

Privacy Impact Assessment (PIA)

Name of Project: Insider Threat Program Support System (ITPSS)

Project's Unique ID:

Legal Authority(ies):	<p>Executive Order 13231 - Critical Infrastructure Protection in the Information Age</p> <p>Executive Order 13526 - Classified National Security Information</p> <p>Executive Order 13556 - Controlled Unclassified Information</p> <p>Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information</p> <p>44 U.S. Code Chapter 21 - National Archives and Records Administration</p> <p>44 U.S. Code Chapter 23 - National Archives Trust Fund Board</p> <p>44 U.S. Code Chapter 31 - Records Management By Federal Agencies</p> <p>General Records Schedule 5.6: Security Records</p> <p>Intelligence Authorization Act of 1995 (50 USC 402a) Section 811(c)(1)(a)</p>
------------------------------	---

Purpose of this System/Application:

The ITPSS supports the NARA data collection and analysis of machine data related to insider threat monitoring activities.
ITP staff process machine data from a variety of sources as well as perform analysis and create case files for the Insider Threat Program.

Section 1: Information to be Collected

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

Employees	Name, Address, Date of Birth, Social Security Number (SSN), Driver License Number, Passport Number, Bank & Credit Card Accounts and Records
External Users	N/A
Audit trail information (including employee log-in information)	<p>ITPSS Staff login are tracked by NARA operations. ITPSS staff work is also tracked within Splunk.</p> <p>File Integrity Management product (Tripwire or similar tool) will be provisioned to detects changes to case files, and reduce risk due to unauthorized changes by ITP staff.</p>

Other (describe)	N/A
Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?	
NARA operational records	<p>The following employee machine data are ingested into the ITPSS. Data for the individuals without access to classified information are filtered and deleted before further ITP review is completed for NARA employees who have access to classified information and maintain an active security clearance:</p> <ol style="list-style-type: none"> 1. Machine generated data from Email Logs. 2. Machine generated data from Authentication Change Logs. 3. Machine generated data from DNS Logs. 4. Machine generated data from File Access Logs. 5. Machine generated data from Firewall Logs. 6. Machine generated data from Configuration Change Logs. 7. Machine generated data from Account Creation Logs. 8. Machine generated data from Mobile Device Manager Logs. 9. Machine generated data from Help Desk Ticket System Logs. 10. Machine generated data from Network Packet Tags. 11. Machine generated data from Intrusion Detection and Prevention Logs. 12. Machine generated data from Printer, Scanner, Copier, and Fax Logs. 13. Machine generated data from Telephone Records. 14. Machine generated data from User Activity Monitoring Logs. 15. Machine generated data from HTTP/SSL Proxy Logs. 16. Machine generated data from VPN Logs. 17. Machine generated data from Human Capital systems 18. Machine generated data from Removable Media Manager Logs. 19. Machine generated data from Active Directory Logs. 20. Machine generated data from Anti-Virus Logs. 21. Information from Anonymous Reporting. 22. Machine generated data from Network Monitoring Logs. 23. Information from Asset Management Logs. 24. Machine generated data from Permission Change Monitoring Logs. 25. AUP Violation Records. 26. Background Investigations. 27. Conflict of Interest Reporting. 28. Corporate Credit Card Records. 29. Disciplinary Records. 30. IP Policy Violation Records. 31. Foreign Contacts Reporting. 32. Physical Security Violation report 33. Physical Access Records
External users	N/A
Employees	<p>The following data for employees who have access to classified information and maintain an active security clearance:</p> <ol style="list-style-type: none"> 1. Name.

	<ol style="list-style-type: none"> 2. Address. 3. Social Security Number (SSN). 4. Date of Birth (DoB). 5. Driver's License Number. 6. Bank Account Number. 7. Personnel Records 8. Performance Evaluations. 9. Physical Security Violation Records. 10. Travel Reporting. 11. Security Clearance Records.
Other Federal agencies (list agency)	<p>Federal Bureau of Investigation (FBI) - provides NARA with Foreign travel information (who, where, when) on an ad hoc basis.</p> <p>Also on an ad hoc basis, Insider Threat Program(s) at other federal agencies may provide information when applicable. Whenever there is an opportunity for such cooperation, NARA ITP Office will reach out to such Federal agency via an email to request specific information on the employee.</p>
State and local agencies (list agency)	<p>Records from local law enforcement agencies such as DUI, Arrest Records, and Medical Records (that may be included in, and provided from local (State and County) authorities as justification for use of a controlled substance) may be included within an employee's Personnel Security file.</p>
Other third party source	N/A

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.

Yes, to ensure that the classified information is not wrongly handled, exfiltrated, shared or destroyed.

2. Is there another source for the data? Explain how that source is or is not used?

No. There is no other source to collect needed insider threat information.

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?

Yes, case files are produced (as Microsoft Words documents) from aggregation of available data elements ingested from mainly NARA and few external sources. Case files are maintained locally on ITPSS dedicated server restricted by an isolated VLAN.

The system will allow the aggregation of data and analysis of that data using machine learning techniques to detect patterns in behavior that may be suspicious.

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

No. As far as ITPSS function of review and referring cases up to the FBI, no new data is placed in any individual records.
FBI, upon their review/investigation, may decide to add new data to the individual record.

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?

ITPSS ensures that data ingested are from approved, authoritative sources.
Technical data such as computer use logs are usually coordinated with technical POCs administering the applicable tools to identify possible false positives before determining log relevance to ITPSS review.
Technical POCs are: IS for security tools (Tenable Security Center, FireEye);
Operation Team for Firewall logs, System use logs, etc.

On a weekly basis, ITPSS obtains updated list of employees with access to classified information from NARA Security Office as well as NARA Human Resources from which a current ITPSS list is derived. As a first step and a mandatory requirement before any insider threat review starts, all ingested logs and data sets are filtered to match the current list of individuals with access to classified information. All other data sets are immediately deleted.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Access control (user name/password).
Isolated VLAN limited to the ITPSS.
Encrypted Remote Desktop Protocol (RDP) for file and print operations.

ITP staff actions are tracked and monitored via Splunk indexing and use of File Integrity Management (FIM) such as Tripwire (or equivalent) tool. ITP staff system logs are reviewed on a weekly basis by the ISSO.

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

N/A.

The ITPSS does not consolidate any existing process.

7. Generally, how will the data be retrieved by the user?

Data from different NARA sources is directly ingested into Splunk and available to ITP user for insider threat analysis.

External data from FBI (when applicable) available through removable media (such as DVD) are added to case files (Word Document).

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, personal identifiers listed below are included within insider threat case files/records as well as some Splunk logs:

1. Name
2. Address
3. Social Security Number (SSN)
4. Date of Birth (DoB)
5. Driver's License Number
6. Bank Account Number
7. Passport Number

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

Case files (Microsoft Word documents in Memo format) are referred to the FBI as a Section 811 Referral (Section 811 of the Intelligence Authorization Act of 1995 (50 USC 402a)).

These reports may also be shared with the Insider Threat Program managers of other Federal agencies (when applicable to a current investigation).

Reports and inquiries regarding non-national security concerns may be referred to NARA OIG or NARA supervisors/managers when appropriate.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.

Public:

-No, public information is not affected.

Employees:

-Yes; If NARA's Personnel Security Officer or NARA senior leadership determines that such employee's further access to certain NARA information or assets should be stopped or limited to mitigate threats of exfiltration, destruction, or any mis-handling of classified information. Reports referred to FBI under a Section 811 referral may result in criminal prosecution of an employee.

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.

ITPSS may perform monitoring of IT resource use, proximity access and travel records.

12. What kinds of information are collected as a function of the monitoring of individuals?

IT resource use (listed in Section 1), Proximity Access and Travel Records are collected as part of insider threat monitoring.

13. What controls will be used to prevent unauthorized monitoring?

The NARA Security Office provides list of employees with security clearances having access to classified information that should be monitored as part of insider threat protection support. This list helps identify individuals for the insider threat monitoring.

As new users are on-boarded or removed from Personnel Security Office databases, the ITP staff updates their working list to avoid unauthorized monitoring of individuals.

System Admin/ISSO reviews ITPSS user access logs on weekly basis for inappropriate use, and refer any violation to System Owner for action.

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

N/A - ITPSS is not web-based.

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)?

1. ITP Staff (3 individuals) have full data and case file access.
2. NARA Operations System Administrators can monitor ITPSS access logs.

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.). Are safeguards in place to terminate access to the data by the user?

There are only 2 (two) levels of access within the ITPSS - System Administrator and Basic User access.

The System Administrator is designated and approved by the System Owner to manage the hardware/software and provide oversight of operational activities, including account management for other ITPSS users.

Regular Users are ITP Staff accessing the system to complete insider threat analysis; they do not need privileged access to administrative functions.

-Access controls are strictly enforced within the ITPSS.

-User activities are tracked and reviewed on weekly basis for inappropriate use.

-Encryption for data at rest and in transit are implemented via Windows Bitlocker and encrypted RDP for scan and print.

A File Integrity Management (FIM) product such as Tripwire (or equivalent) tool will track user activities on case files while Splunk logs all user activities within the aggregated logs. These logs are reviewed on weekly basis.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

ITPSS users will be restricted by AD policy to limit user access to weekdays from 0600 hours to 2100 hours only.

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)? How will these controls be monitored and verified?

Splunk logs for user activities; and FIM change records are reviewed on a weekly basis.

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. Contractors supporting the NARA Operations Team may be involved implementing patches, updates and VLAN management.
Privacy Act contract clauses are included in contractor's contract.

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.

Yes: NARAnet, Physical Access Control System (PACS), CCTV, Badging and Access, Archives Investigation Management System (AIMS), HR databases, and Information Security System Operation Network (ISSON) provide insider threat data to the ITPSS.

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

All have current ATOs except ISSON and AIMS. ISSON is currently undergoing ATO process.

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

ITPSS ISSO - Chuck Hughes.

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.

Yes. Case files are sent to the FBI as a Section 811 Referral.
Responsibility for ensuring the proper use of data is on the ITPSS ISSO - Chuck Hughes.

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; every NARA user consents to IT system use monitoring in accordance with NARA 802.4.

2. Does the system ensure “due process” by allowing affected parties to respond to any negative determination, prior to final action?

No. ITPSS does not solicit/engage individuals for confirmation of their information. If reports are referred to the FBI as part of a Section 811 referral, then due process will be afforded by the criminal investigative process.

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.).

Machine data on ITPSS is a subset of data generated by, and residing on, other NARA IT systems and is not the system of record for the data sets listed in Section 1.

1. Monitored employees' list are updated on a weekly basis to keep current.
2. Data related to IT assets use are coordinated and reviewed with technical POCs (Security and Operations) to remove any false positives prior to being referred to the FBI.
3. Weekly review/Audit of ITP staff activities to mitigate any misuse of the data/system

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?

N/A - The system is not operated in any other site other than A-2.

3. What are the retention periods of data in this system?

Case Files - 25 years

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 unclassified that cannot be destroyed or purged until the schedule is approved.

General Records Schedule 5.6, Items # 210 - 230, describe the retention period of ITP records.

Case files are numbered to include the year of creation. Example: O-YYYY-002. The middle four characters (YYYY) depict the year of creation and implies that in year YYYY+25, the file should be destroyed. (ref. General Records Schedule 5.6)

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.

Yes. The ITPSS provides a new capability to aggregate data from several NARA (and few non-NARA) sources for the inside threat review; and generating case files from same.

6. How does the use of this technology affect public/employee privacy?

For the first time, a significant amount of personal information about employees will be consolidated into a signal repository for analysis. While employees have no expectation of privacy in this information, the aggregation of the data has the potential to expose additional information about an employee to the Insider Threat program staff. Insider Threat program staff work closely with the FBI to ensure a thorough investigation of any suspicious behavior is confidentially conducted.

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?

A Security Assessment of Security (and Privacy) Controls is scheduled, and identified risks will be noted with Plan of Actions and Milestones (POA&M).

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.

In addition to the Security Assessment prior operation, FireEye, Tenable Security Center, McAfee Antivirus, and other security tools on NARA network will be installed, maintained and monitored by Security and NITTSS personnel to ensure the security of ITPSS and its data elements.

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

ITPSS ISSO - Chuck Hughes

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 - 45

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

Yes, if new data sets are introduced.

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?

The need to introduce a File Integrity Management (FIM) product such as Tripwire, Netwrix (or equivalent) to monitor and track case file changes was discussed.
The need to limit access to 0600 hours - 2100 hours on week days was discussed.


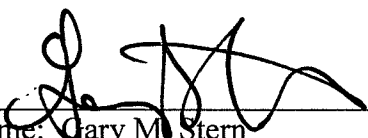
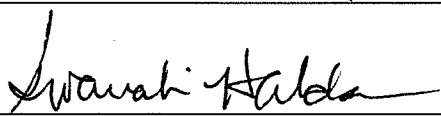
2. If so, what changes were made to the system/application to compensate?

File Integrity Management (FIM) such as Tripwire, Netwrix (or equivalent) will be introduced.
Access to ITPSS will be limited to 0600 hours - 2100 hours during week days.

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	
System Manager (Project Manager)	
 (Signature)	5/23/18 (Date)
Name: Neil Carmichael	
Title: Insider Threat Program Manager	
Contact information: 8601 Adelphi Road, Room 8110 8530, College Park, MD 20740-6001 301-502-3704, neil.carmichael@nara.gov	
Senior Agency Official for Privacy (or designee)	
 (Signature)	5/16/18 (Date)
Name: Gary M. Stern	
Title: General Counsel	
Contact information: 8601 Adelphi Road, Room 3110, College Park, MD 20740-6001 301-837-3026, Garym.stern@nara.gov	
Chief Information Officer (or designee)	
 (Signature)	6/8/18 (Date)
Name: Swarnali Haldar	
Title: Executive for Information Services/CIO (I)	
Contact information: 8601 Adelphi Road, Room 4415, College Park, MD 20740-6001 301-837-1583, swarnali.haldar@nara.gov	