are in place to mitigate the risk:

- There are no direct data interfaces: a person must create a data extract and transfer the data via secure transport method(s)
- Access to data is role based
- Personnel receive security training before being granted privileges to handle sensitive information

Section 6
Notice

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

In all cases, individuals are provided a notice required by the Privacy Act, 5 USC 552(a). The privacy statement, as required by the Privacy Act, 5 USC 552(a)(e)(3) states the reasons for collecting information, the consequences of failing to provide the requested information, and explains how the information is used. (See Appendix A of this document to view OPM SF-85 & SF-86 security statements.)

In addition, notice is provided through the following, System of Records Notice:

- DOJ Personnel Investigation and Security Clearance Records for the Department of Justice (DOJ-006).
- First recorded in the Federal Register September 24, 2002 in Volume 67 from pages 59864-59867)
- Twice amended
  - November 10, 2004 in Volume 69, page 65224
  - January 25, 2007 in Volume 72, pages 3410-3414

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Providing information is required in order to work for the Department. Individuals who opt not to provide information cannot meet suitability requirements and are therefore ineligible for Federal service. Furthermore, they are ineligible to serve a role as a government contractor at the DOJ.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Individuals are required to sign authorization forms as part of their completion of the Questionnaire for Non-Sensitive Positions (OPM SF-85), the Questionnaire for Public Trust Positions (OPM SF-85P) or the Questionnaire for National Security Positions (OPM SF-86). These authorization forms may consist of the following: (1) a general authorization to obtain information relating to the applicant's activities from individuals, schools, residential management agents, employers, criminal justice agencies, and other sources of information; (2) a specific authorization to obtain certain medical information; and (3) a specific authorization to obtain consumer/credit reports. Copies of these authorization forms are attached.

Privacy Impact Analysis:

Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Individuals are provided notice of the information collection on the forms provided to them prior to submission of their data. Additionally, the System of Records Notice and this PIA provide additional notice of the collection, use, maintenance, and dissemination of the personally identifiable information.

Section 7
Individual Access and Redress

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

JSTARS stores an individual's PII, personnel security process tracking dates and information, security determinations, as well as imaged copies of respective background investigations. The PII is self-reported by the individual undergoing the investigation when they submit their completed SF-85, SF-85P, SF-85PS or SF-86 form. Once that data has been submitted to JSTARS for suitability review and clearance processing by PERSG, individuals may contact PERSG directly or through their SPM to request correction of any erroneous PII.

Each Subject has the ability to address and provide mitigating information related to any derogatory information that is identified as part of his/her background investigation. Subjects are notified of any pending actions based on derogatory information and are provided a mechanism to provide resolution information. If a derogatory finding is made, they have appeal rights.

Individuals seeking access to records contained in JSTARS should submit an access request through the DOJ Freedom of Information Act (FOIA) office at the following address:

U.S. Department of Justice
Justice Management Division
Attention: FOIA Staff

950 Pennsylvania Avenue, N.W.
Room 1111, RFK
Washington, DC 20530-0001
(202) 514-3101

Individuals who specifically seek access to a copy of their completed background investigative report should submit an access request to the agency (i.e., OPM or FBI) that conducted the background investigation, at the appropriate following address:

FBI FOIA/PA
JEH Building
935 Pennsylvania Ave., N.W.
Washington, D.C. 20535-0001

OPM
Federal Investigations Processing Center
FOIA/PA
PO Box 618
Boyers, PA 16018-0618

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

The specific procedures depend on the findings and the type of case. Subjects are notified in writing when DOJ is prepared to make a derogatory finding based on the information at hand.

The written notice advises the Subject of the mechanism for addressing the derogatory information. The individual will be notified based on a review of their response whether the derogatory information will result in a change to their clearance status. If their clearance is denied, suspended or revoked, they will be notified in writing and be provided with the specific information regarding their appeal rights and due process. Additionally instructions are provided on related security forms regarding changes or updates to data that may be required after submission. The Privacy Act Systems of Records Notice and DOJ regulations also provide notice of such procedures.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

N/A

Privacy Impact Analysis:

Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

Justice Security Tracking and Adjudication Record System uses standard Privacy Act access and correction procedures to ensure individuals can contest information used within the system for adjudication purposes and thus ensure correct and accurate information is held within the system.

Section 8
Technical Access and Security

8.1 Which user Roles(s) will have access to the system?

Below is a list of the Roles as defined under the current JSTARS System Design Document. These roles may be modified or the list updated as processes change and new organizations begin to use the system. Any future requests for the creation of new Roles will be presented to the JSTARS Change Control Board for disposition prior to implementation.

○ No Access ⭘Read Only ●Read / Edit	Case	Employment	Investigation	Clearance	SCI Access Ticket	Certification	Processing Activity	Analysis / Design	Reason Code	Briefing	Briefing Ticket	Review	Correspondence	Citizenship	Alias	Document	Transactions	Case Log	Routing	Inventory	NFC Update
Clerk	●	●	●	●	●	●	●	○	○	○	○	○	○	●	●	●	⭘	⭘	●	⭘	⭘
Security Assistant	⭘	⭘	⭘	⭘	⭘	●	●	●	○	○	○	○	●	⭘	⭘	⭘	⭘	⭘	●	⭘	⭘
Specialist	●	●	●	●	●	●	●	●	●	●	●	⭘	●	●	●	●	⭘	⭘	●	●	⭘
Supervisor	●	●	●	●	●	●	●	●	●	●	●	⭘	●	●	●	●	⭘	⭘	●	●	⭘
Assistant Directory	●	●	●	●	●	●	●	●	●	●	●	⭘	●	●	●	●	⭘	⭘	●	●	⭘
Deputy Director	●	●	●	●	●	●	●	●	●	●	●	⭘	●	●	●	●	⭘	⭘	●	●	⭘
DSO	●	●	●	●	●	●	●	●	●	●	●	⭘	●	●	●	●	⭘	⭘	●	●	⭘
Admin	●	●	●	●	●	●	●	●	●	●	●	⭘	●	●	●	●	⭘	⭘	●	●	⭘
SCI Admin	⭘	⭘	⭘	●	●	⭘	⭘	⭘	●	●	⭘	⭘	⭘	●	⭘	⭘	⭘	⭘	●	⭘	⭘
CVS Admin	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘
NFC Admin	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	●
Authorized Reviewer	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘	⭘

JSTARS Access Roles

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Only contractors that provide direct support to PERSG will have full access to the system. Secondary users (DOJ Component Security Program Managers (SPM) and DOJ Investigative Offices and their approved contractors) only receive access to the data that pertains to personnel in their employment. DOJ requires, through legal agreements, that all its contractors abide by the department's policies regarding the handling and transmittal of personally identifiable information.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, the level of a user's access (what they can do & how much they can see, what reports they can run) is determined by which Role they are assigned.

8.3 What procedures are in place to determine which users may access the system and are they documented?

Access to JSTARS is primarily limited to PERSG personnel, with secondary users being all DOJ Component Security Program Managers (SPM), Hiring Officers, DOJ Investigative Offices.

Request for access must be approved by the requesting component supervisor and submitted to the PERSG AD and/or their designee. User access requests are reviewed, approved or denied on an individual basis. The requesting component is informed of the outcome within 1 to 2 business days of submittal. Role memberships are based upon the user's job function and need-to-know. Requests are submitted to the PERSG AD either by email or facsimile. In either case the JSTARS access is retained as an official record.

8.4 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Role membership is based upon the user's job function and need-to-know.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Audit logs are reviewed by the Application Administrator on a weekly and monthly basis. Indications of inappropriate behavior are reported to the PERSG AD for further review and disposition.

8.6 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All DOJ employees and contractor staff receive annual computer security awareness training, and have undergone the necessary background investigations and/or security clearances for access to sensitive information. All PERSG personnel are briefed on the use and protection of PII data.

8.7 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Certification and Accreditation of the JSTARS system is currently underway. Full accreditation should be granted to JSTARS by June 2008.

Privacy Impact Analysis:

Given access and security controls, what privacy risks were identified and describe how they were mitigated.

While limited risk of PII exposure remains, the steps below have been taken to mitigate that risk:

- Access to JSTARS requires a DOJ domain account and requires that the user be logged into a DOJ A LAN computer
- JSTARS user accounts are individually approved by DOJ PERSG AD or designee before they are created
- All users have received DOJ Computer Security training and have been vetted and cleared for access to sensitive and privacy information
- Access to JSTARS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access
- Write capability is limited, tracked and audited
- Information transmitted to external Government entities contains the least amount of PII information possible
- JSTARS is currently undergoing the Certification and Accreditation (C&A) criteria required of a system hosting privacy data

Section 9
Technology

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Multiple detailed proposals were obtained from vendors regarding the JSTARS project.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

A Statement of Work (SOW) was developed with input and consensus from the stakeholders. The SOW contained the necessary system and security requirements. Submitted proposals were reviewed during the source selection process. Each proposal was evaluated against several criteria including how well they demonstrated an understanding of the established security requirements.

9.3 What design choices were made to enhance privacy?

- Secure encrypted communication (HTTP / SSL) between the client and the server
- Not accessible through the Internet
- Not available to VPN or Dial-up users
- The application is only accessible internally from DOJ JMD network
- Access to JSTARS requires a DOJ domain account and requires that the user be logged into a DOJ A LAN computer

- JSTARS user accounts are individually approved by PERSG AD before they are provisioned
- Access to JSTARS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access
- Write capability is tracked and audited
- External users are transmitted the least information possible

Conclusion

The Justice Security Tracking and Adjudication Record System was developed and designed by the Department of Justice to accurately store, track, retrieve and create personnel security records electronically (i.e. Background Investigations, Security Clearances, etc). JSTARS equipment is hosted in a secured DOJ facility and physical access to these devices is limited to support and administrative personnel.

Access to JSTARS data is based on the concept of the least privilege principle. Each Role is granted only the rights and privileges necessary to allow users to perform their job function and meet their need to know. User accounts are individually approved by the PERSG Assistant Director and/or designee prior to being granted access to the system. All DOJ personnel requiring access to JSTARS have been vetted and, at a minimum, cleared for access to sensitive information.

JSTARS is only available to approved users directly connected to the DOJ network; Internet, VPN and Dial-up connectivity to JSTARS is not permitted and is blocked by system boundary devices. While JSTARS has no direct connections to other systems, periodically PII data is uploaded to the OPM Clearance Verification System (CVS). However, the information is securely transmitted and contains the least amount of PII possible.

Signatures Page

Responsible Officials

☒ Recommend
☐ Not Recommend

/S/
David Todd
JSTARS Project Manager
Date:

☒ Recommend
☐ Not Recommend

/S/
Dorianna Rice, User Representative
Chief of Operations Section, Personnel Security Group
Date:

☒ Recommend
☐ Not Recommend

/S/
Anna Harrison, Data Owner
Assistant Director Personnel Security Group
Date:

Reviewing Official

☒ Recommend Approve
☐ Recommend Not Approve

/S/
Vance Hitch
Chief Information Officer
Date:

Approving Official

☒ Approved
☐ Not Approved

/S/
Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer
Date: 5/2/08

Appendix A

Office of Personnel Management
Security Form Privacy Act Notice(s)

Excerpt taken from:
Office of Personnel Management Standard form SF-85
Revised September 1995; 5 CFR Parts 731 and 736
OMB No. 3206-0005
https://www.opm.gov/forms/pdf_fill/SF85.pdf

* Begin Excerpt

"The U.S. Government conducts background investigations to establish that applicants or incumbents either employed by the Government or working for the Government under contract, are suitable for the job. Information from this form is used primarily as the basis for this investigation. Complete this form only after a conditional offer of employment has been made.

Giving us the information we ask for is voluntary. However, we may not be able to complete your investigation, or complete it in a timely manner, if you don't give us each item of information we request. This may affect your placement or employment prospects.

Authority to Request this Information The U.S. Government is authorized to ask for this information under Executive Order 10577, sections 3301 and 3302 of title 5, U.S. Code; and parts 5, 731, and 736 of Title 5, Code of Federal Regulations.

Your Social Security Number is needed to keep records accurate, because other people may have the same name and birth date. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

The Investigative Process Background investigations are conducted using your responses on this form and on your Declaration for Federal Employment (OF 306) to develop information to show whether you are reliable, trustworthy, and of good conduct and character. Your current employer must be contacted as part of the investigation, even if you have previously indicated on applications or other forms that you do not want this."

UNITED STATES OF AMERICA AUTHORIZATION FOR RELEASE OF INFORMATION

Carefully read this authorization to release information about you, then sign and date it in black ink. I Authorize any investigator, special agent, or other duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain any information relating to my activities from schools, residential management agents, employers, criminal justice agencies, retail business establishments, or other sources of information. This information may include, but is not limited to, my academic, residential, achievement, performance, attendance, disciplinary, employment history, and criminal history record information.

I Understand that, for some sources of information, a separate specific release will be needed, and I may be contacted for such a release at a later date.

I Authorize custodians of records and sources of information pertaining to me to release such information upon request of the investigator, special agent, or other duly accredited representative of any Federal agency authorized above regardless of any previous agreement to the contrary.

I Understand that the information released by records custodians and sources of information is for official use by the Federal Government only for the purposes provided in this Standard Form 85, and may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for two (2) years from the date signed.

* End Excerpt

Excerpt taken from:
Office of Personnel Management Standard Form 85P Revised September 1995
5 CFR Parts 731, 732, and 73
OMB No. 3206-0191
https://www.opm.gov/forms/pdf_fill/SF85P.pdf

* Begin Excerpt

Purpose of this Form

"The U.S. Government conducts background investigations and reinvestigations to establish that applicants or incumbents either employed by the Government or working for the Government under contract, are suitable for the job and/or eligible for a public trust or sensitive position. Information from this form is used primarily as the basis for this investigation. Complete this form only after a conditional offer of employment has been made.

Giving us the information we ask for is voluntary. However, we may not be able to complete your investigation, or complete it in a timely manner, if you don't give us each item of information we request. This may affect your placement or employment prospects.

Authority to Request this Information

The U.S. Government is authorized to ask for this information under Executive Orders 10450 and 10577, sections 3301 and 3302 of title 5, U.S. Code; and parts 5, 731, 732, and 736 of Title 5, Code of Federal Regulations.

Your Social Security number is needed to keep records accurate, because other people may have the same name and birth date. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

The Investigative Process

Background investigations are conducted using your responses on this form and on your Declaration for Federal Employment (OF 306) to develop information to show whether you are reliable, trustworthy, of good conduct and character, and loyal to the United States. The information that you provide on this form is confirmed during the investigation. Your current employer must be contacted as

part of the investigation, even if you have previously indicated on applications or other forms that you do not want this."

UNITED STATES OF AMERICA AUTHORIZATION FOR RELEASE OF MEDICAL INFORMATION

Carefully read this authorization to release information about you, then sign and date it in black ink. Instructions for Completing this Release.

This is a release for the investigator to ask your health practitioner(s) the three questions below concerning your mental health consultations. Your signature will allow the practitioner(s) to answer only these questions.

I am seeking assignment to or retention in a position of public trust with the Federal Government as a (n)

As part of the investigative process, I hereby authorize the investigator, special agent, or duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain the following information relating to my mental health consultations:

Does the person under investigation have a condition or treatment that could impair his/her judgment or reliability?

If so, please describe the nature of the condition and the extent and duration of the impairment or treatment.

What is the prognosis?

I understand that the information released pursuant to this release is for use by the Federal Government only for purposes provided in the Standard Form 85P and that it may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for 1 year from the date signed or upon termination of my affiliation with the Federal Government, whichever is sooner.

* End Excerpt.

Excerpt taken from:
Office of Personnel Management Standard Form 86 Revised September 1995
OMB No. 3206-0007
5 CFR Parts 731, 732, and 736
https://www.opm.gov/forms/pdf_fill/SF86.pdf

* Begin Excerpt

"Purpose of this Form

The U.S. Government conducts background investigations and reinvestigations to establish that military personnel, applicants for or incumbents in national security positions, either employed by the Government or working for Government contractors, licensees, certificate holders, and grantees, are

eligible for a required security clearance. Information from this form is used primarily as the basis for investigation for access to classified information or special nuclear information or material. Complete this form only after a conditional offer of employment has been made for a position requiring a security clearance.

Giving us the information we ask for is voluntary. However, we may not be able to complete your investigation, or complete it in a timely manner, if you don't give us each item of information we request. This may affect your placement or security clearance prospects.

Authority to Request this Information

Depending upon the purpose of your investigation, the U.S. Government is authorized to ask for this information under Executive Orders 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; and parts 5, 732, and 736 of Title 5, Code of Federal Regulations.

Your Social Security number is needed to keep records accurate, because other people may have the same name and birth date. Executive Order 9397 also asks Federal agencies to use this number to help identify individuals in agency records.

The Investigative Process

Background investigations for national security positions are conducted to develop information to show whether you are reliable, trustworthy, of good conduct and character, and loyal to the United States. The information that you provide on this form is confirmed during the investigation. Investigation may extend beyond the time covered by this form when necessary to resolve issues. Your current employer must be contacted as part of the investigation, even if you have previously indicated on applications or other forms that you do not want this.

In addition to the questions on this form, inquiry also is made about a person's adherence to security requirements, honesty and integrity, vulnerability to exploitation or coercion, falsification, mis-representation, and any other behavior, activities, or associations that tend to show the person is not reliable, trustworthy, or loyal."

UNITED STATES OF AMERICA AUTHORIZATION FOR RELEASE OF MEDICAL INFORMATION

Carefully read this authorization to release information about you, then sign and date it in black ink. Instructions for Completing this Release.

This is a release for the investigator to ask your health practitioner(s) the three questions below concerning your mental health consultations. Your signature will allow the practitioner(s) to answer only these questions.

I am seeking assignment to or retention in a position of public trust with the Federal Government as a (n)

As part of the investigative process, I hereby authorize the investigator, special agent, or duly accredited representative of the authorized Federal agency conducting my background investigation, to obtain the following information relating to my mental health consultations:

Does the person under investigation have a condition or treatment that could impair his/her judgment or reliability?

If so, please describe the nature of the condition and the extent and duration of the impairment or treatment.

What is the prognosis?

I understand that the information released pursuant to this release is for use by the Federal Government only for purposes provided in the Standard Form 85P and that it may be redisclosed by the Government only as authorized by law.

Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for 1 year from the date signed or upon termination of my affiliation with the Federal Government, whichever is sooner.

* End Excerpt

Excerpt taken from:
United States Department of Justice Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act (Title 15, U.S. Code, Section 1681)
Revised September 1997
Form DOJ - 555

This is a release for the Department of Justice to obtain one or more consumer/credit reports about you in connection with your application for Federal employment, during the course of your Federal employment (including employment under contract), and/or in connection with your security clearance or your access to classified information. One or more reports about you may be obtained for purposes of evaluating your fitness for employment, promotion, reassignment, retention, access to classified information, or other employment purposes.

I, _____, hereby authorize the Department of Justice to obtain, and I further instruct any consumer/credit reporting agency to release to DOJ, any such report(s) for the above purposes.