# Privacy Impact Assessment

## Name of Project: NARANET
## Project's Unique ID: NARANET

## Legal Authority (ies):

## Purpose of this System/Application:

NARANET is a general support system (GSS) utilized as NARA's Information Technology Infrastructure on which agency administrative and mission critical activities are accomplished electronically. NARANET connects the entire agency internally and the agency to its public and government customers via the Internet. NARANET fosters the agency's ability to create, maintain, retrieve, and analyze vital agency resources and information for sharing essential evidence. NARANET also provides the network backbone needed to support distributed access to all NARA electronic access systems. NARANET provides file, print and e-mail services for the agency.

NARANET provides a transmission medium for NARA's IT systems. It does not in and of itself control other system's PII data. The system does not have any mechanisms which are designed to recognize, process or extract PII data, and does not have any mechanisms designed to protect PII data other than the access controls which limit user access to the data they are authorized to see.

## Section 1: Information to be Collected:

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

Privacy information contained varies greatly depending on the needs of the data owner.

   a. **Employees**
   b. **External Users**
   c. **Audit trail information (including employee log-in information)**
   d. **Other (describe)**

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

Data elements obtained vary greatly depending on individual data owner needs.

a. **NARA operational records**
b. **External users**
c. **Employees**
d. **Other Federal agencies (list agency)**
e. **State and local agencies (list agency)**
f. **Other third party source**

## Section 2: Why the Information is Being Collected:

Personal information is not collected by NARANET. Users of this (GSS) support system utilize the network file servers to store data that may contain privacy information. NARANET in itself is not an infrastructure designed for the collection or retrieval of privacy data; it provides the space and connection capabilities to allow users to store and share data. Individual data owners use NARANET in support of their business processes.

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

Each personal data element contained on NARANET are for the business purpose of the individual data owner, not NARANET (see items 1 and 2, above).

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

Information is shared based on the business need of the individual data owner.

## 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?**

This question is applicable to each individual data owner. The system does not have any mechanisms designed to recognize, process or extract PII data.

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

This question is applicable to individual data owner business needs.

**3. Can the system make determinations about employees/the public that would not be possible without the new data?**

N/A

**4. How will the new data be verified for relevance and accuracy?**

This question is applicable to individual data owner business needs.

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

This question is applicable to individual data owner business needs.

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

This question is applicable to individual data owner business needs

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

This question is applicable to individual data owner business needs.

**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.**

This question is applicable to individual data owner business needs.

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

This question is applicable to individual data owner business needs.

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

This question is applicable to individual data owner business needs.

**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.**

This question is applicable to individual data owner business needs.

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

This question is applicable to individual data owner business needs.

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

This question is applicable to individual data owner business needs

**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)?**

Data will be accessed by individual data owners and users who require access to this data.

**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.).**

Access is determined by individual data owners.

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

Data is restricted base on individual data owner requirements. NARANET does not have any mechanisms designed to protect PII data other than the access controls which limit user access to the data they are authorized to see. Individual data owners are responsible to manage and secure any PII data which resides in NARANET according to agency directive

**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)?**

NARANET components (firewalls, switches, and routers) do restrict access to non-public facing, internal systems/applications residing on NARANET. However, NARANET does not have any mechanisms which are designed to recognize, process or extract PII data, and does not have any mechanisms designed to protect PII data other than the access controls which limit user access to the data they are authorized to see. Individual data owners are responsible to manage and secure any PII data which resides in NARANET according to agency directive.

**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?**

NARANET is operated and maintained by contractor personnel. Appropriate Privacy Act

clauses are in place.

**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.**

N/A.

**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?**

Individual data owners are responsible for managing and securing any PII data which resides in NARANET according to agency directive.

**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?**

N/A.

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

N/A.

## 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.).**

N/A

**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

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

Not applicable to NARANET; retention of information in NARANET is in accordance with the individual data owner needs and NARA's records disposition schedule.

**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.**

Not applicable to NARANET, disposition is per individual data owner needs.

**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.**

N/A.

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

N/A

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

Yes, to a large degree NARANET meets NARA's IT security requirements, as well as those requirements set down by federal law and policy. NARANET is the GSS that provides many of the security controls for the systems that reside on it. As such, NARANET itself is responsible for handling and meeting many of the NARA IT security requirements for those systems. NARA's IT security requirements are based on Federal law, policy, and procedures.

**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, a risk assessment has been performed. The NARANET GSS comprises many components. The risk assessment for the NARANET GSS is continually reviewed and updated as significant changes occur to this GSS. A POA&M has been established for NARANET, which is also continuously reviewed and updated to reflect planned actions

to mitigate identified risks.

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

NARA conducts vulnerability scans on all network devices on a monthly basis according to a predefined schedule. A quarterly report of open vulnerabilities is compiled and analyzed. In addition, a subset of NIST 800-53 controls are tested for NARA systems on an annual basis.

NARANET also has an Intrusion Detection System in place and participates in the Department of Homeland Security's EINSTEIN program. Components of NARANET also feed log files into a Security Information Management (SIM) system which provides correlation with

Various components of the GSS have centrally-managed, and monitored anti-virus software and host-based intrusion detection software in place.

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

Any addition questions regarding the security of the system can be directed to Bernarr Coletta or Keith Day.

## 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.**

N/A

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

N/A.

## 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?**

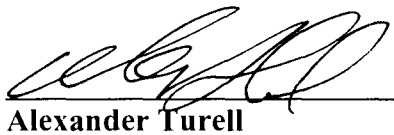
N/A

**See Attached Approval Page**

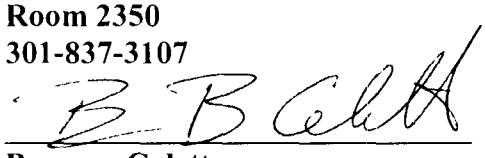
Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

IT Security Manager
Privacy Act Officer

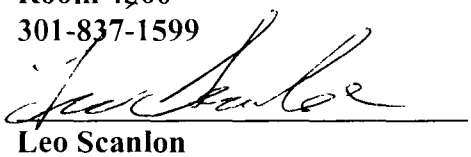
**The Following Officials Have Approved this PIA**

 (Signature) 9/2/08 (Date)

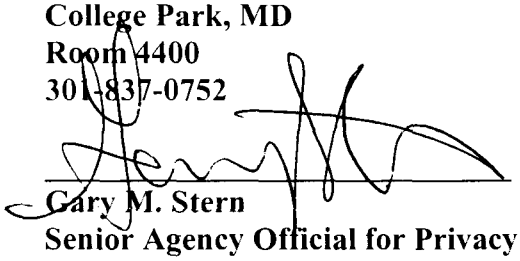
**Alexander Turell**
**Acting NARANET System Owner**
**8601 Adelphi Rd.,**
**College Park, MD**
**Room 2350**
**301-837-3107**

 (Signature) 9/2/08 (Date)

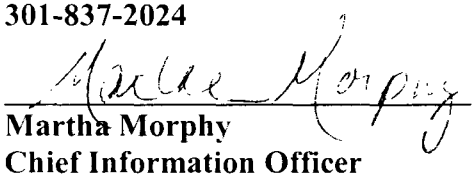
**Bernarr Coletta**
**NARANET ISSO**
**8601 Adelphi Rd.,**
**College Park, MD**
**Room 4500**
**301-837-1599**

 (Signature) 9/3/08 (Date)

**Leo Scanlon**
**IT Security Officer**
**8601 Adelphi Rd.,**
**College Park, MD**
**Room 4400**
**301-837-0752**

 (Signature) 9/3/08 (Date)

**Gary M. Stern**
**Senior Agency Official for Privacy**
**8601 Adelphi Rd.,**
**College Park, MD**
**Room 3110**
**301-837-2024**

 (Signature) 9/2/08 (Date)

**Martha Morphy**
**Chief Information Officer**
**8601 Adelphi Rd.,**
**College Park, MD**
**Room 4400**
**301-837-1992**