

Privacy Impact Assessment (PIA)

Name of Project: Classified Interim System - Top Secret

Project's Unique ID: CIS - TS

Legal Authority(ies):	44 U.S. Code Chapter 21-National Archives and Records Administration 44 U.S. Code Chapter 29-Records Management by the Archivist of the United States 44 U.S. Code Chapter 31-Records Management by Federal Agencies 44 U.S. Code Chapter 33-Disposal of Records
------------------------------	---

Purpose of this System/Application: The Classified Interim System (CIS) TS provides over 40 terabytes of managed storage for classified electronic records to include ingest, managed storage, backup, accession-level metadata management, selected search, workflow, and output. Archivists from the electronic records unit of Research Services use CIS TS to store and manage classified electronic records.

Section 1: Information to be Collected

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

Employees	Name and account name
External Users	N/A
Audit trail information (including employee log-in information)	Employee login information and work tracking files
Other (describe)	N/A
Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?	
NARA operational records	N/A
External users	N/A
Employees	N/A

Other Federal agencies (list agency)	Any Federal agency may transfer permanent classified electronic records consistent with approved records disposition schedules. Some permanent classified electronic records contain personally identifiable information. Permanent classified electronic records are retained on CIS TS until declassification or until the development and transition to the Classified Electronic Records Archives (CERA).
State and local agencies (list agency)	N/A
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 confirm that only authorized users are gaining access to the records.

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 new data will be derived or aggregated through the permanent retention/storage of classified electronic records.

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

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?
 N/A

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

N/A

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

N/A

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

Employee login (Username and Password)

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.

No

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

No reports are produced on individuals.

However; CIS TS audit trail functionality provides the ability to report on configuration and change compliance of processes and identify changes made by individuals for audit purposes or to remediate a change that may cause service interruption.

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. CIS TS can only monitor access (log in) and work activity on the system.

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

Log in and work activity.

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

N/A - Only authorized personnel have access to CIS TS. The system is isolated and internal to NARA. Physical and technical security controls are in place to prohibit unauthorized access and production oversight is provided by the system owner; currently, the SO and one administrator maintain the system.

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

N/A. CIS TS is only available to cleared RDE staff.

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)?

Managers, system administrator(s), and authorized users

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?

Access is determined at three tiered levels. The top tier level is determined by the Personnel Security Officer who validates that the archivist has a Top Secret (TS) clearance with a favorable Single Scope Background Investigation (SSBI) for Sensitive Compartmented Information (SCI) eligibility and a Q access authorization (RD / FRD). At the second tier level, the director identifies only staff who will

be assigned classified projects. At the third level, the system administrator creates a user account. Technical controls protect against unauthorized access to, or misuse of CIS TS.

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

Explain.

Authorized users have access to all of the data in CIS TS.

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?

Restrictive physical security controls protect against unauthorized access to the CIS TS workstations. Technical controls protect against unauthorized access to or misuse of CIS TS and facilitate detection of security violations by generating audit logs to record users' activities and warn of anomalous conditions on the CIS TS network. Audit tools create, maintain, and protect a trail of actions of users and administrators that trace security-relevant events to an individual, ensuring accountability. Also, in an effort to prevent data/record loss or unauthorized modification, the delete function has been disabled on the Preservation folder in CIS TS.

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?

No

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. The server is connected to the CIS TS network and has the capability to copy files to and from the CIS storage component. Current initiative is in place to connect the Archival Electronic Records Inspection and Control (AERIC) TS system to the CIS TS network. When approved, AERIC TS will have the capability to copy data files to and from the CIS TS storage component.

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

The Archival Electronic Records Inspection and Control (AERIC) TS system was assessed on September 10, 2015. However, the system is undergoing a security assessment and accreditation (SA&A) update. The CIS TS is currently being proposed for formal implementation and accreditation.

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

The CIS TS owner (SO) and individual users are responsible for managing and securing any personal data which resides in the system. NARA's Senior Agency Official for Privacy is responsible for ensuring compliance with the privacy rights of the public and NARA employees.

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?

CIS TS does not accept data from the public. The only data in CIS TS has been transferred from other Federal agencies.

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

N/A. The electronic records in CIS TS are archival records transferred to the custody of the Archivist of the United States for permanent retention. Archival records are specifically excluded from the access and amendment provisions of the Privacy Act.

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.).

The transferred classified electronic records are compared to the applicable records disposition schedule listed in the Electronic Records Archives (ERA) Transfer Request (TR). The electronic records are not verified for accuracy, timeliness, or completeness but are assumed to be accurate, timely, and complete at the time of transfer by the originating Federal agency. Specific procedures relating to verification are outlined in the office's standard operating procedures.

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?

Permanent classified electronic records are retained on the CIS TS until declassification or until the development and transition to the Classified Electronic Records Archives (CERA).

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.

CIS TS will store permanent classified electronic records until declassification or until the development and transition to the Classified Electronic Records Archives (CERA), which is currently under development.

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?

N/A

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

CIS TS is being developed and configured to operate in accordance with NARA's IT security requirements and all applicable federal laws and policies. CIS TS is currently going through the Security Authorization and Assessment (SA&A) process to ensure that NARA's IT security requirements and applicable federal laws and policies have been met.

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?

As part of the SA&A process, a risk assessment of all applicable security controls and related documentation will be conducted on CIS TS to ensure that the necessary procedures are in place to safeguard CIS TS information.

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

System audit log(s) and log reviews.

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

Mr. Theodore Hull, System Owner: (301) 837-1824

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?

CIS TS requires a Security Assessment and Accreditation (SA&A) package.

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

No changes to CIS TS. RDE will request the SA&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

System Manager (Project Manager)



(Signature)

JUL 17 2017

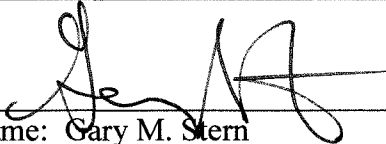
(Date)

Name: Theodore Hull

Title: Supervisory Archives Specialist

Contact information: 8601 Adelphi Road, Room 6305, College Park, MD 20740-6001
(301) 837-1824, Theodore.Hull@nara.gov

Senior Agency Official for Privacy (or designee)



(Signature)

7/17/17

(Date)

Name: Gary M. Stern

Title: General Counsel

Contact information: 8601 Adelphi Road, Room 3110, College Park, MD 20740-6001
301-837-1750, garym.stern@nara.gov

Chief Information Officer (or designee)



(Signature)

7/19/2017

(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