

## Privacy Impact Assessment (PIA)

**Name of Project:** Digital Capture System

**Project's Unique ID:** DCS

<b>Legal Authority(ies):</b>	44 USC 2108, 2110, and 2907
------------------------------	-----------------------------

**Purpose of this System/Application:** The Digital Capture System 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 FRCP site.

### Section 1: Information to be Collected

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

<b>Employees</b>	User identifiers (user login ID) and authenticator (password)
<b>External Users</b>	N/A
<b>Audit trail information (including employee log-in information)</b>	<p>Windows OS Audit Trails and Logging</p> <p>All servers that are components of the Document Capture System are running Microsoft Windows Server 2003 Operating System. These operating systems are configured to audit the following information on the servers:</p> <ul style="list-style-type: none"> <li>• Account Logon Events - both successful and failed account logon attempts are audited</li> <li>• Account Management - both successful and failed attempts to manage (create, delete, edit) user accounts are audited</li> <li>• Logon Events - both successful and failed logon events are audited</li> <li>• Object Access - both successful and failed object access attempts are audited</li> <li>• Policy Change - both successful and failed attempts to audit system policies are audited</li> <li>• Privilege Use - failed attempts to privileged resources are audited</li> <li>• System Events - both failed and successful system events are audited</li> </ul> <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 include logins/logoffs, batch information, user performed functions tracked, creation of batches and images within Kofax, account management activities, etc</p> <p>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</p>

		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.
<b>Other (describe)</b>		Servers attached to the DCU system contain document images which have been 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, Veterans Administration benefit or medical files and related records, or images which do not contain PII such as maps or architectural drawings.
<b>Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?</b>		
<b>NARA operational records</b>		N/A
<b>External users</b>		N/A
<b>Employees</b>		N/A
<b>Other Federal agencies (list agency)</b>		N/A
<b>State and local agencies (list agency)</b>		N/A
<b>Other third party source</b>		N/A
<b>Section 2: Why the Information is Being Collected</b>		
<p><b>1. Is each data element required for the business purpose of the system? Explain.</b>  Information concerning users of the Digital Capture System is necessary to ensure that there is controlled access within the system based on the performance of authorized tasks.</p>		
<p><b>2. Is there another source for the data? Explain how that source is or is not used?</b>  Data in the Digital Capture 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>		
<b>Section 3: Intended Use of this Information</b>		
<p><b>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?</b>  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.</p>		
<p><b>2. Will the new data be placed in the individual's record?</b>  The data captured is not new data, but rather the original data captured in electronic format.</p>		

**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 Digital Capture System can access any of the consolidate data stored on a temporary basis. Electronic files, like paper files, are protected under the Privacy Act.

In addition, the employees who perform the scanning received NACI checks, underwent NARA IT Security Training, and are well-orientated as to the confidentiality requirements of their positions.

**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 Digital Capture System 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 Digital Capture System 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 Volumes, 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 Digital Capture 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 Digital Capture System 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 Digital Capture System 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 Digital Capture 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 (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.**

With the implementation of the Veterans Benefit Management System Project in the St Louis facility, the system can be configured to receive and send data to other NARA locations that provide scanning services.

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

Currently in the process of getting both of these items approved.

**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.**

The Veterans Administration will be able to receive and transfer data to the NARA system. The VA Information Security Office and the NARA Information Security Office will be responsible. The data being received or sent between the VA and NARA systems will be used to convert paper files to electronic files. The users of the systems will perform indexing, quality control and verification of the data prior to being delivered into the Veterans Benefit Administration's document management system.

### **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?**

No individuals can decline to provide or use any information residing in the Digital Capture System without meeting the requirements for access to 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 Digital Capture System are 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?**

Standard Operating Procedures are currently being written for maintaining the temporary data residing on the Digital Capture System. The application software is configured using a standard configuration and use across all sites.

**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 FRC site for media disposal actions of the temporary data.

**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

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.**

NHI performs routine security scans of all Digital Conversion Systems connected to NARANET.

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



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

Any modifications to the Privacy Act system of records notices that may apply to records in this system are the responsibility of the submitting Agency. There are no modifications to Digital Capture System at this time.

### **Conclusions and Analysis**

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

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

### **Sec 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)

8/18/11

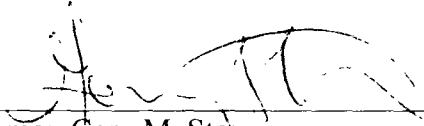
(Date)

Name:  
David Weinberg

Title:  
FRC program director

Contact information:

**Senior Agency Official for Privacy (or designee)**



(Signature)

11/4/11


(Date)

Name: Gary M. Stern

Title: SAOP and General Counsel

Contact information: NARA, 8601 Adelphi Road, Suite 3110, College Park, MD 20740  
301-837-3026

**Chief Information Officer (or designee)**



(Signature)

9.13.11

(Date)

Name: Michael Wash

Title: CIO

Contact information: NARA, 8601 Adelphi Road, Suite 3110, College Park, MD 20740  
301-837-1583

## Appendix I – NPRC- CPR (VBMS Project Specific Information)

NARA – Federal Record Center Program (FRCP) has signed an agreement 2011 with the Veterans Administration (VA) to design, develop, configure and implement a state of the art scanning workflow system, for veteran Disability and Compensation Claims.

### **Software**

The system consists of three core software products, Kofax Ascent Capture 9.0, KTM 5.0 and Seibel Tracking Application. Below is a basic description for each software product:

- Kofax Ascent Capture 9.0 and KTM 5.0 – These software products perform the capture, form classification and metadata extractions for the conversion to digital formats. These software products require certain processes to have Administration rights. Kofax provides a feature called Security Boost that allows these rights to be assigned to specific users within Kofax. This prevents the Kofax users from performing functions outside of the rights needed to perform the permitted functions assigned in Kofax. This software may require access to some ports for internal processes. (I.E. - 1443 for User Datagram Protocol (UDP), Transmission Control Protocol/Internet Protocol (TCP-IP))
- Kofax 9.0 provides connectivity to FileNet Document Management systems, which VA has implemented for the VBMS Project. The secure connection is established using SSL/TSL certificates, an assigned IP Range and authentication server to validate and allow data exchanges between the NARA FRCP system and the VA VBMS System. The data upload is an automated process that can be triggered during off-business hours. Any transmission which failed during this upload process is returned to the NARA Kofax system and marked as In-Error, which can be reviewed by system support personnel for resolution.
- Seibel Tracking Application – This application was developed by Optimos and contains similar functionality as the Case Management Reporting System (CMRS) system. The application allows end-users (Agencies) to create shipping manifests on boxes of OPF being submitted for Digital Capture work. The application will also allow the end-users (Agencies) to query the application for status information on any given box or OPF submitted.

**Equipment**

<b>Components</b>	<b>Manufacturer / Model</b>	<b>Serial # / Version #</b>	<b>Owner</b>	<b>Physical Location</b>	<b>Logical Location</b>
CPR-VA1	Dell PowerEdge 2950 Server		NR	CPR (St. Louis) Room 117	Attached to NARANET via Cisco 4506 Gigabit production switch
CPR-VA2	Dell PowerEdge 2970 Server		NR	CPR (St. Louis) Room 117	Attached to NARANET via Cisco 4506 Gigabit production switch
CPR-VA3	Dell PowerEdge 2970 Server		NR	CPR (St. Louis) Room 117	Attached to NARANET via Cisco 4506 Gigabit production switch
CPR-VA4	Dell PowerEdge 2970 Server		NR	CPR (St. Louis) Room 117	Attached to NARANET via Cisco 4506 Gigabit production switch
CPR-VA5	Dell PowerEdge 2970 Server		NR	CPR (St. Louis) Room 117	Attached to NARANET via Cisco 4506 Gigabit production switch
Cisco 4506 Switch	Cisco 4506 240-port Gigabit Switch	FOX11370C0H	NHT	CPR (St. Louis) Room 117	Attached to NARANET via primary CPR Production Router
Cisco 3845 Router	Cisco 3845 Router (CPR Primary Router)	FTX0943A11	NHT	CPR (St. Louis) Room 117	Primary CPR Production Router
Dell PowerVault 124 Tape Backup System	Dell PV-124T	CH6FB30629 Firmware v0031	NR	CPR (St. Louis) Room 117	Attached to NARANET via Cisco 4506 Gigabit production switch
Tape Backup Software	Symantec (Veritas) Backup Exec for Windows Servers	12.5	NR	Installed on CPR-DCU5	N/A

**POC**

Richard Morgan or James Berenz

## Appendix II – NPRC- (Annex / Valmeyer Specific Information)

### ***Project(s)***

NPRC - National Personnel Records Center (NPRC) has signed an agreement with the Office of Personnel Management (OPM) to digitize and transfer to the OPM electronic Official Personnel File (eOPF) system, civilian Official Personnel Files (OPFs) for various OPM Agencies. NPRC has also signed an agreement with the Air Force Material Command, to digitize and transfer to the electronic Official Personnel File (eOPF-Paris) system, civilian Official Personnel Files (OPFs) for AFMC personnel.

### ***Software***

The system consists of three core software products, Kofax Ascent Capture and Indicius, Connect:Direct Secure Plus, and Seibel Tracking Application. Below is a basic description for each software product:

- Kofax Ascent Capture 8.0 and Indicius 5.5 – These software products perform the capture, form classification and metadata extractions for the conversion to digital formats. These software products require certain processes to have Administration rights. Kofax provides a feature called Security Boost that allows these rights to be assigned to specific users within Kofax. This prevents the Kofax users from performing functions outside of the rights needed to perform the permitted functions assigned in Kofax. This software may require access to some ports for internal processes. (I.E. - 1443 for User Datagram Protocol (UDP), Transmission Control Protocol/Internet Protocol (TCP-IP))
- Connect:Direct Secure Plus – This software is required to securely connect and transmit the digital images and metadata created by the Document Capture System. This connection and secure upload will be initiated from NPRC-CPR Document Conversion Unit dedicated workstation through a secure Virtual Private Network (VPN) session using Connect:Direct Secure Plus software. The data upload is an automated process triggered nightly during off-business hours(04:00pm to 04:00am), to the OPM owned Enterprises Human Resources Initiative (EHRI) system at the National Business Center (NBC) in Denver CO. After the upload is completed the EHRI eOPF system will generate Extensible Markup Language (XML) confirmation receipt files that indicate that the transmission was successfully processed, or that errors were encountered with the upload files.
- Seibel Tracking Application – This application was developed by Optimos and contains similar functionality as the Case Management Reporting System (CMRS) system. The application allows end-users (Agencies) to create shipping manifests on boxes of OPF being submitted for Digital Capture work. The application will also allow the end-users(Agencies) to query the application for status information on any given box or OPF submitted.

**Equipment**

<b>Components</b>	<b>Manufacturer / Model</b>	<b>Serial # / Version #</b>	<b>Owner</b>	<b>Physical Location</b>	<b>Logical Location</b>
CPR-DCU1	Dell PowerEdge 2950 Server	D63FDB1	NR	CPR (St. Louis) Room 117	Attached to NARANET via Cisco 4506 Gigabit production switch
CPR-DCU2	Dell PowerEdge 2950 Server	C63FDB1	NR	CPR (St. Louis) Room 117	Attached to NARANET via Cisco 4506 Gigabit production switch
CPR-DCU3	Dell PowerEdge 2950 Server	G63FDB1	NR	CPR (St. Louis) Room 117	Attached to NARANET via Cisco 4506 Gigabit production switch
CPR-DCU4	Dell PowerEdge 2950 Server	F63FDB1	NR	CPR (St. Louis) Room 117	Attached to NARANET via Cisco 4506 Gigabit production switch
Cisco 4506 Switch	Cisco 4506 240-port Gigabit Switch	FOX11370C0H	NHT	CPR (St. Louis) Room 117	Attached to NARANET via primary CPR Production Router
Cisco 3845 Router	Cisco 3845 Router (CPR Primary Router)	FTX0943A11	NHT	CPR (St. Louis) Room 117	Primary CPR Production Router
Dell PowerVault 124 Tape Backup System	Dell PV-124T	CH6FB30629 Firmware v0031	NR	CPR (St. Louis) Room 117	Attached to NARANET via Cisco 4506 Gigabit production switch
Tape Backup Software	Symantec (Veritas) Backup Exec for Windows Servers	101 (10d)	NR	Installed on CPR-DCU4	N/A

**POC**

Richard Morgan or Richard Townsend

**Project Cost(s) To-Date**

Currently gathering data and will add once gathered.

**Appendix III – (Riverside Specific Information)**

***Project(s)***

The FRCP site is offering paper document to electronic format. conversion services for various Federal Agencies.

***Software***

Kofax Ascent Capture 8.0 – These software products perform the capture, form classification and metadata extractions for the conversion to digital formats. These software products require certain processes to have Administration rights. Kofax provides a feature called Security Boost that allows these rights to be assigned to specific users within Kofax. This prevents the Kofax users from performing functions outside of the rights needed to perform the permitted functions assigned in Kofax. This software may require access to some ports for internal processes. (I.E. - 1443 for User Datagram Protocol (UDP), Transmission Control Protocol/Internet Protocol (TCP-IP))

***Equipment***

<b>Components</b>	<b>Manufacturer / Model</b>	<b>Serial # / Version #</b>	<b>Owner</b>	<b>Physical Location</b>	<b>Logical Location</b>
DCU1	Dell PowerEdge 2950 Server				Attached to NARANET via Cisco 4506 Gigabit production switch
Cisco 4506 Switch	Cisco 4506 240-port Gigabit Switch				Attached to NARANET via Cisco 4506 Gigabit production router
Cisco 3845 Router	Cisco 3845 Router (Primary Router)				Attached to NARANET via Cisco 4506 Gigabit production router
Deli PowerVault 124 Tape Backup System	Dell PV-124T				

***POC***

Mike Kretch

***Project Cost(s) To-Date***

Currently gathering data and will add once gathered.

**Appendix IV – (Atlanta Specific Information)**

**Project(s)**

The FRCP site is offering paper document to electronic format. conversion services for various Federal Agencies.

**Software**

Kofax Ascent Capture 8.0 – These software products perform the capture, form classification and metadata extractions for the conversion to digital formats. These software products require certain processes to have Administration rights. Kofax provides a feature called Security Boost that allows these rights to be assigned to specific users within Kofax. This prevents the Kofax users from performing functions outside of the rights needed to perform the permitted functions assigned in Kofax. This software may require access to some ports for internal processes. (I.E. - 1443 for User Datagram Protocol (UDP), Transmission Control Protocol/Internet Protocol (TCP-IP))

**Equipment**

<b>Components</b>	<b>Manufacturer / Model</b>	<b>Serial # / Version #</b>	<b>Owner</b>	<b>Physical Location</b>	<b>Logical Location</b>
DCU1	Dell PowerEdge 2950 Server				Attached to NARANET via Cisco 4506 Gigabit production switch
Cisco 4506 Switch	Cisco 4506 240-port Gigabit Switch				Attached to NARANET via Cisco 4506 Gigabit production router
Cisco 3845 Router	Cisco 3845 Router (Primary Router)				Attached to NARANET via Cisco 4506 Gigabit production router
Dell PowerVault 124 Tape Backup System	Dell PV-124T				

**POC**

Chris Pickney

**Project Cost(s) To-Date**

Currently gathering data and will add once gathered.



## Appendix V – (Fort Worth Specific Information)

### **Project(s)**

The FRCP site is offering paper document to electronic format. conversion services for various Federal Agencies.

### **Software**

Kofax Ascent Capture 8.0 – These software products perform the capture, form classification and metadata extractions for the conversion to digital formats. These software products require certain processes to have Administration rights. Kofax provides a feature called Security Boost that allows these rights to be assigned to specific users within Kofax. This prevents the Kofax users from performing functions outside of the rights needed to perform the permitted functions assigned in Kofax. This software may require access to some ports for internal processes. (I.E. - 1443 for User Datagram Protocol (UDP), Transmission Control Protocol/Internet Protocol (TCP-IP))

### **Equipment**

<b>Components</b>	<b>Manufacturer / Model</b>	<b>Serial # / Version #</b>	<b>Owner</b>	<b>Physical Location</b>	<b>Logical Location</b>
DCU1	Dell PowerEdge 2950 Server				Attached to NARANET via Cisco 4506 Gigabit production switch
Cisco 4506 Switch	Cisco 4506 240-port Gigabit Switch				Attached to NARANET via Cisco 4506 Gigabit production router
Cisco 3845 Router	Cisco 3845 Router (Primary Router)				Attached to NARANET via Cisco 4506 Gigabit production router
Dell PowerVault 124 Tape Backup System	Dell PV-124T				

### **POC**

Kevin Smith

### **Project Cost(s) To-Date**

Currently gathering data and will add once gathered.

## Appendix VI – (Philadelphia Specific Information)

### **Project(s)**

The FRCP site is offering paper document to electronic format. conversion services for various Federal Agencies.

### **Software**

Kofax Ascent Capture 8.0 – These software products perform the capture, form classification and metadata extractions for the conversion to digital formats. These software products require certain processes to have Administration rights. Kofax provides a feature called Security Boost that allows these rights to be assigned to specific users within Kofax. This prevents the Kofax users from performing functions outside of the rights needed to perform the permitted functions assigned in Kofax. This software may require access to some ports for internal processes. (I.E. - 1443 for User Datagram Protocol (UDP), Transmission Control Protocol/Internet Protocol (TCP-IP))

### **Equipment**

<b>Components</b>	<b>Manufacturer / Model</b>	<b>Serial # / Version #</b>	<b>Owner</b>	<b>Physical Location</b>	<b>Logical Location</b>
DCU1	Dell PowerEdge 2950 Server				Attached to NARANET via Cisco 4506 Gigabit production switch
Cisco 4506 Switch	Cisco 4506 240-port Gigabit Switch				Attached to NARANET via Cisco 4506 Gigabit production router
Cisco 3845 Router	Cisco 3845 Router (Primary Router)				Attached to NARANET via Cisco 4506 Gigabit production router
Dell PowerVault 124 Tape Backup System	Dell PV-124T				

### **POC**

Aaron Swan

### **Project Cost(s) To-Date**

Currently gathering data and will add once gathered.

## Appendix VII – (Chicago Specific Information - Future)

### ***Project(s)***

The FRCP site is offering paper document to electronic format, conversion services for various Federal Agencies.

### ***Software***

Kofax Ascent Capture 8.0 – These software products perform the capture, form classification and metadata extractions for the conversion to digital formats. These software products require certain processes to have Administration rights. Kofax provides a feature called Security Boost that allows these rights to be assigned to specific users within Kofax. This prevents the Kofax users from performing functions outside of the rights needed to perform the permitted functions assigned in Kofax. This software may require access to some ports for internal processes. (I.E. - 1443 for User Datagram Protocol (UDP), Transmission Control Protocol/Internet Protocol (TCP-IP))

### ***Equipment***

<b>Components</b>	<b>Manufacturer / Model</b>	<b>Serial # / Version #</b>	<b>Owner</b>	<b>Physical Location</b>	<b>Logical Location</b>
DCUI	Dell PowerEdge 2950 Server				Attached to NARANET via Cisco 4506 Gigabit production switch
Cisco 4506 Switch	Cisco 4506 240-port Gigabit Switch				Attached to NARANET via Cisco 4506 Gigabit production router
Cisco 3845 Router	Cisco 3845 Router (Primary Router)				Attached to NARANET via Cisco 4506 Gigabit production router
Dell PowerVault 124 Tape Backup System	Dell PV-124T				

### ***POC***

Pam Wegner

### ***Project Cost(s) To-Date***

Currently gathering data and will add once gathered.