Privacy Impact Assessment

Name of Project: Security Clearance Tracking System (SCTS)
Project's Unique ID:

Legal Authority(ies): Privacy Act, 5 U.S.C. 552a

Purpose of this System/Application: The NARA Security Clearance Tracking System (SCTS) will track all background investigations or security investigations for all NARA employees, contractors, foundation staff, and unpaid interns.

Section 1: Information to be Collected

1. Describe the information (data elements and fields) available in the system in the following categories:

a. Employees. Full Name; Date of Birth; Place of Birth; Title; Grade; Office Symbol; Sensitivity of position; Risk level of position; Investigation Type; Agency doing the investigation; Date Submitted to Office of Personnel Management (OPM) for investigation; Date completed by OPM; Access Level of Clearances; Date granted; date briefed (if required) and debrief date (if required).

b. External Users: Micropact will host the Server in Herndon, VA.

c. Audit trail information (including employee log-in information) Yes

d. Other: N/A

e. Other third party source: None

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?

a. **NARA operational records.** As stated in Section 1.1 along with documents for NARA's HR department.

b. **External users.** N/A

c. **Employees.** All Security Management Division (BX) personnel will have access to the system.

d. **Other Federal agencies (list agency).** Office of Personnel Management (OPM)

e. **State and local agencies (list agency).** None

f. Other third party source. <u>None</u>

Section 2: Why the Information is Being Collected

1. **Is each data element required for the business purpose of the system? Explain.** Each element is relevant to individual at NARA for their background investigation or their security investigation.

2. **Is there another source for the data? Explain how that source is or is not used?** No

Section 3: Intended Use of this Information

1. **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?** No.

2. **Will the new data be placed in the individual's record?** Yes

3. **Can the system make determinations about employees/the public that would not be possible without the new data?** No

4. **How will the new data be verified for relevance and accuracy?** By BX personnel users.

5. **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?** All data will be housed on a secure server, which has met NARA's IT security requirements.

6. **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.** Yes, the hosted solution has received an Authority to Operate following a Certification and Accreditation by NARA IT security.

7. **Generally, how will the data be retrieved by the user?** All data will be on a secure server and NASS personnel will have log ons and passwords to retrieve data.

8. **Is the data retrievable by a personal identifier such as a name, SSN or other unique identifier? If yes, explain and list the identifiers that will be used to retrieve information on an individual.** Yes. The personal identifier can be last name, SSN or first name.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?** The system will allow reports

regarding employee security clearances, which will be used to identify when an employee needs an update to the employee's background investigation or security clearance.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain. No

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain. No

12. What kinds of information are collected as a function of the monitoring of individuals? We are NOT monitoring individuals.

13. What controls will be used to prevent unauthorized monitoring? We are NOT monitoring.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors? n/a

Section 4: Sharing of Collected Information

1. Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)? All BX personnel, and three Micropact Contractors.

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.).

The BX Systems Administrator determines who uses the system. The system documents everyone's use.

3. Will users have access to all data on the system or will the user's access be restricted? Explain. Only three BX personnel will have full access and others will have limited access.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)? All individuals will be required to have a unique log in and password to the secure site.

5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures

addressed? Yes.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. If no, continue to question 7. No.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment? N/A

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface? Micropact

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used. No.

Section 5: Opportunities for Individuals to Decline Providing Information

1. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent? None.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not applicable.

Section 6: Security of Collected Information

1. How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.).

   a. Data is inputted by BX personnel. It is their responsibility to ensure it is accurate. There is no timeliness, only completeness when a background investigation or security investigation is complete.

2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites? The server is hosted off site and all users will be using the internet through a secure website.

3. What are the retention periods of data in this system? Same as the File 203 manual states for personnel files. Once an individual leaves, the data will remain in the server but the employee is designated as inactive.

4. **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Cite the disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled that cannot be destroyed or purged until the schedule is approved.** See question 3, above.

5. **Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe.** No

6. **How does the use of this technology affect public/employee privacy?** The technology automates a business process, making it more efficient with few risks of human error.

7. **Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?** Yes

8. **Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information?** Yes, no risks were identified.

9. **Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.** Yes, this was part of the risk assessment.

10. **Identify a point of contact for any additional questions from users regarding the security of the system.**

Paula L. Ayres (NASS)
Personnel Security Officer
Paula.ayres@nara.gov
301-837-1494

Section 7: Is this a system of records covered by the Privacy Act?

1. **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**
    NARA 24

2. **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

    At this time the SORN does not need to be modified, but will be reviewed regularly to ensure it is current.

Conclusions and Analysis

1. **Did any pertinent issues arise during the drafting of this Assessment?** No.

2. **If so, what changes were made to the system/application to compensate?** n/a
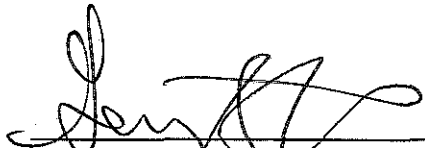

See Attached Approval Page

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:
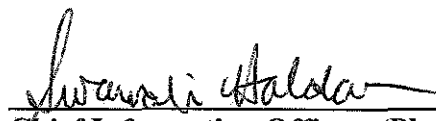
 IT Security Manager
 Privacy Act Officer

The Following Officials Have Approved this PIA

PAULA L. AYRES
NARA Personnel Security Officer _____ (Signature) _~~~~~~~~~~~~~~ (Date) _10/23/14_
System Manager, (Please include name, title and contact information)

_____ (Signature) _11/7/14_ (Date)
Senior Agency Official for Privacy, (Please include name, title and contact information)

_____ (Signature) _10/27/14_ (Date)
Chief Information Officer, (Please include name, title and contact information)

7