

Privacy Impact Assessment (PIA)

Name of Project: Document Conversion Unit

Project's Unique ID: DCU

Legal Authority(ies):	44 USC 2108, 2110, and 2907
------------------------------	------------------------------------

Purpose of this System/Application: The Document Conversion Unit provides the functionality to digitize paper material to various electronic format(s), capture metadata, and generate final output using customer agencies defined formats. The final output is then delivered using agreed upon method(s), which may vary by customer agency and Federal Record Center Program (FRCP) site.

Section 1: Information to be Collected

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

Employees	User identifiers (user login ID) and authenticator (password)
External Users	N/A
Audit trail information (including employee log-in information)	<p>Windows OS Audit Trails and Logging</p> <p>All servers that are components of the Document Capture System are running Microsoft Windows Server 2008 R2 (Valmeyer – central DCU servers) and 2012 R2 (DCU servers at field sites in Atlanta, Chicago, Ft. Worth, and Riverside FRCs) Operating System. These operating systems are configured to audit the following information on the servers:</p> <ul style="list-style-type: none"> • Account Logon Events - both successful and failed account logon attempts are audited • Account Management - both successful and failed attempts to manage (create, delete, edit) user accounts are audited • Logon Events - both successful and failed logon events are audited • Object Access - both successful and failed object access attempts are audited • Policy Change - both successful and failed attempts to audit system policies are audited • Privilege Use - failed attempts to privileged resources are audited • System Events - both failed and successful system events are audited <p>Kofax Ascent Capture and Indicius Audit Trails</p> <p>The Kofax Ascent Capture and Indicius software has auditing functions enabled within the application. This audit log captures all activities and events performed on the system by all Kofax users. These events and activities that are logged</p>

	<p>include logins/logoffs batch information, user performed functions tracked, creation of batches and images within Kofax account management activities. etc Input/Output Controls.</p> <p>Audit trails are used for receipt of: inputs/outputs from the information system. A record is kept of individuals who implement media disposal actions and individuals who verify that such information or media was properly sanitized. Inventory records of all storage media containing organizational information are maintained for purposes of control and accountability.</p>
Other (describe)	Servers attached to the DCU system contain document images which have been (describe) created in the scanning process. At each location and for each project the content of these scans will vary but may include official personnel files.
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)	N/A
State and local agencies (list agency)	N/A
Other third party source	N/A
Section 2: Why the Information is Being Collected	
<p>1. Is each data element required for the business purpose of the system? Explain. Information concerning users of the Document Conversion Unit system is necessary to ensure that there is controlled access within the system based on the performance of authorized tasks.</p>	
<p>2. Is there another source for the data? Explain how that source is or is not used? Data in the Document Conversion Unit System are scanned image(s) of original paper material, any associated metadata captured during the conversion, and final output. The data is stored on a temporary basis, until the conversion customer agency reviews and approves delivered product.</p> <p>Once the original paper material is captured into electronic format, the original paper material is handled according to conversion customer agency direction</p>	

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?

The data in the system are scanned image(s) of original paper material, associated metadata captured and final output. The data captured during conversion is only stored on a temporary basis, and will be purged once the conversion customer agency has reviewed and approved the final product.

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

The data captured is not new data, but rather the original data captured in electronic format.

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?

The data captured is not new data, but the image(s) and metadata are verified against original paper material for quality assurance purposes. The percentage of the quality assurance is based on customer agency agreements.

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

Only authorized users of the NARANET with specific access rights assigned to the Document Conversion Unit System can access any of the consolidate data stored on a temporary basis. Electronic files, like paper files, are protected under the Privacy Act.

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

Each separate conversion project built within the Document Conversion Unit application is designed to control and protect the temporary conversion data until removal from the system.

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

The system is only accessible to user(s) that perform the digital conversion work. The data is stored on a temporary basis, until the customer agency has performed the Quality Review of the product. Once the delivered product is validated by the customer agency, notification is sent by customer agency to the FRC site for media disposal actions of the temporary 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.

No. The system is only accessible to user(s) that perform the digital conversion work. The data is retrievable only through the unique Batch Name of the conversion work. The content of the imaged data cannot be searched.

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 Document Conversion Unit can generate productivity reports based on the processing information during the conversion work. Only the Supervisor, support personnel and Lead Technician have access to these reports.

Example report types: Billing Volume, Task data captured, Productivity Statistics, etc.

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.

The Document Conversion Unit system can monitor the various work queues and user activities. Only the Supervisor, support personnel and Lead Technician have access to these tools.

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

Productivity. Work Activities (Current and Past actions)

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

The Document Conversion Unit application allows the system administrator to assign the monitoring functions by user(s). Any user(s) not assigned by the system administrator are prevented access to the monitoring tools through the Document Conversion Unit application security.

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)?

System administrators, users, and when required for support purposes, service contractors will have access to the system.

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?

The system and its users are subject to NARA-wide input/output security controls as specified in the NARA IT Security Handbook, Operations Controls.

NARA has standard rules of behavior, which all users must acknowledge during new user orientation and annual user training. In addition users (employee, contractor, intern, or others performing work for NARA with access to NARA IT resources) of NARA information technology and computing resources, are required to comply with NARA regulations, policies, procedures, and guidelines regarding the protection of NARA automated information systems from misuse, abuse, loss, or authorized access. Users understand that they will be held accountable for their actions related to the NARA data, information, and computing resources entrusted to them. Users further understand that they may be subject to criminal prosecution, and/or administrative disciplinary action, including reprimand, suspension from duty without pay, or removal from my position and/or Federal employment for failure to comply with the states rules of behavior. The complete rules of behavior are outlined in the System Security Plan for the system.

Individuals requiring access to Document Conversion Unit system information must be screened (e.g., verification of background checks and investigations as well as security and non-disclosure agreements) prior to being granted access authorization in accordance with organizational personnel security policies. Privileged users (i.e., individuals who are authorized to bypass significant technical and operational controls), are screened prior to access and periodically every two years. For prospective employees, references are contacted and background checks performed, as appropriate. Periodic reinvestigations are performed no more than every five years, consistent with the criticality/sensitivity rating of the position, according to criteria from the Office of Personnel Management. Security agreements are required for employees and contractors assigned to work with mission information. The period during which nondisclosure requirements remain in effect is identified.

Each user or process is authorized the most restrictive set of privileges or accesses needed for the performance of authorized tasks.

Information system owners identify authorized users and their respective access authorizations. Emergency and temporary access authorizations to the information system are explicitly approved by designated organization officials, monitored, and removed as soon as no longer required. Where appropriate, access is authorized based on time and/or location. Security administrators set parameters in security software to provide access as authorized and restrict access that has not been authorized. This includes access to files, load libraries, batch operational procedures, source code libraries, security files and operating system files.

Comprehensive account management, monitored and enforced by the system manager ensures that only authorized users can gain access to information systems. Account management includes:

- Identifying types of accounts (i.e., individual and group, conditions for group membership and associated privileges)
 - Establishing an account (i.e., required identification, approval, and documentation procedures)
- Activating an account
- Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators)
 - Terminating an account

When the user's employment is terminated, the organization terminates information system access, conducts exit interview, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures the individual no longer has access to official records created by the employee that are stored on organizational information systems.

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

Explain.

Each user or process is authorized the most restrictive set of privileges or accesses needed for the performance of authorized tasks. Levels of access are outlined above.

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?

See number 2, above.

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. Contractors performed the installation of the software components and were required to sign the on-site access documents for entering the building. There was not a contract except for the purchase contract for the software, installation and software support maintenance for upgrades/problem-solving. NH/ITSS performs the on-going maintenance of the Operating System software and hardware related to the system. The FRCP National Digital Imaging Specialist supports the Application software.

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?

NARA and the customer agency providing documents to NARA for digitizing are jointly responsible for protecting the privacy right of the public and 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?

Individuals cannot decline to provide or use any information residing in the Document Conversion Unit system without meeting the access requirements for this system.

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

Any individual denied access to the Document Conversion Unit system is provided "due process" for any negative determination prior to final action, following NARA standard policies.

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 data is verified for accuracy during the capture process for image quality, metadata accuracy and completeness by the FRCP staff.

The customer agency and the FRCP document the requirements of the quality standards within the project service agreements.

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 business rules for a given scanning project are encapsulated in a “batch class” so that any FRC doing the scanning will produce the same output.

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

The system is only accessible to user(s) that perform the digital conversion work. The data is stored on a temporary basis, until the customer agency has performed the Quality Review of the product. Once the delivered product is validated by the customer agency, notification is sent by customer agency to the FRCP site for media disposal actions of the temporary data.

Images and metadata from project scanning are deleted 90 days after the customer acknowledges receipt. SmartScan images are deleted after 30 days.

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.

The temporary conversion data being stored on the system is removed once customer agency has reviewed and approved the delivered electronic copies of records based on service agreements. The disposition instructions for all original materials, electronic or paper are the responsibility of the customer agency. Procedures on the purging of the temporary conversion data are currently being written and will be supplied as an amendment to this document.

Procedures will address the following which are being followed but have not yet been formalized as a standard operating procedures:

Unauthorized individuals cannot read, copy, alter, or destroy information in printed form or on media removed from the information system. Media accountability and control mechanisms (e.g., audit trail logs) provide protection comparable to that for equivalent paper documents. Electronic media is controlled and protected in a manner similar to that used for paper materials. Output from the information system is given only to authorized users.

Appropriate security labels that reflect any distribution limitations and handling caveats of the information are affixed to all information system output, which includes printed output. Removable information storage media contains external labels indicating the distribution limitations and handling caveats of the information.

Only authorized users pick up, receive, or deliver input and output information and media from the information system. Appropriate controls are established for all information entering or leaving the facility, including for mailing media and/or printed output from the information system. Erroneous or unauthorized transfer of information, regardless of media or format, is precluded.

Information system hardware and machine-readable media is cleared, sanitized, or destroyed before being reused or released outside of the organization. Retired, damaged, discarded, or unneeded information is disposed in a manner that prevents unauthorized persons from using it. Information is never disclosed during disposal unless authorized by statute. Cleared or sanitized media that previously contained information at a designated FIPS Publication 199 security category (for confidentiality) is reused at the same or higher security category. Sanitized media is downgraded only with appropriate approval(s). The media and output control is monitored and enforced by the system manager.

Destruction of Paper Media Hard copy documents are destroyed when no longer needed. For information requiring such protection, destruction methods for organizational information in paper form are as follows:

- (i) Burning - the material is burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle is separated to ensure all pages are consumed
- (ii) Mulching or pulping - all material is reduced to particles one inch or smaller
- (iii) Shredding or disintegrating - paper is shredded in cross-cut shredders (preferred) or strip shredders (alternative).

Information storage media is destroyed in accordance with organization-approved methods. An authorized contractor accomplishes document destruction in the absence of the organization's direct participation.

Release of Systems and Components Equipment removal procedures for information systems and components that have processed or contained organizational information are followed. This includes inspection of the information system by designated individuals to ensure that all media, including internal disks, have been removed or sanitized.

Optical disks (including compact disk/read only memory, write once/read many, digital versatile disk, and read-write compact discs) offer no mechanism for sanitization. Therefore they will be destroyed.

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?

NARA staff who have access to the files being digitized

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.

Routine security scans of all Digital Conversion Units connected to NARANET.

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

N/A

Richard Morgan (AFOR-S)

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

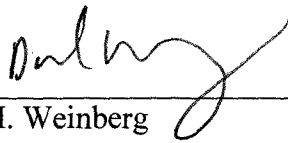
See Attached Approval Page

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

System Manager (Project Manager)



(Signature)

6/26/18

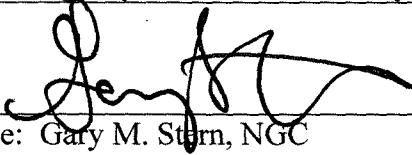
(Date)

Name: David M. Weinberg

Title: Director, Records Center Program

Contact information: 8601 Adelphi Road, Room 3600, College Park, MD 20740-6001
301-837-3115, david.weinberg@nara.gov

Senior Agency Official for Privacy (or designee)



(Signature)

6/19/18

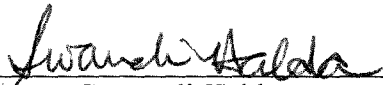
(Date)

Name: Gary M. Stern, NGC

Title: Senior Agency Official for Privacy

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)

7/9/2018

(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