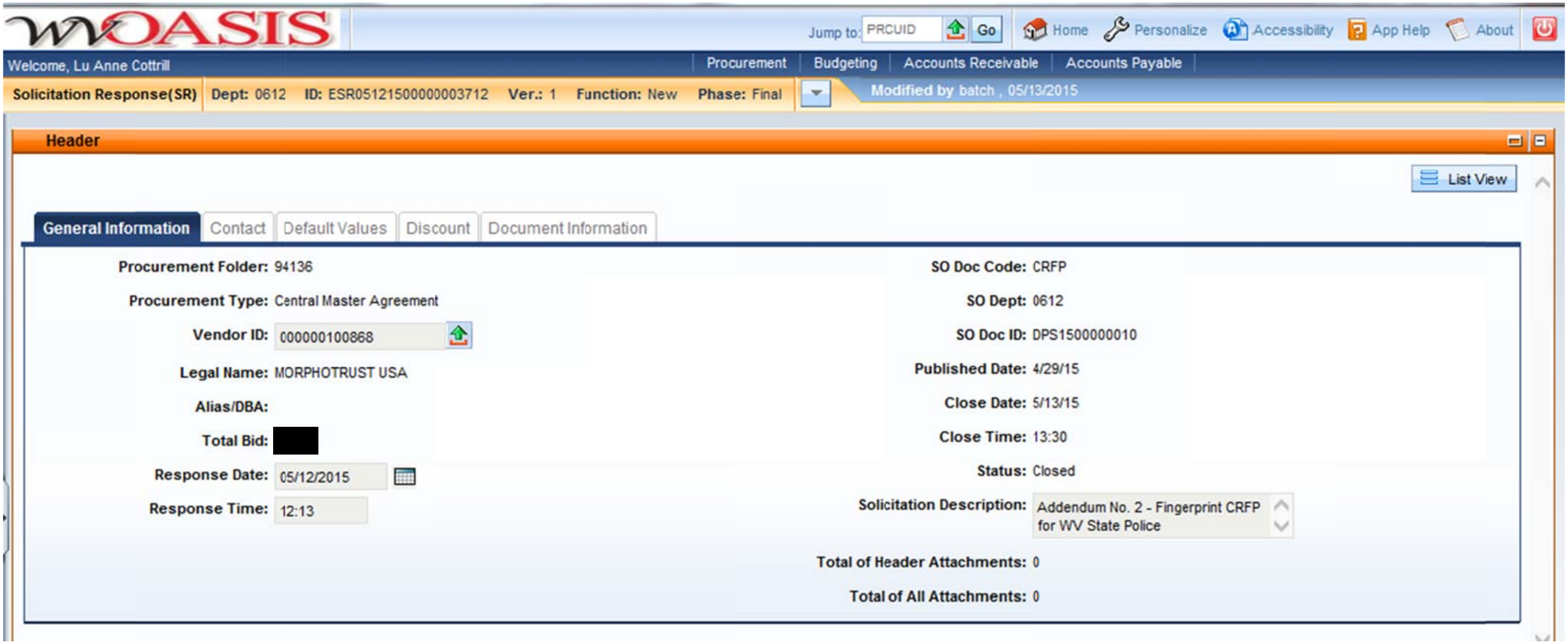
2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

West Virginia Purchasing Division

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.



Welcome, Lu Anne Cottrill

Solicitation Response(SR) Dept: 0612 ID: ESR051215000000003712 Ver.: 1 Function: New Phase: Final

Modified by batch , 05/13/2015

Procurement Folder:	94136	SO Doc Code:	CRFP
Procurement Type:	Central Master Agreement	SO Dept:	0612
Vendor ID:	000000100868	SO Doc ID:	DPS1500000010
Legal Name:	MORPHOTRUST USA	Published Date:	4/29/15
Alias/DBA:		Close Date:	5/13/15
Total Bid:	[redacted]	Close Time:	13:30
Response Date:	05/12/2015	Status:	Closed
Response Time:	12:13	Solicitation Description:	Addendum No. 2 - Fingerprint CRFP for WV State Police
		Total of Header Attachments:	0
		Total of All Attachments:	0

Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder : 94136

Solicitation Description : Addendum No. 2 - Fingerprint CRFP for WV State Police

Proc Type : Central Master Agreement

Date issued	Solicitation Closes	Solicitation No	Version
	2015-05-13 13:30:00	SR 0612 ESR05121500000003712	1

VENDOR

000000100868

MORPHOTRUST USA

FOR INFORMATION CONTACT THE BUYER

Tara Lyle
(304) 558-2544
tara.l.lyle@wv.gov

Signature X **FEIN #** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Fingerprint services	1.00000	LS	$12.50	$12.50

Comm Code	Manufacturer	Specification	Model #
92121602			

Extended Description :

Addendum No. 2 - See attached pages. The bid opening has moved from 05/07/2015 to 05/13/2015. Responses to vendor questions attached.

Applicant Fingerprint Services

MorphoTrust USA

The Identity Company

State of West Virginia
Department of Administration
Purchasing Division

TECHNICAL PROPOSAL

In Response to:
CRFP DPS1500000010
West Virginia State Police
Applicant Fingerprinting Services

Submission Date:
May 13, 2015

Submitted via wvOASIS to:
Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Authorized Signature:

Robert Eckel
CEO and President

FINGERPRINTING SERVICES

Submitted by:
MorphoTrust USA, LLC
296 Concord Road, Suite 300
Billerica, Massachusetts 01821
www.morphotrust.com

Contact:
John Olson
Principal Proposal Manager
Telephone: 952-945-3307
Fax: 952-932-7181
Email: jolson@morphotrust.com

SAFRAN
MorphoTrust USA

Confidential Notice

Certain information in this proposal is protected from disclosure to the public because it is a proprietary trade secret or confidential commercial or financial information of MorphoTrust USA, LLC or its affiliates (individually and collectively, “MorphoTrust USA” or “MorphoTrust”).

MorphoTrust has endeavored to identify each page of its proposal that contains any such proprietary or confidential information with the legends “**COMPANY CONFIDENTIAL – Not for Public Disclosure**” or “PROPRIETARY” (or words of similar import) somewhere on the relevant page or pages of its proposal. MorphoTrust’s proposal includes all exhibits and appendices thereto, as well as all extrinsic documents and materials that may be identified and incorporated therein by specific reference. MorphoTrust’s proprietary information typically includes, but is not limited to, information related to proprietary security features and related designs, techniques and materials, formulas, manufacturing methods, business plans, pricing and other financial information, technology and product roadmaps, and customer lists and references. Subject to applicable law, such proprietary or confidential information may not be disclosed (pursuant to freedom of information legislation or otherwise), reproduced in whole or in part, or used for any purpose other than the recipient’s evaluation of this proposal, without the prior written consent of an executive officer or the General Counsel of MorphoTrust USA, LLC.

Our Mission

To simplify, protect and secure the lives of the American people.

COPYRIGHT AND TRADEMARKS

SAFRAN
MorphoTrust USA

May 11, 2015

Tara Lyle
Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Subject: **MorphoTrust Response to CRFP DPS1500000010 for West Virginia State Police Applicant Fingerprinting Services**

Dear Ms. Lyle:

Please find enclosed our response to your CRFP DPS1500000010 for statewide applicant fingerprinting services. MorphoTrust USA, LLC (MorphoTrust) has been fingerprinting applicants in the State of West Virginia since 2011 and today serves nearly 70,000 applicants annually. We are excited to expand our partnership with the West Virginia State Police.

Our proposal illustrates how our proven solutions, qualifications, and capabilities will meet all of the requirements of this CRFP and will continue to serve the State Police and the residents of West Virginia. Throughout our response we have made an effort to show proof points from the current program in place today in the State of West Virginia.

We are committed to providing the highest levels of customer service and a quality experience for each applicant. We also commit to developing a strong, long-term partnership in delivering high quality electronic fingerprinting services, building on an already successful program.

This submittal letter is signed by Mr. Robert Eckel, who is authorized to legally bind MorphoTrust to fulfill the performance and pricing commitments outlined in this proposal. In addition, please send all notices relative to a contract to Mr. John Olson, email address: jolson@morphotrust.com.

Thank you for your time and consideration.

Sincerely,

Robert Eckel
President and Chief Executive Officer

REQUEST FOR PROPOSAL

(West Virginia State Police, Applicant Fingerprinting Services)

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

MorphoTrust USA, LLC
(Company)

(Representative Name, Title) Robert Eckel, President and CEO

978-215-2400
(Contact Phone/Fax Number)

April 24, 2015
(Date)

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP DPS1500000010

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X] Addendum No. 1

[X] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

MorphoTrust USA, LLC
Company

Authorized Signature

May 8, 2015
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Proposal
31 — Public Safety

Proc Folder: 94136

Doc Description: Applicant Fingerprint Services

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2015-04-01	2015-04-28 13:30:00	CRFP 0612 DPS1500000010	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Name, Address and Telephone Number:

MorphoTrust USA, LLC
296 Concord Road, Suite 300
Billerica, Massachusetts 01821
978-215-2400

FOR INFORMATION CONTACT THE BUYER

Tara Lyle
(304) 558-2544
tara.l.lyle@wv.gov

Robert Eckel, President and CEO

Signature X **FEIN #** 04-3320515 **DATE** April 24, 2015

All offers subject to all terms and conditions contained in this solicitation

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Proposal
31 — Public Safety

Proc Folder: 94136

Doc Description: Addendum No. 1 - Extend bid opening; Fingerprint CRFP

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2015-04-22	2015-05-07 13:30:00	CRFP 0612 DPS1500000010	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Name, Address and Telephone Number:

MorphoTrust USA, LLC
296 Concord Road, Suite 300
Billerica, Massachusetts 01821
978-215-2400

FOR INFORMATION CONTACT THE BUYER

Tara Lyle
(304) 558-2544
tara.l.lyle@wv.gov

Signature X Robert Eckel, President and CEO **FEIN #** 04-3320515 **DATE** April 24, 2015

All offers subject to all terms and conditions contained in this solicitation

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Proposal
31 — Public Safety

Proc Folder: 94136

Doc Description: Addendum No. 2 - Fingerprint CRFP for WV State Police

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2015-04-29	2015-05-13 13:30:00	CRFP 0612 DPS1500000010	3

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Name, Address and Telephone Number:

MorphoTrust USA, LLC
296 Concord Road, Suite 300
Billerica, Massachusetts 01821
978-215-2400

FOR INFORMATION CONTACT THE BUYER

Tara Lyle
(304) 558-2544
tara.l.lyle@wv.gov

Signature X Robert Eckel **FEIN #** 043320515 **DATE** May 8, 2015

All offers subject to all terms and conditions contained in this solicitation

RFQ No. CRFP 0612 DPS 1500000010

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

MANDATE: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: MorphoTrust USA, LLC

Authorized Signature: ______________ Date: April 24, 2015

State of Massachusetts

County of Middlesex, to-wit:

Taken, subscribed, and sworn to before me this 10th day of April, 2015.

My Commission expires 7/9, 2021.

AFFIX SEAL HERE

AMY E. YOUNG
Notary Public
COMMONWEALTH OF MASSACHUSETTS
My Commission Expires
July 9, 2021

NOTARY PUBLIC Amy E Young

Table of Contents

Executive Summary

No Risk Evolution of our Proven West Virginia Solution to our Next Generation Enrollment Software Platform

MorphoTrust currently serves the citizens and agencies of West Virginia and we have met your call to action.

Significant investment in our AFIS interface, customized User Agency workflow, and program infrastructure allow us to understand and meet your needs now and in the future.

We will expand and upgrade the current network to incorporate innovative new features of our Universal Enrollment Platform (UEP).

The West Virginia Department of Administration, Purchasing Division seeks an experienced vendor to serve the residents of West Virginia by providing statewide electronic Livescan fingerprinting services for state and private agencies in conjunction with licensing, volunteering, employment responsibilities, or any other required non-criminal justice fingerprinting purposes currently being processed by or through the State Central Repository.

MorphoTrust USA, LLC (MorphoTrust) submits the enclosed response to this opportunity to provide Applicant Fingerprint Services.

A Trusted Partner in West Virginia

Since 2011, we have enjoyed a collaborative relationship with the State of West Virginia and the agencies serviced by the program. Our joint success in growing a program that serviced over 70,000 applicants in 2014 is due to much more than simply collecting fingerprints.

Together, West Virginia and MorphoTrust have deployed a fingerprinting service that is critical for protecting the citizens in your communities. Our commitment as a partner to you is rooted in our mission statement: "***To simplify, protect and secure the lives of American people***." While our first priority is safety, we also partner with agencies like you to deliver an innovative user experience that simplifies the customer applicant process. In addition to the high value we place on the end-user experience, our solution places equal importance on supporting the agencies that must manage complex criminal history reporting workflows.

Since 2012, we have met with more than 50 major West Virginia agencies and we have designed, developed, and deployed customized solutions for many of these agencies, enabling efficient backend processing for criminal history management. These solutions include extensive reporting, status notifications via email, optional billing account services, and other features. With thousands of hours invested by agencies and MorphoTrust in creating these solutions, it is critical that any new system not disrupt the existing environment.

Our significant investment in these customized solutions, our experienced program management team, and the West Virginia infrastructure we have already in place make MorphoTrust the clear choice for this procurement.

Our Priorities are Quality of Service and Customer Support

In early 2013, the Select Committee on Public Employees Insurance Agency (PEIA) called our attention to a need for improvement and challenged us to bring forward a plan to resolve and improve processes within the state. MorphoTrust acknowledged these issues and our team embraced a ***call to action*** to make immediate adjustments to the program, seizing the opportunity to build a level of trust with both the West Virginia State Police and the agencies represented. The Select Committee asked for and received monthly written progress reports detailing the program refinements that we implemented to deliver on our promise of improvement.

MorphoTrust has met the challenge and delivered on our promises.

Through meetings with West Virginia state agencies, school systems, and the State Police, we identified specific program problem areas needing our immediate and long-term attention. The state requested immediate resolution of three specific high-priority items shown in Table 1. We have resolved all issues, both reported and observed.

Table 1: West Virginia Program Improvements

Program Request	Status on January 8, 2013	Status Today
Reduce the average wait time from fingerprint capture to result issuance	Average 6.78 days from capturing fingerprints to printing result letters	Average 3.44 days from capturing fingerprints to printing the result letters
Resolve billing issues, improve customer service, provide faster resolution of issues	Inaccurate, untimely billing statements	Regular, routine, and accurate billing statements

Program Request	Status on January 8, 2013	Status Today
Improve Enrollment Center coverage across the state of West Virginia	12 Enrollment Centers	22 Enrollment Centers

Working through these challenges resulted in a number of benefits to program stakeholders including:

- Better communication with West Virginia State Police and the User Agencies
- Improved responsiveness and customer service
- A better understanding of the needs of each agency
- Proof that we say what we do and do what we say
- A solid relationship built through adversity

As we move into the future, please know that MorphoTrust will continue to prove our commitment to the success of this program, by devoting the time and resources necessary to resolve all outstanding program-related issues and by making quality of service to the State of West Virginia our #1 objective.

Upgrade to Advanced Technology

Together we have built the trusted and reliable fingerprinting service for West Virginia citizens that is in place today. MorphoTrust's commitment to our partner agencies is to continue to innovate. We propose a ***NO RISK*** upgrade our next-generation advanced technology Universal Enrollment Platform (UEP) during the first year of the new contract.

UEP – An Award Winning Product

As evidence of the success of UEP, the TSA Pre✓® program recently received the *ACT-IAC Igniting Innovation Dynamite Award* for the Greatest Citizen Impact and the 2015 *SAFRAN Innovation Award* for Customer Satisfaction.

UEP has been in use since 2013 for our fingerprinting services contract with the U.S. Department of Homeland Security, Transportation Security Administration (TSA), which includes the popular TSA Pre✓® program. Our TSA program serves more than 1.5 million customers annually in more than 330 Enrollment Centers throughout the United States and currently maintains a customer satisfaction rate of over 99.8% based on applicant surveys.

UEP is also operational for our state fingerprinting services program in Texas. Just as we are doing Texas, we will phase in a UEP deployment in West Virginia while maintaining your current system, to prevent downtime or disruption in the State's service.

UEP offers the following benefits for West Virginia agencies and applicants:

- ***New Livescan enrollment workstations*** deployed to all Enrollment Centers, which will reduce equipment downtime.
- ***Improved fingerprint quality***, which will lower rejection rates.
- ***Simpler and more intuitive registration process***, which will improve the online experience and reduce calls to our Customer Service Center.
- ***Identity document authentication***.
- ***Automated internal transaction monitoring and auditing***.
- A suite of ***advanced site-utilization monitoring and scheduling lead-time tools*** as optional enhancements to the UEP product.
- ***Out-of-State Electronic Fingerprinting*** in selected cities throughout the country, using local operating procedures and technology.

UEP will secure the State of West Virginia's position as the leader in state fingerprint enrollment technology with the latest solutions for data integrity, image and photo quality, interstate electronic submissions, and optional enhanced features for automated delivery status and real-time program metric dashboards.

We appreciate the opportunity to have served the State of West Virginia as a trusted, proven, and reliable partner. We look forward to bringing you our latest fingerprint services platform to deliver state-of-the-art services to serve you in the future.

Our proposal response is organized as follows, in compliance with the RFP instructions:

Technical Proposal

- Cover Letter with required forms
- Vendor Response Sheet (Attachment A)
  - Section 4, Subsection 4.3: Qualifications and Experience
  - Section 4, Subsection 4.4: Project and Goals
- Mandatory Specification Checklist (Attachment B)
  - Section 4, Subsection 4.5: Mandatory Requirements

Cost Proposal - Enclosed in a separate sealed envelope in our submission package

Exempt Information – Separate volume containing information to be exempt from public disclosure

Bid Bond – Submitted directly (see Appendix G for copy)

Vendor Response Sheet (Attachment A)

Since 2011, MorphoTrust has provided fingerprinting services for more than 220,000 West Virginia applicants. We propose an experienced Program Manager and project team for the West Virginia Applicant Fingerprinting Services program, from a company with past performance in fingerprinting more than 21 million applicants over the past 20 years.

Section 4, Subsection 4.3: Qualifications and Experience

4.3 Vendors will provide information regarding their firm, such as staff qualifications and experience in completing similar projects; references; copies of any staff certifications or degrees applicable to this project; proposed staffing plan; descriptions of past projects completed entailing the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.

MorphoTrust Company Information

MorphoTrust is the industry's leading fingerprinting services company, currently operating 26 state and federal fingerprinting services programs. We have fingerprinting Enrollment Centers in all 50 states and the District of Columbia, strategically deployed to support the volumes and unique geographic needs of each specific program.

In addition to our state government programs, MorphoTrust's fingerprinting services are used nationwide for the U.S. Department of Homeland Security, Transportation Security Administration's (TSA) program.

Notable Achievements

MorphoTrust has received several accolades for our performance, including the following recent awards:

2013 North American Company of the Year for Government Biometrics

MorphoTrust USA, LLC

FROST & SULLIVAN
2013
BEST PRACTICES AWARD
NORTH AMERICAN GOVERNMENT BIOMETRICS COMPANY OF THE YEAR AWARD

NIST Biometrics Performance

MorphoTrust's biometric solutions are regularly recognized for accuracy and performance by the independent reports issued by the National Institute of Standards and Technology (NIST).

North American Government Biometrics Company of the Year Award

We are proud to have been recognized by a 2013 Frost and Sullivan "Company of the Year Award." Frost & Sullivan is in its 50th year in business with a global research organization of 1,800 analysts and consultants who monitor more than 300 industries and 250,000 companies.

Key benchmarking criteria for the award include:

- Leadership in Customer Value
- Grown Implementation Excellence
- Degree of Innovation with Products and Technologies

NorthFace "World-Class" Customer Service

We are honored to be a four-time recipient of a NorthFace ScoreBoard Award (SM) for delivering "World-Class" Customer Service from the Omega Management Group Corp. The NorthFace ScoreBoard (NFSB) award is presented annually to companies who, as rated solely by their own customers, achieved excellence in customer satisfaction and loyalty during the prior calendar year.

Staff Qualifications and Experience

Figure 1 shows our organization chart for the West Virginia Applicant Fingerprinting Services program. Key icons designate MorphoTrust personnel who are we consider to be critical to the success of this program.

The personnel assigned to our West Virginia project team represent one of the most experienced teams available. Seven team members listed on our organizational chart have more than eight years of direct Livescan services industry experience.

Our Executive Advisory Board, identified in the organizational chart, will meet regularly during the contract period to assure a smooth deployment, monitor performance, and encourage program improvements throughout the life of the contract.

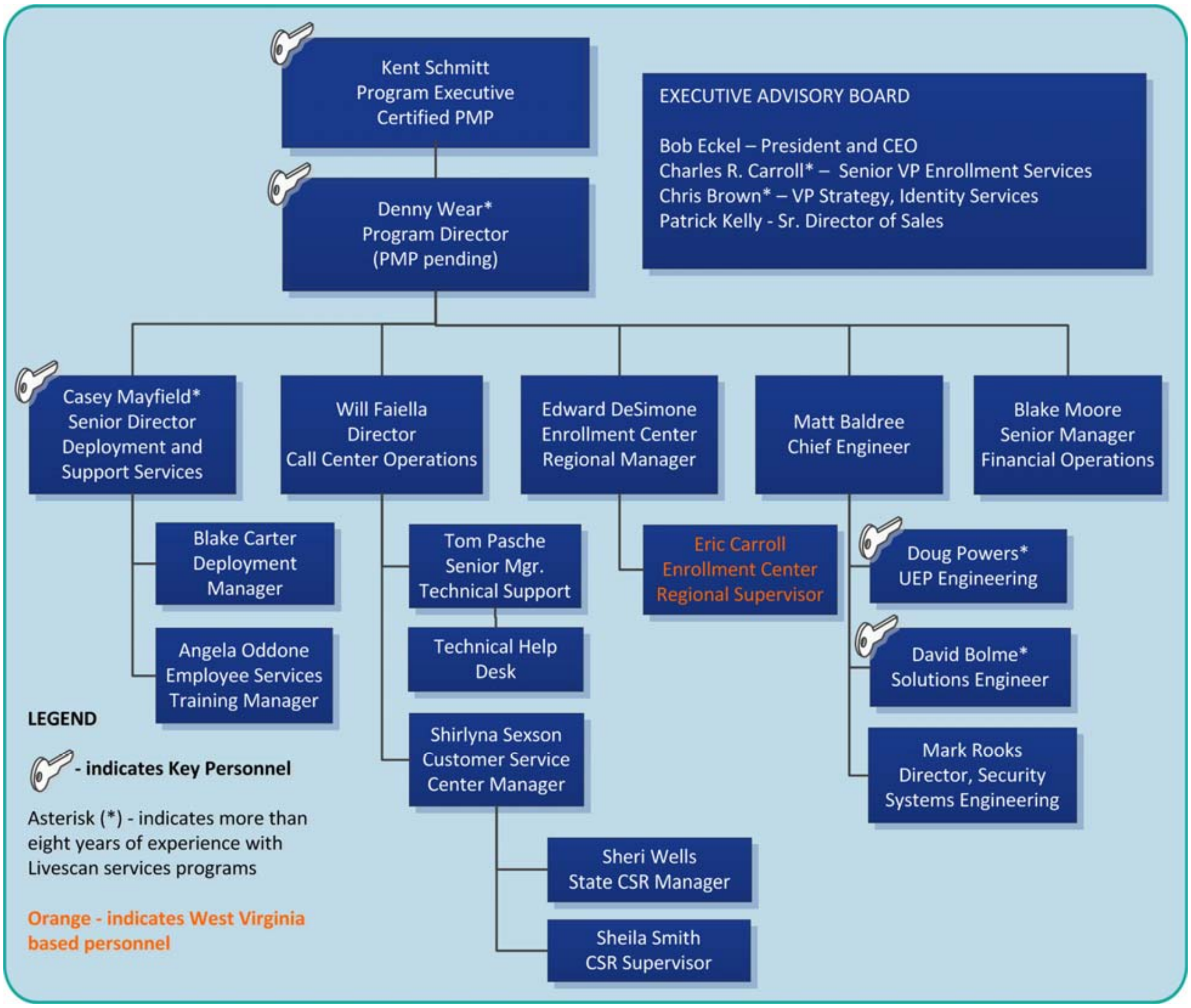


Figure 1: MorphoTrust's Project Team for West Virginia Applicant Fingerprinting Services

The following brief biographies summarize the demonstrated experience of each key project team member in providing West Virginia fingerprinting services.

Kent Schmitt, PMP — West Virginia Account Executive

As Account Executive for the West Virginia Applicant Fingerprinting Services program, Kent Schmitt will provide program oversight and hold ultimate responsibility to make sure all contractual and programmatic requirements are met. He will serve as liaison between the Program Manager and the MorphoTrust Executive Advisory Board to ensure that all necessary resources are provided to support the West Virginia contract. He will also serve as the Executive Point of Contact for West Virginia executives.

Mr. Schmitt is an experienced Program and Project Management professional who has provided strategic leadership and tactical management for multiple federal Government contracts. He is a certified Project Management Professional (PMP) and holds a Bachelor of Science (BS) in Mathematics from Pennsylvania State University.

As MorphoTrust's Program Manager for TSA Universal Enrollment Services, he has been responsible for contract performance and compliance as well as day-to-day management of MorphoTrust's Enrollment Services under the TSA Universal Enrollment Services contract. Through his leadership, MorphoTrust successfully transitioned the legacy Transportation Worker Identification Credential (TWIC) and HazPrint Enrollment Center network to Universal Enrollment Services.

During 2013 and 2014, Mr. Schmitt led MorphoTrust's team to expand the Universal Enrollment Services network to support the newly created TSA Pre✓® application program services, which recently received the ACT-IAC Igniting Innovation Dynamite Award for the Greatest Citizen Impact and the 2015 SAFRAN Innovation Award for Customer Satisfaction.

Mr. Schmitt also manages MorphoTrust's Identity Services nationwide network of 1,200 Enrollment Centers and program management team that serves MorphoTrust's federal and state agency clients and their respective customers.

Mr. Schmitt has been with MorphoTrust since 2012. His customer references include the U.S. Department of Homeland Security, Transportation Security Administration.

Denny Wear — Program Manager

Our program manager, Denny Wear, has been with MorphoTrust for over 15 years, most recently as Program Manager for Livescan fingerprinting service programs. He has been instrumental in the successful deployment of large-scale statewide fingerprint networks including Massachusetts, the District of Columbia, New York, and Indiana, as well major expansion of the Florida statewide network and a fingerprint and identification badging solution for Broward County, Florida School Board, the nation's sixth largest school system.

Mr. Wear has been Program Manager specifically for the West Virginia network for more than two years. He will continue in his role, serving as the single point of contact for the West Virginia State Police for MorphoTrust's performance in support of the contract.

During the implementation phase, Mr. Wear will facilitate the flow of information from WVSP to the appropriate MorphoTrust workgroup and will manage the delivery of all program components. He will host regular meetings with WVSP and MorphoTrust personnel to ensure all matters are communicated clearly and issues are addressed in a timely manner. He will be responsible for day-to-day operations at all Enrollment Centers and will work with the stakeholders and State representatives to resolve any issues or problems that occur at Enrollment Centers in a timely manner.

Mr. Wear holds a Bachelor's Degree in Accounting from Illinois College. His program references include Massachusetts, West Virginia, and the District of Columbia.

Casey Mayfield — Deployment Director

As Deployment Director, Casey Mayfield will ensure that all tasks related to successful deployment are achieved in a timely manner. She will coordinate with all teams involved in deployment activity to ensure a unified program rollout.

Ms. Mayfield has 16 years of experience managing fingerprinting services networks. She oversees the deployment of all new civil applicant fingerprinting programs for MorphoTrust and the ongoing management of more than 700 subcontractors for MorphoTrust state, federal, and commercial networks nationwide.

Under her leadership, her team is in contact with more than 7,000 applicants each day and they routinely exceed customer service and other program requirements in each program they support. Her group also provides support services such as Cardscan and site support services.

In total, Ms. Mayfield has more than 19 years of business management and human resources experience. She has extensive supervisory and training experience and has been instrumental in establishing effective policies and procedures for the operation of each area under her responsibility. Her organizational skills and ability to delegate efficiently enable her to successfully manage multiple areas of responsibility.

Ms. Mayfield holds a B.A. in Criminal Justice from the University of Illinois at Springfield and an A.A.S. in Law Enforcement from the Lincoln Land Community College. Her program references include U.S. Department of Homeland Security, Transportation Security Administration, New York Division of Criminal Justice Services, Tennessee Bureau of Investigation, Department of Administration (Indiana State Police), and Texas Department of Public Safety.

Doug Powers — UEP Engineering

Doug Powers coordinates all product design and engineering activities for MorphoTrust's Universal Enrollment Platform. He has more than 15 years of experience in software and product engineering, with over eight years of experience in engineering leadership.

Mr. Powers began his career in identity and biometric solutions in 1999 with ChoicePoint, and has worked with a number of government agencies including the Federal Bureau of Investigation, the National Center for Missing and Exploited Children, the Transportation Security Agency, and the New Jersey State Police. He has been credentialed by the Agile Alliance as a Certified Scrum Master and Certified Product Owner.

Mr. Powers holds a Bachelor's of Science in Computer Science from the Georgia Institute of Technology (Georgia Tech). His program references include the Texas Department of Public Safety and the U.S. Department of Homeland Security, Transportation Security Administration.

David Bolme, PMP — Solutions Engineer

David Bolme will serve as Solutions Engineer, providing program oversight for engineering efforts, ensuring that the State's needs are being met by our solution, and resolving any issues that may arise. He has more than 20 years of experience in planning, implementing, and managing complex and integrated systems.

Mr. Bolme has been with MorphoTrust for more than 10 years. He manages all of MorphoTrust's state fingerprinting contracts and has led the implementation of major MorphoTrust projects such as Tennessee, Indiana, Florida, South Carolina, Maryland and Nevada.

Prior to MorphoTrust, Mr. Bolme was responsible for the development and management of major information systems programs for the Tennessee Bureau of Investigation. He holds a Bachelor's of Science in Computer Science from Tennessee Technological University and Project Management Professional (PMP) certification. His program references include the Tennessee Bureau of Investigation.

Staffing Plan

In addition to the project personnel shown in our organization chart (Figure 1), MorphoTrust's proposed staffing for the West Virginia program includes 30-40 Enrollment Agents (more than 30 of whom are currently vetted and trained on the program), 3-6 Customer Service Representatives (three of whom are currently on staff), and additional support personnel who are mostly on our staff today.

Descriptions of Past Projects

In Table 3 through Table 8, MorphoTrust has provided detailed descriptions of six past projects we have successfully completed, including the location, project manager name and contact information, type of project, and an overview of MorphoTrust's approach to meeting the project goals and objectives.

In addition, Table 2 provides a snapshot view of the six fingerprint networks we currently provide in Texas, Tennessee, Massachusetts, New York, Michigan, and for the TSA Universal Enrollment Services program, in comparison to the West Virginia network. Our success with these projects demonstrates that we will accomplish the goals of the West Virginia program. We encourage the evaluation team for the State of West Virginia to speak with them to learn about our successes and challenges in rolling out a hosted fingerprinting solution.

Table 2: Examples of MorphoTrust Programs Similar to West Virginia

Attribute	West Virginia Proposed Network	Texas	Tennessee	Massa-chusetts	New York	Michigan	TSA Universal Enrollment Services
Number of sites	**27**	148	50	32	102	55	330
Annual Volume	**65,000**	800,000	225,000	150,000	300,000	150,000	1.5 million
Contract Period	**2011 - Present**	2005 - Present	2001-2006 2011-Present	2014-Present	2009-Present	2005-2010 2013-Present	2012-Present
Geographic Coverage	**Statewide**	Statewide	Statewide	Statewide	Statewide	Statewide	Nationwide
Square mileage	**24,230**	261,797	42,143	10,550	54,520	96,700	3.8 M
Location strategy	**Fixed and Mobile**	Fixed and Mobile	Fixed and Mobile	Fixed and Mobile	Fixed and Mobile	Fixed and Mobile	Fixed and Mobile
Full Operational Capability	**12 weeks**	12 weeks	6 weeks	16 weeks	16 weeks	9 weeks	12 months (IOC 12 weeks)
Central Server (single transmission point)	**Yes**	Yes	Yes	Yes	Yes	Yes	Yes
AFIS Interface	**Yes**	Yes	Yes	Yes	Yes	Yes	Yes
Pre-enrollment Web site	**Yes**	Yes	Yes	Yes	Yes	Yes	Yes
Pre-enrollment Call Center	**Yes**	Yes	Yes	Yes	Yes	Yes	Yes

Attribute	West Virginia Proposed Network	Texas	Tennessee	Massa-chusetts	New York	Michigan	TSA Universal Enrollment Services
Fee Collection and Remittance	**Yes**	Yes	Yes	Yes	Yes	Yes	Yes
Cardscan for non-resident applicants	**Yes**	Yes	Yes	No	Yes	Yes	Yes
Manual fingerprinting	**Yes**	Yes	No	No	No	No	No
Signature capture	**Yes**	No	No	No	No	No	Yes
User agency Interfaces	**No**	Yes	Yes	Yes	Yes	Yes	Yes
Results Management/Dissemination	**Yes**	No	Yes	Pending	No	No	Yes

In total, our network currently services over 4.5 million customers annually at over 1,200 digital Enrollment Centers across the United States.

4.3.1 The Vendor must have at least 3 (three) successful statewide Applicant fingerprinting networks of similar size and scope (equipment installation/training projects are not considered of similar scope) and provide references of such projects.

We have provided successful statewide applicant fingerprint networks for the states of Texas, Tennessee, and Massachusetts. Contact information, size and scope of networks and other required information are noted in the following Table 3 through Table 5.

4.3.2 References must include projects where services such as call center, employment of live scan operators, centralized data center, and fee collection were provided including:

- Company name, address and telephone number
- Contact person name, title, business address, phone number and email address
- Annual fingerprint volume
- Brief description of the services provided
- List the agency or agencies using the network
- Description of the technical solution including systems and applications installed
- List of fingerprinting centers including the hours of availability
- Letter of recommendation

In Table 3 through Table 5, MorphoTrust has provided the required contact information for three of our fingerprinting programs that are comparable to West

Virginia Applicant Fingerprinting Services including call center, employment of live scan operators, centralized data center, and fee collection.

In Appendix C we have provided a list of the Enrollment Centers for each of these programs and in Appendix D we have provided letters of reference.

Table 3: Texas Department of Public Safety

Company	Texas Department of Public Safety
Company Address and Telephone Number	5805 North Lamar Blvd, Building G Austin, TX 78752-4431 512-424-2000
Contact Person	Mike Lesko, Chief – Crime Records Service 5805 North Lamar Blvd, Building G Austin, TX 78752-4431 512-424-2524 mike.lesko@txdps.state.texas.us
Annual Fingerprint Volume	800,000

Description of Services

In early 2006, MorphoTrust was chosen by the Texas Department of Public Safety to establish a statewide fingerprinting network, Fingerprint Applicant Service of Texas (FAST), with locations throughout the state to provide fingerprinting services to both urban and rural areas of the state. MorphoTrust was recently awarded a new contract in Texas which extends our relationship until August, 2021.

Currently we fingerprint between 50-60,000 applicants each month and have almost 150 fingerprinting centers operating currently throughout the state. We provide the following services in association with this network:

- Bi-lingual appointment scheduling by phone to Call Center or through secure website
- Convenient Enrollment Centers equipped with Enrollment Workstations and Enrollment Agents (Livescan operators)
- Card Scan for out-of-state applicants
- Customized agency system integration
- Centralized data center
- Electronic connection to the state AFIS Reporting
- Administrative Queue Review
- Fee Collection
- Customer account and billing services
- Onsite fingerprinting for groups of 30 or more

Use of the MorphoTrust Administrative Queue Review product which consolidates all background check results and allows staff to automatically disposition ‘no-hit’ records, has allowed Texas DPS to streamline their backend process. Staff is able to print or send all dispositioned result letters with a single command. This allows for increased traffic of electronic submissions of civil applicant records with less need for manual intervention by Texas DPS staff, making the most of limited staffing resources.

Many of the State licensing agencies were not prepared to utilize the service without making significant modifications to their internal processes. MorphoTrust worked closely with these individual agencies to create customized systems that provided efficient services for the agencies involved as well as for the applicant within the context of the network.

<table>
<tr><th>Company</th><th>Texas Department of Public Safety</th></tr>
<tr><td colspan="2">The State of Texas has an established E-Pay system used to facilitate the collection of fees for services provided by State agencies. MorphoTrust technical staff successfully integrated the MorphoTrust components of the FAST program into the E-Pay system. This allows applicants who must pay licensure fees to pay for the fingerprinted fees at the same time in a secure web-based environment, greatly simplifying the process for the applicant and for agencies.

We developed a customized web-based solution for the Texas Board of Nursing, Department of Family Protective Services (DFPS), Real Estate Commission (TREC) and State Board of Educator Certification (SBEC) which verifies that applicants scheduling appointments for fingerprinting have been approved by the agency to complete the process. This solution saves time, money and frustration for the agencies and applicants by ensuring that all required steps for certification or licensing are taken before the applicant is fingerprinted.

In 2007, the Texas State Board of Education (SBEC) was given a mandate to comply with requirements to obtain a fingerprint-based background check on every certified teacher throughout the state (approximately 400,000) within 4 years from passage of the legislation. We worked closely with SBEC to develop a plan (The Blitz) to conduct on-site fingerprinting sessions for more than 1,200 Independent School Districts at more than 8,000 campuses in a manner that would satisfy all of their requirements in their timeframe. Out of these planning sessions, we expanded the responsibilities of one of our major minority subcontractors with extensive fingerprinting experience, MRi, to hire “Blitz Teams” which would work within a geographical region to visit each campus according to schedules developed each quarter by MorphoTrust and SBEC personnel. Schedules are developed to take into consideration holiday and testing dates and were refined with local and District-specific or campus considerations. As an added convenience, certified teachers were also able to use our established Enrollment Centers to complete their fingerprinting requirements if they were unavailable during the time MorphoTrust Blitz Teams visited their campus.

MorphoTrust provides fingerprinting for applicants at the TxDPS Headquarters office in Austin, TX, having taken over this service from TxDPS staff, freeing them for other duties.</td></tr>
<tr><td>Participating Agencies</td><td>Sole Source Statewide Network – includes all State agencies required to obtain fingerprint-based background checks, such as Board of Nursing, Board of Pharmacy, Department of Insurance, Department of Family and Protective Services, Real Estate Commission, and Board of Education.</td></tr>
<tr><td>Description of Technical Solution</td><td>Upgrade from legacy technology to Universal Enrollment Platform (UEP)
MorphoTrust Live Scan system
MorphoTrust Store and Forward Server
Secure connection to State AFIS
Cisco Virtual Private Network encryption of data transfer circuits
Proprietary registration, back end and billing software
Customized agency system integration and data sharing protocols
Photo capture system
Card scan system</td></tr>
<tr><td>List of Fingerprinting Centers (with hours of operation)</td><td>Included in Appendix C</td></tr>
<tr><td>Letter of Recommendation</td><td>Included in Appendix D</td></tr>
</table>

Table 4: Tennessee Bureau of Investigation

Company	Tennessee Bureau of Investigations
Company Address and Telephone Number	901 R.S. Gass Blvd. Nashville, TN 37216 615-744-4000
Contact Person	Brad Truitt Assistant Director for Information Services 901 R.S. Gass Blvd. Nashville, TN 37216 615-744-4008 brad.truitt@tn.gov
Annual Fingerprint Volume	225,000

Description of Services

MorphoTrust provides a full-service network of civil applicant fingerprinting services for the State of Tennessee. Under this statewide single source solution, referred to as TAPS, MorphoTrust provides fingerprinting services to more than 20,000 education professionals throughout the State of Tennessee annually.

We provide the following services in association with our TBI network:

- Bi-lingual registration assistance by telephone to Call Center
- Secure bilingual web registration and scheduling portal
- Convenient statewide Enrollment Centers equipped with Enrollment Workstations/ Livescan equipment and Enrollment Agents (Livescan operators)
- Card Scan for out-of-state applicants
- Customized agency system integration
- Central data center
- Electronic connection to the state AFIS
- Reporting
- Fee Collection and remittance
- Customer account and billing services

In June 2011, MorphoTrust was re-awarded the contract to operate TAPS program. Within 35 days of contract award, MorphoTrust performed a successful end-to-end system test, secured 60 Enrollment Center sites, and procured all Live Scan systems required for the program. The network was fully operational seven weeks from contract execution with no interruption of services. We activated the registration Call Center and website during the week before the August 1 deadline to enable applicants to begin fingerprinting on August 1.

Additional tasks performed by MorphoTrust included developing customized interfaces with major state agencies to allow data and reporting exchanges so that those agencies would also experience no interruption to their workflow. We met with each state agency participating in the network prior to “go live” to discuss their specific network needs and previous pain points to ensure our network met the needs of the agencies and their applicants. We developed an information sheet and application packet which TBI distributed to all user agencies providing information about the network changes and steps to setting up an account with MorphoTrust, should they require this service. By the first week of service we had established almost 140 escrow accounts for Tennessee user agencies and fingerprinted more than 3,500 applicants.

Because of MorphoTrust’s experience in deploying networks, we were able to accomplish a successful transition within the extremely tight time frame required by TBI with no interruption of service to applicants.

Company	**Tennessee Bureau of Investigations**
Participating Agencies	Sole Source Statewide Network – includes all State agencies required to obtain fingerprint-based background checks, including the Department of Human Services, Department of Children's Services, Department of Mental Health, Department of Commerce and Insurance, Department of Safety, Health Care, Department of Transportation, and Tennessee Supreme Court
Description of Technical Solution	MorphoTrust Live Scan system MorphoTrust Store and Forward Server Proprietary registration, back end and billing software Secure connection to State MorphoTrak AFIS Cisco Virtual Private Network encryption of data transfer circuits Customized agency system integration and data sharing protocols Photo capture system MorphoTrust iA-thenticate document authentication system Card scan system
List of Fingerprinting Centers (with hours of operation)	Included in Appendix C
Letter of Recommendation	Included in Appendix D

Table 5: Massachusetts Executive Office of Public Safety

Company	Massachusetts Executive Office of Public Safety
Company Address and Telephone Number	One Ashburton Place, Room 2133 Boston, MA 02108 614-727-7775
Contact Person	Curtis Wood, Undersecretary for Forensic Science and Technology The Commonwealth of Massachusetts Executive Office of Public Safety and Security One Ashburton Place, Room 2133 Boston, MA 02108 614-727-7775, Ext 25512 Curtis.Wood@state.ma.us
Annual Fingerprint Volume	150,000
Description of Services	MorphoTrust was chosen as the statewide vendor for live scan fingerprint submissions to MA EOPSS in 2013. Program requirements include 30 fingerprinting centers across the state, supporting 100,000 – 200,000 applicants annually; online and telephonic appointment scheduling; capture of demographic data; livescan fingerprint images and photo capture; card scanning services for transition to the network and out-of-state applicants; transaction processing and adjudication software; customized data interface protocols for major agencies; secure data center; and management of the network throughout the state. We provide the following services in association with our MA network: • Bi-lingual registration assistance by telephone to our Call Center • Secure online registration via secure website • Convenient Enrollment Centers equipped with Enrollment Workstations and Enrollment Agents (Livescan operators) • Secure centralized Data Center • Customized agency system integration • Electronic connection to the state AFIS • Reporting • Fee collection • Results dissemination (pending)
Participating Agencies	Department of Early Education and Care Department of Elementary and Secondary Education Department of Children and Families

Company	Massachusetts Executive Office of Public Safety
Description of Technical Solution	MorphoTrust Live Scan system MorphoTrust Store and Forward Server Proprietary registration, back end and billing software Secure connection to State MorphoTrak AFIS Cisco Virtual Private Network encryption of data transfer circuits Customized agency system integration and data sharing protocols MorphoTrust iA-thenticate document authentication system Card scan system
List of Fingerprinting Centers (with hours of operation)	Included in Appendix C
Letter of Recommendation	Included in Appendix D

4.3.3 The Vendor must also submit at least 3 (three) additional references that may be outside the scope of this project but will demonstrate the Vendor's ability to implement and complete projects comparable to the size and scope of this RFP.

MorphoTrust has provided an additional three successful applicant fingerprint networks for the states of New York and Michigan and the Transportation Security Administration. Contact information, size and scope of networks and other required information are noted below.

Table 6: New York Department of Criminal Justice Services

Company	New York Department of Criminal Justice Services
Company Address and Telephone Number	NYS Division of Criminal Justice Services 4 Tower Place Albany, NY 12203-3764 518-457-5837
Contact Person	Ann Sammons, Manager – Civil Identification Bureau NYS Division of Criminal Justice Services 4 Tower Place Albany, NY 12203-3764 518-457-3700 ann.sammons@dcjs.state.ny.us
Annual Fingerprint Volume	300,000
Description of Services MorphoTrust was chosen as the statewide vendor for live scan fingerprint submissions to NY DCJS. Program requirements include fingerprinting centers within 20 miles or 30 minutes of applicant's home or work; online and telephonic appointment scheduling; capture of demographic data; livescan fingerprint images and photo capture; card scanning services for transition to the network and out-of-state applicants; transaction processing and adjudication software; customized data interface protocols for major agencies; secure data center; and management of the network throughout the state. Because major agencies had independent processes in place for the processing of their large volumes of applicants, MorphoTrust was required to do an in-depth analysis of current procedures and work with	

Company	New York Department of Criminal Justice Services
each agency individually to ensure that the new network provided uninterrupted service to both the agencies and their applicants. Solutions included taking over current agency card scan processes that cleared hard fingerprint card backlogs and allowed agencies to establish a cut-off for hard card submission while new applicants were routed into the network of more than 90 Enrollment Centers throughout the state. For some agencies, MorphoTrust established data transfer protocols and software interfaces that allowed the agencies to take advantage of time and money-saving technological solutions to manual processes or to replace previous technology solutions as seamlessly as possible. We developed sophisticated interfaces for specific agencies which allow for the interchange of data in support of established agency processes with no disruption to users. MorphoTrust was able to stand up more than 90 Enrollment Centers in both urban and rural areas of the state in a very short period of time to ensure that the network met contractual requirements. While Centers in urban areas are relatively easy to identify, rural areas of upstate New York required intense effort. We provide the following services in association with this network: Multi-lingual appointment scheduling by telephone to Call Center or via secure website Convenient Enrollment Centers equipped with Enrollment Workstations and Enrollment Agents (Livescan operators) iA-thenticate – ID screening Card Scan for out-of-state applicants Customized agency system integration Centralized secure Data Center Electronic connection to the state AFIS Reporting Administrative Queue Review Fee Collection Customer account and billing services Onsite fingerprinting for groups of 30 or more	
Participating Agencies	Department of Criminal Justice Services Department of Motor Vehicles Department of State Office of Children and Family Services Lottery
Description of Technical Solution	MorphoTrust Live Scan system MorphoTrust Store and Forward Server Proprietary registration, back end and billing software Secure connection to State MorphoTrak AFIS Cisco Virtual Private Network encryption of data transfer circuits Customized agency system integration and data sharing protocols Photo capture system MorphoTrust iA-thenticate document authentication system Card scan system

Table 7: Michigan State Police

Company	Michigan State Police
Company Address and Telephone Number	Criminal Justice Information Center Michigan State Police 333 S. Grand Ave, P.O. Box 30634 Lansing, MI 48909-0634 517-241-0604
Contact Person	Gregory Rivet Manager, Criminal History Section Criminal Justice Information Center Michigan State Police 333 S. Grand Ave, P.O. Box 30634 Lansing, MI 48909-0634 (517) 241-0626 Rivetg1@michigan.gov
Annual Fingerprint Volume	150,000
Description of Services MorphoTrust provides a full-service network of civil applicant fingerprinting services for the State of Michigan. This statewide single source solution includes secure bilingual web registration and scheduling portal, Call Center, statewide Enrollment Centers equipped with Livescan equipment and Enrollment Agents, fee collection/remittance, central data center, and AFIS interface. In 2013, MorphoTrust was re-awarded the contract to operate the statewide applicant fingerprinting network. Within 9 weeks of contract award, MorphoTrust completed necessary updates and expansion efforts to perform for the new contract. There was no interruption of services to applicants.	
Participating Agencies	Long Term Care Licensed Healthcare Professionals Schools Adoption/Foster Care Concealed Carry
Description of Technical Solution	MorphoTrust Live Scan system MorphoTrust Store and Forward Server Proprietary registration, back end and billing software Secure connection to State MorphoTrak AFIS Cisco Virtual Private Network encryption of data transfer circuits Customized agency system integration and data sharing protocols MorphoTrust iA-thenticate document authentication system Card scan system

Table 8: Transportation Security Administration (TSA) Universal Enrollment Services

Company	Transportation Security Administration
Company Address and Telephone Number	601 S. 12th Street TSA-25, 10th Floor Arlington, Virginia 20598 866-289-9673
Contact Person	Gloria Uria, TSA Contracting Officer 601 S. 12th Street, TSA-25, 10th Floor Arlington, Virginia 20598 571-227-2429 Email: gloria.uria@tsa.dhs.gov
Annual Fingerprint Volume	MorphoTrust established and maintains a nationwide network of more than 330 Enrollment Centers that provide biometric, photo, and data capture and channeling for more than 1.5 million TSA background check and security threat assessments per year.
Description of Services	MorphoTrust provides a pre-registration website and Customer Service Call Center; capture of fingerprints, demographic data, photo and required documents; onsite fingerprinting sessions; channeling for company-owned equipment; customer reporting; card scan; and program management to ensure that individuals seeking access to critical segments of the nation's transportation system, infrastructure, or sensitive materials do not pose a threat to national security. MorphoTrust delivered this highly visible program ahead of schedule, without incident, and to the high praise of those involved. We transitioned or opened 152 new centers for the TWIC applicant group in 14 weeks, 140 locations for the HTAP applicant group in 24 weeks (ongoing), and added TSA Pre✓® to other Universal Enrollment Services sites. The TSA Pre✓® program has received several awards, including an ACT-IAC Igniting Innovation Dynamite Award for the Greatest Citizen Impact and the 2015 SAFRAN Innovation Award for Customer Satisfaction.
Participating Agencies	Universal Enrollment Services includes the following TSA programs: • Hazardous Materials Endorsement Threat Assessment Program (HTAP) • Transportation Worker Identification Credential (TWIC) • Alien Flight Student Program (AFSP) • TSA Pre✓® • E-Qip
Description of Technical Solution	Secure registration website Customer Service Call Center Nationwide network of Enrollment Centers with trained Enrollment Agents (Livescan operators) Capture of fingerprints, demographic data, photo, and required documents Onsite fingerprinting sessions Channeling for company-owned equipment Customer reporting Card scan Centralized Data Center

Section 4, Subsection 4.4: Project and Goals

4.4 Project and Goals: The project goals and objectives are:

4.4.1 Provide statewide electronic live-scan fingerprinting services for non-criminal justice purposes.

The Trusted Choice for West Virginia

MorphoTrust proposes to evolve our current West Virginia network to meet the new requirements of this RFP, using the current infrastructure in place today to ensure continuous service to the residents of West Virginia.

MorphoTrust operates with the following infrastructure for West Virginia:

- Direct knowledge of the West Virginia program from providing applicant fingerprinting since 2011.
- Executive management team and many key personnel with more than a decade of personal experience in fingerprinting services.
- Project management team with experience implementing and operating fingerprinting networks throughout the United States.
- 24x7x365 multi-lingual Pre-Enrollment Website that currently registers more than two million applicants per year, including 55,000 West Virginia applicants.
- 12,000 square foot U.S.-based multi-lingual Customer Service Center that currently accepts more than two million calls per year, including more than 50,000 calls from the West Virginia program.
- Twenty-two (22) Enrollment Centers located throughout West Virginia with field-proven livescan hardware and software and experienced Enrollment Agents (Livescan operators).
- Centralized Cardscan conversion center processing more than 125,000 paper cards per year, including 20,000 from West Virginia applicants.
- Secure Data Center currently submitting approximately five million fingerprint records per year to more than 20 state AFIS systems, including our interface with the MorphoTrak AFIS systems in West Virginia.
- Certified FBI Channeler and provider of 350,000 criminal history results, including delivery of more than 60,000 paper-based results.
- Fee processing center that accepts money orders, checks, and credit cards. The center also manages more than 5,000 customer billing accounts.
- Technical Help Desk currently supporting more than 1,200 Enrollment Centers in all 50 U.S. states.

Plan for Providing Electronic Livescan Fingerprinting Services

Figure 2 summarizes our current and proposed fingerprinting process in West Virginia, from the applicant's initial request through reporting.

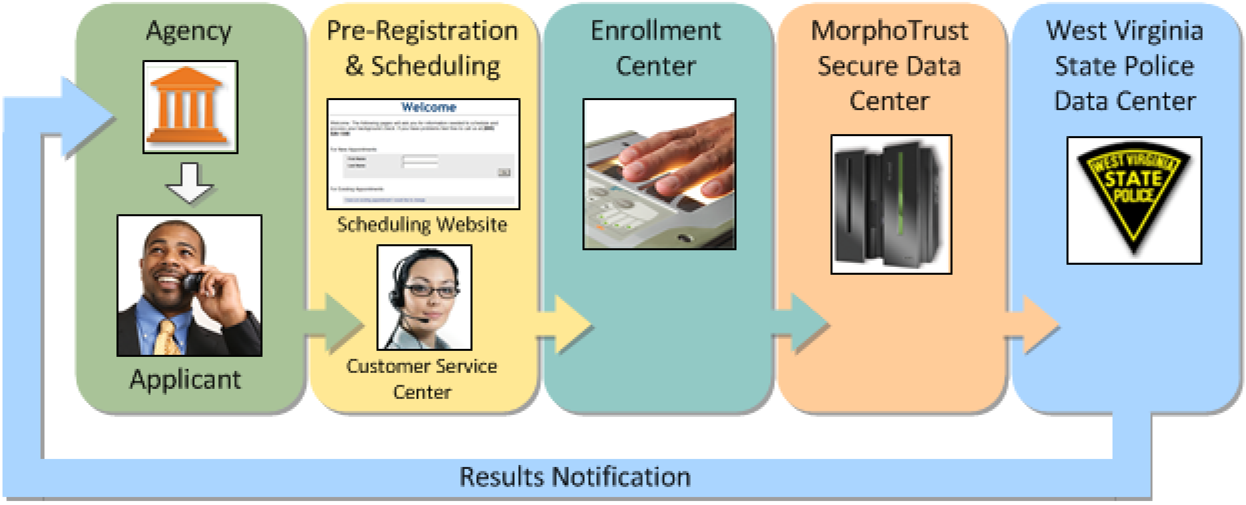

Agency
Pre-Registration & Scheduling
Welcome
Scheduling Website
Customer Service Center
Enrollment Center
MorphoTrust Secure Data Center
West Virginia State Police Data Center
WEST VIRGINIA STATE POLICE
Applicant
Results Notification

Figure 2: Proposed Process for West Virginia Applicant Fingerprinting Services

The steps shown in Figure 2 are as follows:

1. West Virginia agency provides applicant with MorphoTrust's contact information.
2. Applicant pre-enrolls using MorphoTrust's Pre-Enrollment Website or toll-free telephone. During the pre-enrollment process, demographic data is collected or entered, the applicant can pay the required fees, and an appointment is scheduled. The applicant receives a unique identifier and directions to the selected Enrollment Center.
3. Applicant visits an Enrollment Center where their ID and demographic data are verified, fee collected, and they are fingerprinted. The full fingerprint record is transmitted to our Secure Data Center via secure connection. Applicant is given a receipt.
4. MorphoTrust's systems transmit the records over secure connection to the West Virginia State Police Data Center and record the return acceptance.
5. In the West Virginia Data Center, the AFIS collates State and FBI checks and returns results back to a secure Results Server.
6. MorphoTrust disseminates results to the authorized entity or provides access to the Results Server based on agency setup.

Upgrade to Latest Technology Platform

During the first year of the contract, we propose to upgrade the West Virginia Applicant Fingerprinting Services program's technology to our next generation Universal Enrollment Platform (UEP). UEP has been in use since 2013 for our fingerprinting services contract with the U.S. Department of Homeland Security, Transportation Security Administration (TSA), which includes the popular TSA Pre✓® program. Our TSA program serves more than 1.5 million customers annually in more than 330 Enrollment Centers throughout the United States and currently maintains a customer satisfaction rate of over 99.8% based on applicant surveys. UEP is also operational for our state fingerprinting services program in Texas.

Capabilities of UEP include:

- ***New Livescan enrollment workstations*** – Deployed to all Enrollment Centers, which will reduce equipment downtime.
- ***Highest quality fingerprint capture*** – More than 20 fingerprint quality checks are performed at the workstation to ensure high-quality fingerprints are captured. These checks reduce rejection rates, which in turn, reduce the chance that applicants will have to be re-printed.
- ***User-friendly registration process*** – Simplified, mobile and tablet friendly registration website increases volume of applicant self-registration.
- ***Nationwide network*** – Our Universal Enrollment solution allows applicants from other states to submit their fingerprints from enrollment locations other than those located in West Virginia. Local operating procedures and technology will be used.
- ***Improved identity document authentication*** – Workstations will be equipped with our proprietary document authentication software and B5000 reader to analyze State or Federal government-issued photo identification documents for authenticity.
- ***Administrative Support and Reporting Portal*** – Stay connected with the entire process using our optional support and reporting portal. With this web-based portal for state agencies, end users will never lose track of an enrollment, an applicant’s appointment status, or submission results. The suite of portal features includes:
    - Ticketing for managing applicant support inquiries across multiple teams.
    - Detailed transaction history and status for a real-time view of the process.
    - Images of biometrics captured (photos, fingerprints, identity documents) for research and forensics purposes.

With these features and more, the portal provides an indispensable tool for transparency that keeps state agencies, the State Police, and MorphoTrust personnel constantly connected and up to date.

- ***Improved applicant status visibility*** – As an optional feature, applicants can also check on the status of their submission via our secure public website.

Summary of Our Approach

MorphoTrust's approach to this project is to continue serving West Virginia with the current Enrollment Center network in use today, while expanding the network and upgrading the technology over time to our Universal Enrollment Platform.

How does MorphoTrust stand out from our competitors?		
Delivery of both fingerprint capture and background check results The Universal Enrollment Platform, which fully manages the applicant experience, is complemented by our EasyPath results-delivery solution that facilitates adjudication and manages results delivery.	**Technology platform that meets the highest security standards** The security controls that govern the Universal Enrollment Platform map directly to NIST Special Publication 800-53 v4 "Security and Privacy Controls for Federal Information Systems and Organizations." In addition, our UEP solution meets Federal Information Security Management Act of 2002 (FISMA) standards.	**Governance by a National Security Agreement** Every MorphoTrust employee is a U.S. Citizen who undergoes a rigorous background check prior to employment.

4.4.2. Provide a Customer Service Center to serve as a single point of contact.

4.4.2.1 The Vendor should describe in detail their plan to provide a customer service center and include the hours of operation, where the center will be located at and the number of staff assigned. The plan should also detail the type of service the center will provide to the Applicant upon calling.

MorphoTrust operates a centralized, scalable Customer Service Center (CSC), which currently accepts over two million calls per year for numerous statewide networks—including the State of West Virginia.

We operate the CSC in two U.S. cities (Springfield, IL and Des Moines, IA) to minimize outages due to disaster, weather, or telecommunications issues. West Virginia applicants and agencies are able to access the CSC conveniently from anywhere in the United States via a single, toll-free, program-specific telephone number.

The CSC offers an uninterrupted, proven single point of contact to speak with Customer Service Representative (CSR) to register, schedule an appointment, process payment, and ask questions about the process. Our knowledgeable, experienced, and multi-lingual staff is available Monday through Friday, 7:00 A.M. - 4:00 P.M. Central Standard Time (9:00 A.M. to 5:00 P.M. West Virginia local time). If an Applicant calls outside of the business hours, a recorded message directs them to our secure Pre-Enrollment Website where they can register 24x7x365.

The CSC currently employs more than 150 CSRs, including a team of CSRs who are dedicated to the needs of West Virginia Applicants. In addition to the CSRs who are dedicated to this project, all CSRs are cross-trained so that they can be utilized during peak periods, if needed.

Figure 3: MorphoTrust Customer Service Call Center

Our knowledgeable and experienced Customer Service Representatives will assist West Virginia applicants by answering questions, scheduling appointments, processing payments, and providing directions to Enrollment Centers.

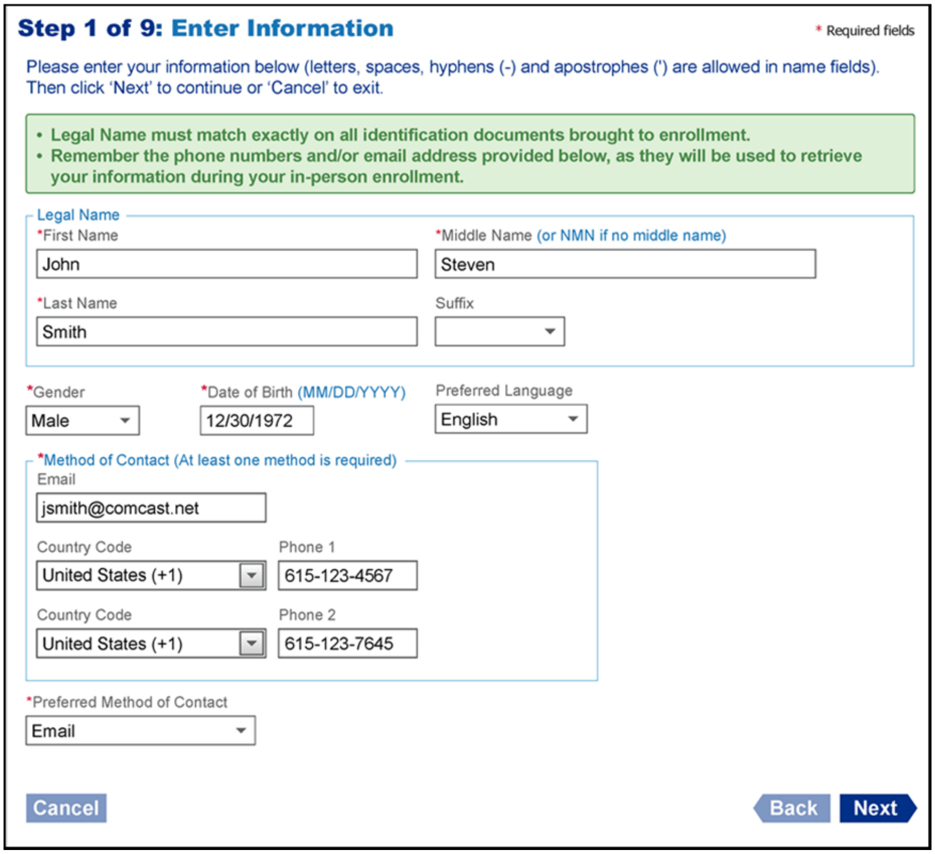
We have provided additional detail about our Customer Service Center in our response to requirement 4.5.1 (a).

4.4.2.2 The Vendor should describe in detail their plan to provide web scheduling to the Applicant and Agencies. Included in the plan should be the ability to demographic information, pay fees, retrieve directions to the fingerprinting centers, the availability of the services and when will maintenance be performed.

MorphoTrust's proven web-based registration system is a key component in delivering excellent customer service to both applicants and the agencies that employ or license them. Applicants can access the web site 24x7x365 to obtain information, enter their demographic information, pay fees, locate an Enrollment Center, schedule an appointment, and retrieve directions to the fingerprinting center.

At the beginning of the new contract period for the Applicant Fingerprinting Services program, applicants will continue to utilize the registration system that has been in place in 2011 and which complies with all the requirements of this RFP.

During the first year of the contract, we will transition to our new UEP Pre-Enrollment Website. Our UEP software has smart logic that allows applicants to pre-enroll, beginning with entering the required demographic information (Figure 4). In a step-by-step process, the applicant searches the list of Enrollment Centers and hours of operation to find a convenient fingerprinting location, selects an open appointment, collects fees if applicants wished to pay at this time, and confirms proper documentation needed. The process is streamlined and specifically designed so that even applicants with limited web skills can schedule their appointments.



Step 1 of 9: Enter Information

* Required fields

Please enter your information below (letters, spaces, hyphens (-) and apostrophes (') are allowed in name fields). Then click 'Next' to continue or 'Cancel' to exit.

- Legal Name must match exactly on all identification documents brought to enrollment.
- Remember the phone numbers and/or email address provided below, as they will be used to retrieve your information during your in-person enrollment.

Legal Name

*First Name: John

*Middle Name (or NMN if no middle name): Steven

*Last Name: Smith

Suffix:

*Gender: Male

*Date of Birth (MM/DD/YYYY): 12/30/1972

Preferred Language: English

*Method of Contact (At least one method is required)

Email: jsmith@comcast.net

Country Code: United States (+1)

Phone 1: 615-123-4567

Country Code: United States (+1)

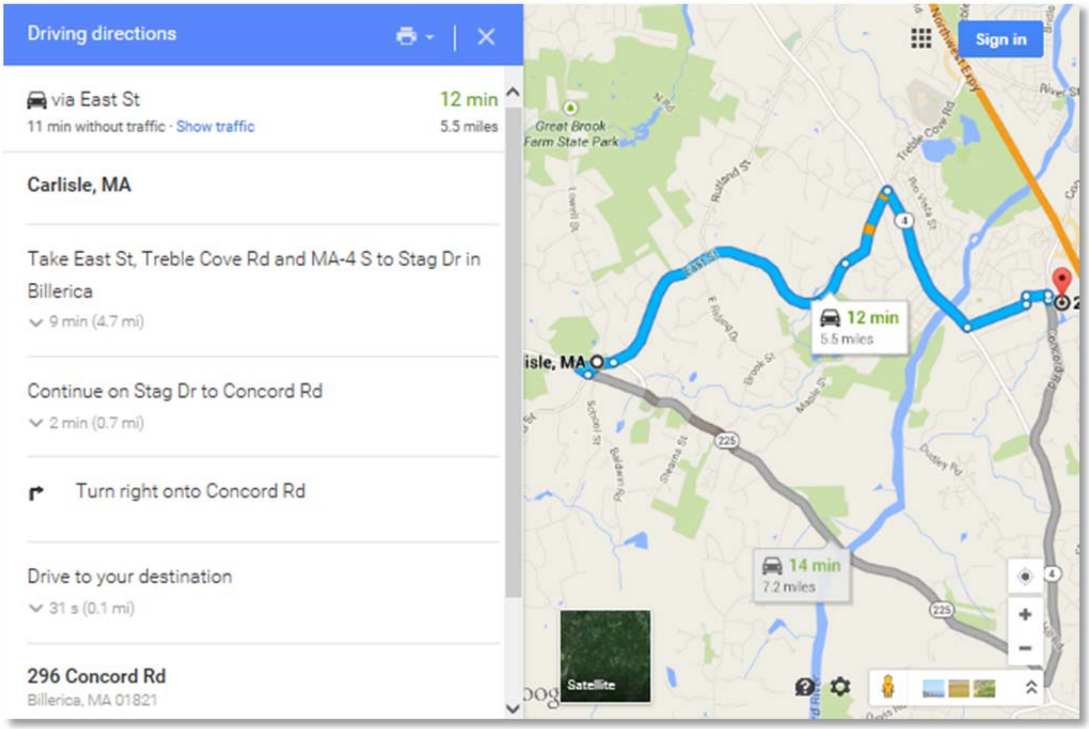
Phone 2: 615-123-7645

*Preferred Method of Contact: Email

Figure 4: Web-Based Scheduling System

Using the 24x7x365 Pre-Enrollment Website, Applicants can enter their demographic information, search for a conveniently located Enrollment Center, schedule a fingerprint appointment, and obtain directions. With our UEP solution (shown), the website is also mobile and tablet friendly.

After the applicant has scheduled an appointment, a confirmation page lists the appointment details and provides reminders to help the applicant prepare for a successful visit to an Enrollment Center. The page displays the address of the Enrollment Center, along with a link that the applicant can click to view a map and directions (Figure 5).



Driving directions

via East St 12 min
11 min without traffic · Show traffic 5.5 miles

Carlisle, MA

Take East St, Treble Cove Rd and MA-4 S to Stag Dr in Billerica
9 min (4.7 mi)

Continue on Stag Dr to Concord Rd
2 min (0.7 mi)

Turn right onto Concord Rd

Drive to your destination
31 s (0.1 mi)

296 Concord Rd
Billerica, MA 01821

Figure 5: Linking to a Map and Directions to an Enrollment Center from the Pre-Enrollment Website

The secure Pre-Enrollment Website is available 24 hours a day, 7 days a week, and 365 days a year with the exception of emergency outages or scheduled maintenance. The UEP website is also mobile and tablet friendly.

A new capability that is offered as part of the UEP upgrade includes the ability for MorphoTrust Administrators to display messages on the website for critical information that impacts usage as well as provide advanced notice if the system will be unavailable for maintenance.

The MorphoTrust software delivery process minimizes downtime to the public, with an average uptime rate of 99.3% in 2014. When an outage does need to occur, the typical outage window is scheduled after 8:00 P.M. CT and requires 15 minutes or less. During a planned outage, a message is presented to the user that the system is down for maintenance with an estimated time to availability.

We have provided additional detail about our Pre-Enrollment Website in our response to requirement 4.5.1 (b).

4.4.2.3 The Vendor should describe in detail how they plan on ensuring Applicant Appointments will be scheduled in a timely manner.

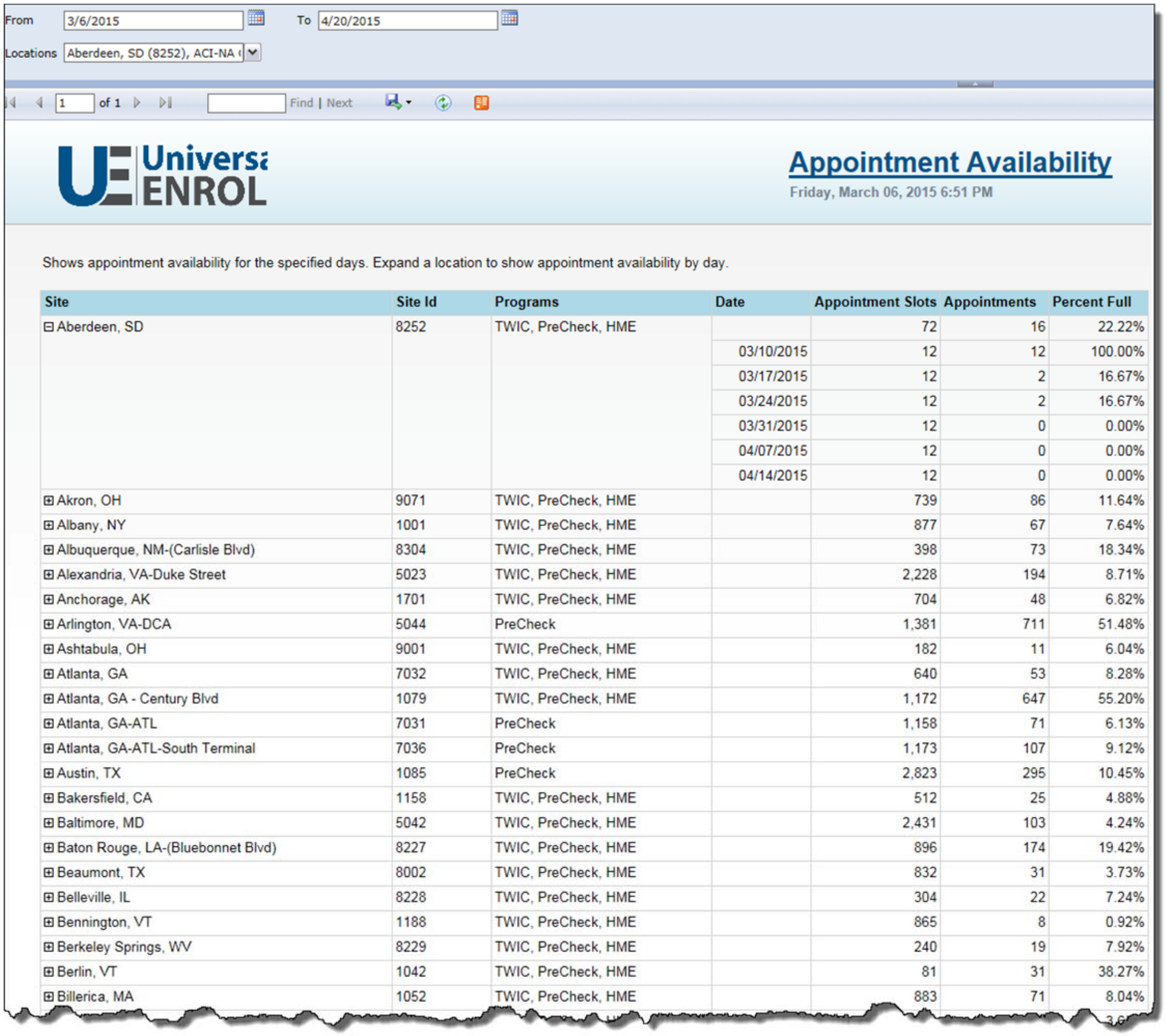
MorphoTrust pays special attention to selecting Enrollment Center locations that are in the right area for ease of access to major traffic arteries, access to public transportation (where available), and in facilities with signage opportunities so applicants can easily locate the Enrollment Center. We will provide statewide coverage of Enrollment Center locations and appointment capacity so that all applicants will be able to schedule their appointment in a timely manner.

We propose to add five (5) new Enrollment Centers to our existing network of fingerprinting locations in West Virginia for a total of 27 Enrollment Centers throughout the state.

We have provided a complete list of proposed locations and hours of operation in Table 10 and a map of the statewide distribution in Figure 7. In addition, we offer on-site mobile fingerprinting services for groups of 25 or more, as we described in our response to requirement 4.4.3.2.

Our program management and regional operations teams will evaluate Enrollment Center capacity and utilization on a recurring schedule to assess and remediate recurring issues related to appointment availability. Figure 6 shows an example of an Appointment Availability Report, which provides real time information about Enrollment Center appointment availability and utilization. MorphoTrust uses this report to proactively address availability before issues arise.

If demand dictates, we will provide multiple Enrollment Centers or Enrollment Centers with multiple workstations in high population areas to ensure timely access to services.



From 3/6/2015 To 4/20/2015

Locations Aberdeen, SD (8252), ACI-NA (

1 of 1

Appointment Availability

Friday, March 06, 2015 6:51 PM

Shows appointment availability for the specified days. Expand a location to show appointment availability by day.

Site	Site Id	Programs	Date	Appointment Slots	Appointments	Percent Full
⊟ Aberdeen, SD	8252	TWIC, PreCheck, HME		72	16	22.22%
			03/10/2015	12	12	100.00%
			03/17/2015	12	2	16.67%
			03/24/2015	12	2	16.67%
			03/31/2015	12	0	0.00%
			04/07/2015	12	0	0.00%
			04/14/2015	12	0	0.00%
⊞ Akron, OH	9071	TWIC, PreCheck, HME		739	86	11.64%
⊞ Albany, NY	1001	TWIC, PreCheck, HME		877	67	7.64%
⊞ Albuquerque, NM-(Carlisle Blvd)	8304	TWIC, PreCheck, HME		398	73	18.34%
⊞ Alexandria, VA-Duke Street	5023	TWIC, PreCheck, HME		2,228	194	8.71%
⊞ Anchorage, AK	1701	TWIC, PreCheck, HME		704	48	6.82%
⊞ Arlington, VA-DCA	5044	PreCheck		1,381	711	51.48%
⊞ Ashtabula, OH	9001	TWIC, PreCheck, HME		182	11	6.04%
⊞ Atlanta, GA	7032	TWIC, PreCheck, HME		640	53	8.28%
⊞ Atlanta, GA - Century Blvd	1079	TWIC, PreCheck, HME		1,172	647	55.20%
⊞ Atlanta, GA-ATL	7031	PreCheck		1,158	71	6.13%
⊞ Atlanta, GA-ATL-South Terminal	7036	PreCheck		1,173	107	9.12%
⊞ Austin, TX	1085	PreCheck		2,823	295	10.45%
⊞ Bakersfield, CA	1158	TWIC, PreCheck, HME		512	25	4.88%
⊞ Baltimore, MD	5042	TWIC, PreCheck, HME		2,431	103	4.24%
⊞ Baton Rouge, LA-(Bluebonnet Blvd)	8227	TWIC, PreCheck, HME		896	174	19.42%
⊞ Beaumont, TX	8002	TWIC, PreCheck, HME		832	31	3.73%
⊞ Belleville, IL	8228	TWIC, PreCheck, HME		304	22	7.24%
⊞ Bennington, VT	1188	TWIC, PreCheck, HME		865	8	0.92%
⊞ Berkeley Springs, WV	8229	TWIC, PreCheck, HME		240	19	7.92%
⊞ Berlin, VT	1042	TWIC, PreCheck, HME		81	31	38.27%
⊞ Billerica, MA	1052	TWIC, PreCheck, HME		883	71	8.04%

Figure 6: Appointment Availability Report

Once UEP is deployed, MorphoTrust will utilize this report to assess Enrollment Center utilization and proactively remediate issues related to appointment availability.

As an option, we offer Expedited Fingerprinting Service with premium same-day fingerprinting slots. We have described this service in Appendix F.

Finally, MorphoTrust will maintain open lines of communication with WVSP and User Agencies in order to respond to actual or anticipated volume increases.

We have experience in expanding many of our existing statewide networks, for example, in response to new legislation or to support new agencies joining the network. During the current contract in West Virginia, we increased the number of Enrollment Centers from 12 to 22 in order to provide a higher level of customer service to the citizens of the state.

4.4.2.4 The Vendor should describe in detail the security measures for protecting Personal and financial information.

MorphoTrust's current solution in West Virginia complies with all State and FBI security measures.

The scope of our information security program includes information systems and technologies, personnel security, physical and environmental security for facilities that house our information systems, and business process security. We employ a team of information system security engineers who are knowledgeable and experienced in delivering State, FBI, and FISMA-compliant security programs.

TSA-Proven Information Assurance

MorphoTrust's track record of seven successful Certifications and Accreditations over four TSA contracts demonstrates our ability to meet rigorous Department of Homeland Security and TSA information security requirements.

Our resources and credentials include:

- Certified Information Systems Security Professionals (CISSP)
- Certified Ethical Hacker (CEH)
- Certified Information Systems Auditor (CISA)
- Certified Information Privacy Technologist (CIPT)
- Co-Authorship of NIST Computer Security Special Publication
- Social Engineering/Phishing Security Awareness Training

Our internal information security program is predicated upon the guidance set forth in NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems. Our information security program meets Federal Information Security Management Act (FISMA) requirements in order to serve our federal customers. We implement and monitor all applicable management, operational, and technical controls defined by NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and we ensure compliance with agency security policies and requirements.

Security Awareness Training is a key component of NIST/FISMA information security controls, and MorphoTrust conducts information security awareness training for all employees who serve our biometric enrollment customers. We work to mitigate the threat of social engineering by requiring social engineering training for each employee when they join the company, and annually thereafter. Additionally, we conduct unannounced social engineering awareness exercises throughout each calendar year for all biometric services employees. We also have strict annual security awareness training requirements imposed upon us by the U.S. Federal Government as a result of our federal contracts.

The security and integrity of our network solutions, including all components, data transmissions, and physical facilities are of the utmost importance to

MorphoTrust. We understand the critical importance of protecting all personal and financial information of our customers. As such, we provide industry standard security measures throughout our network solution to protect this sensitive information and infrastructure.

For example, all PII is encrypted while in transit and while at rest. Further, we ensure that only those persons needing access to the information have it, and when they do, that each access is controlled and logged appropriately.

We have provided additional description of our approach to protecting personal and financial information in our response to requirement 4.5.5. In addition, we have provided our IT Security Policy and Personal Data Privacy Policy in Appendix A.

4.4.2.5 The Vendor should describe in detail how the state can verify the existing Web scheduling and test its performance.

MorphoTrust hosts an existing Pre-Enrollment Website for West Virginia fingerprinting services. The website is currently active for verification and testing at the following URL: https://wv.l1enrollment.com/OpenNetworkPortal/spring/customer?execution=e1s1

Our UEP web pre-enrollment and scheduling solution can be tested at the following URL:

https://universalenroll.dhs.gov

The State can test both sites by completing a pre-registration and scheduling an appointment. Once the appointment is complete, we can provide the resulting pre-registration data and appointment information as proof of the accuracy and successful scheduling. The State may access the sites and schedule as many test scenarios as desired. The current systems are live today, and will continue to be upon contract award.

4.4.2.6 The Vendor will describe in detail their plan to collect fees from the Applicant and Agencies. Included in the plan should be forms of payment online, at fingerprint centers and prepaid accounts set up with governmental agencies.

MorphoTrust recommends that applicants continue to tender the entire enrollment fee directly to MorphoTrust, as we do today in West Virginia. MorphoTrust will remit the associated fees to the State and/or FBI via invoice process or via direct ACH delivery. The frequency and method of remittance can be customized to meet the State’s specific needs.

Our current solution and the UEP solution both allow applicants multiple options for payment tender, including all major credit cards (Visa, MasterCard, American Express, and Discover) as well as payment by check or through a billing account.

Applicants can pay by credit card online or via Call Center at the time of scheduling, as currently provided in the West Virginia program, or in person at the Enrollment Centers. As a best practice, MorphoTrust recommends that credit cards are presented and processed at the time of enrollment to ensure correct application of payment and reduce the number of refund events.

Proven Fee Processing for West Virginia Applicants and Agencies

In 2014, MorphoTrust processed more than 740,000 applicant checks and money orders and more than $135,000,000 in applicant credit card transactions.

Our internal Billing Department ensures superior customer service to thousands of agency and employer billing accounts.

Applicants may pay at the Enrollment Centers by check, which will be remotely deposited the same day. Our solution ensures the instrument clears prior to allowing transmission of the enrollment, limiting the potential for applicants to process with non-sufficient funds or non-conforming instruments.

Both agencies and employers can establish third-party billing accounts and use them to pay for applicants. MorphoTrust will invoice government agencies for activity with Net 30 terms. In certain instances, employers can also receive invoice terms pending approved credit application. Where billing accounts are desired but invoicing terms cannot be provided, employers can pay for applicant transactions with a valid credit card.

In addition, we provide an easy, innovative way for employers and agencies to pay fees on behalf of applicants. Agencies and employers will have the option of distributing single-use “Authorization Codes” to their applicants, which reduces the potential of fraudulent activity. When provided by the applicant online or at the Enrollment Center as a form of payment, these Authorization Codes generate charges for the issuing agency or employer. Because each code is unique, the agency or employer has confidence they are paying only for their applicants. Payment Authorization Codes issued to applicants by agencies or employers can be backed by a traditional or prepaid credit card or be configured to allow MorphoTrust to generate an invoice statement. MorphoTrust reserves the right to deny requests from agencies and employers to have an invoice account based on annually-renewed MorphoTrust policy for extending credit.

Table 9 summarizes the types of transactions currently provided by MorphoTrust in West Virginia and proposed under the new UEP platform.

Table 9: Forms of Payment

Transaction Type	Current WV Platform	UEP Platform
Online Payment by Applicant	e-check Credit Card (V/M/D/A)	e-check : Not Recommended Credit Card (V/M/D/A)
Payment at Enrollment Center by Applicant	Personal check Corporate Check Money Order	Personal check: Not Recommended Corporate Check Money Order Credit Card (V/M/D/A)
Private Agencies and Employers	Prepaid and/or Credit Billing Accounts	Credit Billing Accounts (Credit Pending) Credit Card Backed Accounts
Governmental Agencies	Credit Billing Accounts	Credit Billing Accounts

4.4.3 Provide electronic fingerprint Capture Service Locations (sites).

4.4.3.1 The Vendor should describe in detail their plan to provide electronic fingerprint capture services for West Virginia. Included in the plan, the vendor should discuss site locations, ADA compliance measures, staffing related to site centers, receipt process for Applicants at site locations and the communication process to site location.

Enrollment Center Locations

MorphoTrust proposes to provide 27 public fingerprinting locations across West Virginia. These locations have been selected to assure that no applicant will have to travel more than 35 miles to utilize a MorphoTrust Enrollment Center. All sites will be compliant with the federal Americans with Disabilities Act requirements.

The map in Figure 7 shows the geographical distribution of our proposed Enrollment Center locations including the 22 operational locations we have in West Virginia today, plus 5 new locations that would be deployed following contract award.

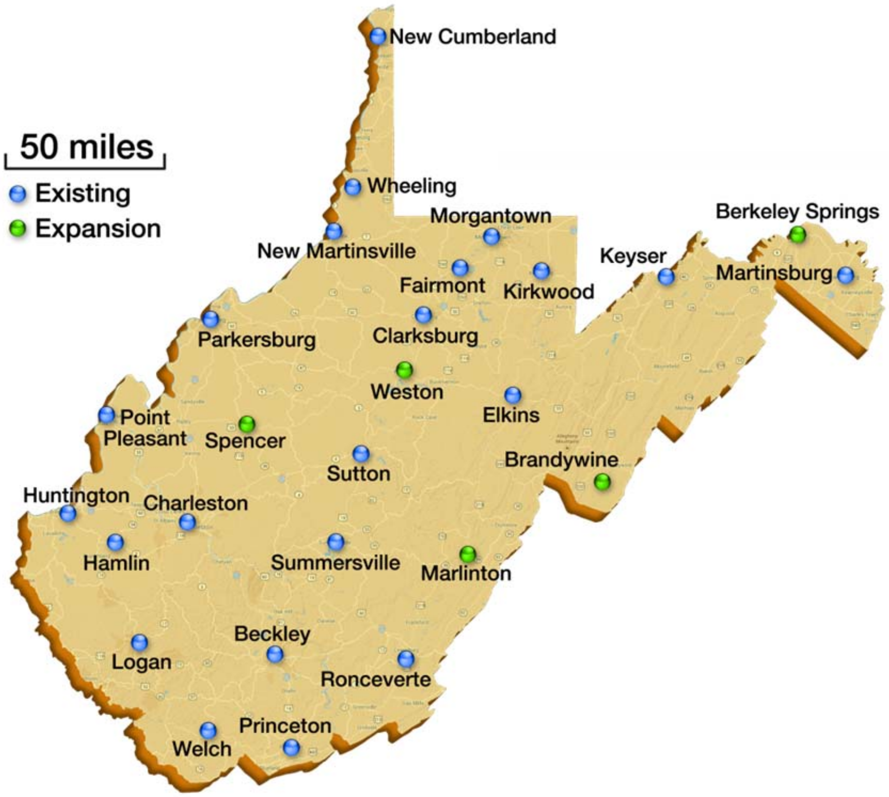


Figure 7: Distribution of Proposed Enrollment Centers in West Virginia

Table 10 lists the proposed Enrollment Centers in West Virginia.

Table 10: Proposed Enrollment Centers in West Virginia

West Virginia City/Town	Location/Address	Hours of Operation
Beckley	On-Site In-Home Drug Testing 351 Prosperity Road Beckley, WV 25801	Monday - Friday 9:30 am - 4:30 pm
Berkeley Springs	TBD Berkeley Springs, WV 25411	TBD
Brandywine	TBD Brandywine, WV 26802	TBD
Clarksburg	TBD Clarksburg, WV 26330	TBD
Elkins	Ultra Care Home Health Agency LLC 598 Harrison Ave Elkins, WV 26241	Tuesday - Thursday 10:00 am - 12:00 pm 1:00 pm - 5:00 pm
Fairmont	Marion County Senior Citizens 105 Maplewood Drive Fairmont, WV 26554	Every other Monday 10:00 am - 1:00 pm 2:00 pm - 4:00 pm

West Virginia City/Town	Location/Address	Hours of Operation
Hamlin	Lincoln County Opportunity Company 360 Main Street Hamlin, WV 25523	Every other Monday 8:00 am - 12:00 pm 12:30 pm - 3:00 pm
Huntington	Denning Industrial Park 4510 Terrace Ave Huntington, WV 25705	Monday - Wednesday 9:00 am - 12:00 pm 1:00 pm - 5:00 pm
Keyser	MorphoTrust USA 196 North Tornado Way Potomac Plaza Suite 11 Keyser, WV 26726	Thursday and Friday 9:00 am - 1:00 pm 2:00 pm - 5:00 pm
Kingwood	Preston County Senior Citizens, Inc. 108 Senior Center Drive Kingwood, WV 26537	Every other Wednesday 9:00 am - 12:00 pm 12:30 pm - 4:00 pm
Logan	Quality Drug Testing 4130 Hanging Rock Highway Stollings, WV 25646	Monday - Friday 9:00 am - 4:00 pm
Marlinton	TBD Marlinton, WV 24954	TBD
Martinsburg	Martinsburg Shopping Plaza 615 Winchester Ave Martinsburg, WV 25401	Monday, Tuesday, Thursday, and Friday 9:00 am - 5:00 pm Wednesday 9:00 am - 1:00 pm 2:00 pm - 5:00 pm
Morgantown	Pace Enterprise of WV Inc. 889 Mylan Park Lane Morgantown, WV 26501	Monday - Thursday 8:30 am - 12:45 pm 2:00 pm - 4:00 pm
New Cumberland	Hancock County Senior Services 647 Gas Valley Road New Cumberland, WV 26047	Monday, Wednesday and Thursday 9:00 am - 3:00 pm
New Martinsville	Wetzel County Committee on Aging 145 Paducah Drive New Martinsville, WV 26155	Every other Monday 9:00 am - 12:00 pm 1:00 pm - 4:00 pm
Parkersburg	SW Resources Inc. 1024 7th Street Parkersburg, WV 26101	Monday - Friday 8:30 am - 12:00 pm 1:00 pm - 3:30 pm
Point Pleasant	Pleasant Valley Nursing And Rehab Center 640 Sandhill Road Point Pleasant, WV 25550	Every other Friday 9:00 am - 12:00 pm 1:00 pm - 4:00 pm
Princeton	Community Connections Inc 215 South Walker Street Princeton, WV 24740	Monday, Wednesday, Friday 10:00 am - 3:00 pm

West Virginia City/Town	Location/Address	Hours of Operation
Ronceverte	Mountain Heart Community Services Inc. Workforce WV 25 Red Oak Shopping Center Ronceverte, WV 24970	Tuesday-Thursday 12:00 pm – 4:00 pm
South Charleston	MorphoTrust USA 38 River Walk Mall South Charleston, WV 25303	Monday - Friday 8:00 am - 6:00 pm
Spencer	TBD Spencer, WV 25276	TBD
Summersville	Seneca Health Services, Inc. 804 Broad Street Summersville, WV 26651	Wednesday 9:00 am - 11:30 am 12:30 pm - 4:00 pm
Sutton	Central WV Aging Services Inc. 101 2nd Street Sutton, WV 26601	Every other Friday 10:00 am - 2:00 pm
Welch	McDowell County Commission on Aging 725 Stewart Street Welch, WV 24801	Every other Thursday 10:00 am - 12:00 pm 12:30 pm - 4:00 pm
Weston	TBD Weston, WV 26452	TBD
Wheeling	Change, Inc. 700 First Street Moundsville, WV 26041	Monday, Thursday, and Friday 8:30 am - 11:00 am Tuesday and Wednesday 8:30 am - 3:00 pm

ADA Compliance

All Enrollment Center locations are required to pass a rigorous Readiness Assessment, which requires the Site Assessor to evaluate over 50 qualities of the facility, including compliance with ADA laws. All sites are reviewed against the following ADA requirements:

ADA accessible entrances:

- Doors have a minimum 32 inch width clearance
- External entrance is accessible directly from ground level, or easily accessible via accessibility ramp if located above ground level
- Internal entrance (if applicable) is accessible directly from ground level, or easily accessible via elevator if located above or below ground level
- Elevators if building is multiple levels
- Hallways have a minimum 36 inch width clearance

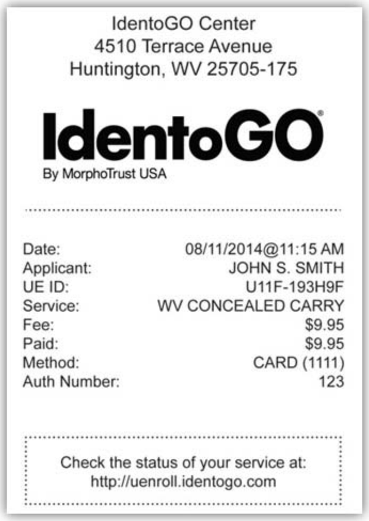
ADA-marked parking spaces for disabled individuals are available at a 1:8 ratio (i.e.: one handicapped parking space to every eight parking spaces)

Enrollment Center Staffing

All of our Enrollment Centers are staffed by certified Enrollment Agents who are fully trained to perform the duties as outlined in the RFP. We propose to support the West Virginia program with 30-40 Enrollment Agents, more than 30 of whom are already on staff and are fully vetted and trained.

Unique to MorphoTrust are the security best practices and policies to which we must adhere. MorphoTrust is one of a rare few companies governed by U.S. Proxy and National Security Agreements and is mandated to follow the highest standards of security to protect all personally identifiable information. We may employ and subcontract with only U.S. citizens who are thoroughly vetted and have successfully passed a background check, drug test, financial review, and security threat assessment.

Certified Enrollment Agents managing the fingerprinting process in our Enrollment Centers must now undergo special screening and training to ensure maximum security, efficiency, and professionalism as we serve the American public. MorphoTrust conducts these vetting processes in addition to State vetting requirements, not in lieu of, ensuring that all Enrollment Center personnel meet and exceed the high standards for safety and security mandated for program employment.



IdentoGO Center
4510 Terrace Avenue
Huntington, WV 25705-175

IdentoGO®
By MorphoTrust USA

Date:	08/11/2014@11:15 AM
Applicant:	JOHN S. SMITH
UE ID:	U11F-193H9F
Service:	WV CONCEALED CARRY
Fee:	$9.95
Paid:	$9.95
Method:	CARD (1111)
Auth Number:	123

Check the status of your service at:
http://uenroll.identogo.com

Figure 8: Transaction Receipt

Receipt Process

MorphoTrust will provide a printed receipt to each applicant at the conclusion of their enrollment, which will contain, at a minimum, the system-unique identifier and the date of service. Figure 8 shows a sample of the enrollment receipt currently in use in the West Virginia program.

Communication Process

During enrollment, every applicant is required to provide either a telephone number or an email address. Applicants who provide both will also select their preferred method of contact.

This method of contact is used to automatically deliver important notifications, such as a need to resubmit fingerprints. Applicants are also notified automatically of an Enrollment Center closure due to inclement weather, if it impacts a scheduled appointment.

When an applicant prefers to be contacted by email, our systems notify them via an automated email. When an applicant prefers to be contacted by phone, our Interactive Voice Response (IVR) system will automatically call the applicant and deliver the notification via a TTS message. In all cases, the applicant is given instructions on how to contact our Customer Service Center should they have follow-up questions or concerns.

4.4.3.2 The Vendor should describe in detail their plan to provide mobile on site fingerprinting services for groups of 25 or more.

Mobile Convenience

On-site services provide added convenience and coverage for specific opportunities like orientation workshops, hiring sessions for new teachers, and other group gatherings.

MorphoTrust has provided more than 150 mobile sessions in West Virginia since 2011.

MorphoTrust currently provides on-site mobile fingerprinting in West Virginia. We will continue to provide this service anywhere in the state for groups of 25 or more. Based on our experience with the demand for onsite services in West Virginia and other states, we are initially planning to have three mobile fingerprinting units throughout the state to support this effort, although additional resources can be added if the demand for mobile services supports an expansion. MorphoTrust typically requests that such sessions be scheduled at least two weeks in advance.

We respond to all requests in a timely manner and work with the requestor to identify the most convenient, available option for the on-site session. Full instructions and guidance are provided to the customers during the schedule setup, including technical and space requirements for the site, sample advanced communication and notifications to applicants, and expectations during the on-site visit.

Our mobile Enrollment Agent brings all equipment required to process applicants. This equipment includes the Livescan device, a laptop, and supplies. Agencies are required to provide a suitable workspace that includes at a minimum a standard desktop space to set up the equipment while affording the applicant some degree of privacy, with at least three electrical outlets. Suitable waiting space is also required.

We have provided additional detail about our mobile solution in our response to requirement 4.5.3 (b).

4.4.3.3 The Vendor should describe in detail their plan for dealing with Applicant appointments. Included in the plan, the Vendor should detail the Applicant identification process, collection of payment, the veracity of Applicant demographic data, release of record authorization process as outlined in 28CFR

50. I 2(b) and the collection of digital prints and signatures.

Figure 9 provides a high-level overview of the enrollment process, including appointment scheduling, collection of payment, verification of demographic data, release of record authorization, and the collection of digital prints and signatures. MorphoTrust will continue to provide these services that currently are part of the West Virginia fingerprinting network.

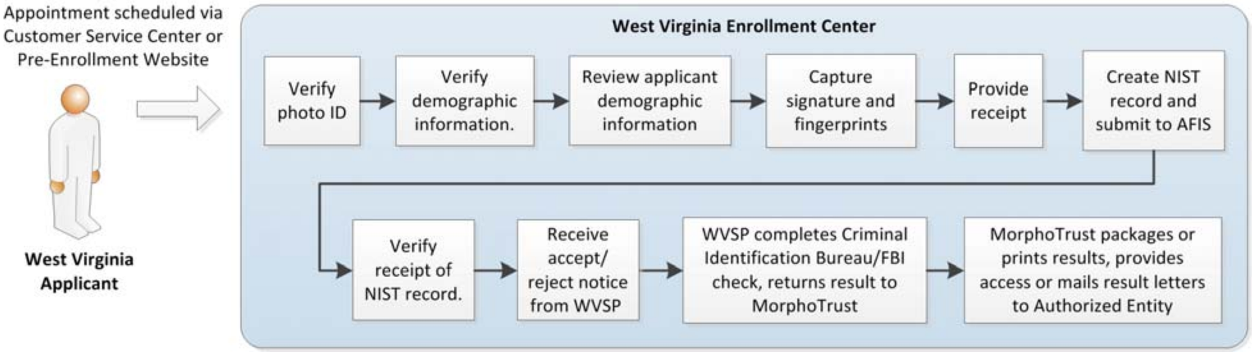

Appointment scheduled via Customer Service Center or Pre-Enrollment Website
West Virginia Applicant
West Virginia Enrollment Center
Verify photo ID
Verify demographic information.
Review applicant demographic information
Capture signature and fingerprints
Provide receipt
Create NIST record and submit to AFIS
Verify receipt of NIST record.
Receive accept/ reject notice from WVSP
WVSP completes Criminal Identification Bureau/FBI check, returns result to MorphoTrust
MorphoTrust packages or prints results, provides access or mails result letters to Authorized Entity

Figure 9: Overview of the Enrollment Process

Table 11 provides a more detailed list of the steps in the appointment process, with additional description of the process on the following pages.

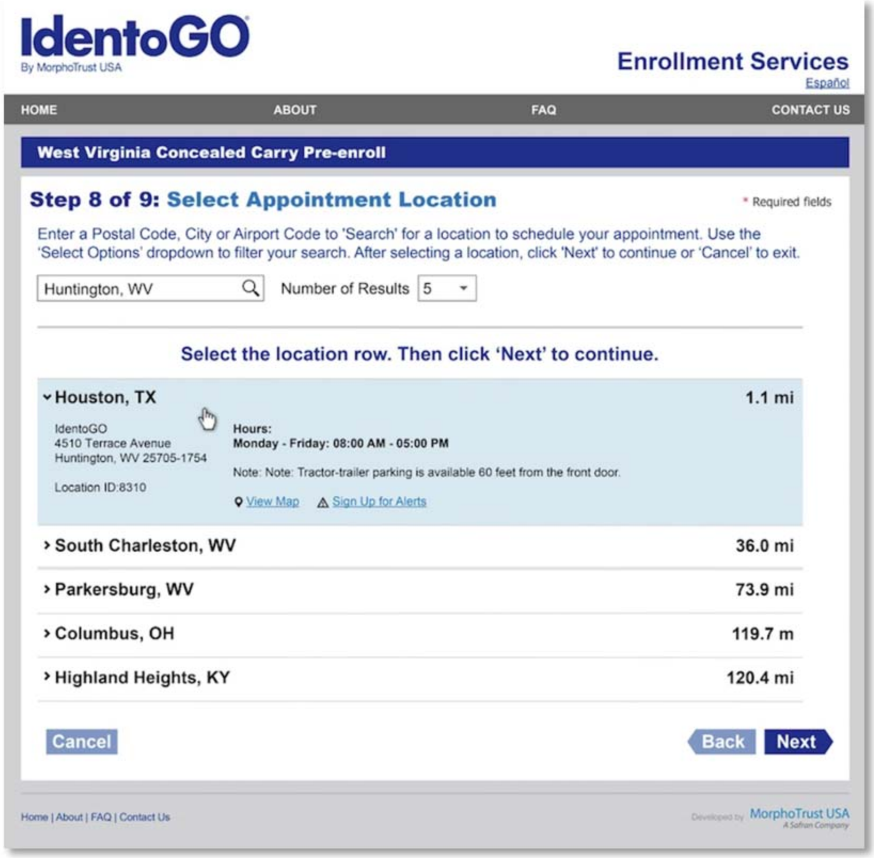
Table 11: Steps in the Applicant Appointment Process

Appointment Scheduling	• Applicant schedules appointment either online or by calling Customer Service Center • Applicant can opt to pay fees by a variety of methods • Applicant receives appointment tracking number and confirmation information • If an email address is provided, appointment information is emailed to the applicant along with a link to an online mapping of appointment location
In Person at Enrollment Center	• Applicant's record is loaded on Livescan from the MorphoTrust Central Server • Applicant’s photo ID is authenticated • Applicant's ID is checked against the demographic data supplied at time of appointment scheduling • Applicant is asked to verify all demographic information • Applicant is asked to review terms and conditions and provide signature through signature pad device • Applicant is fingerprinted • Applicant pays fee if not paid at time of appointment scheduling • Applicant is provided with a receipt of the transaction. Receipt includes the State Control Number, date, applicant type, amount paid and signature of Enrollment Agent
After Appointment	• Records are transmitted in real time from fixed sites • Records are transmitted within 24 hours for mobile sites or onsite fingerprinting sessions without an internet connection

Process for Pre-Enrollment and Appointment Scheduling

Applicants can register and schedule appointments by calling MorphoTrust's Customer Service Center or by scheduling directly through our secure Pre-Enrollment website, which safeguards the applicant's personal and financial information using a Secure Socket Layer protocol (SSL) following industry standards for encryption. Our single point Pre-Enrollment Website provides applicants and the public with general program information and instructions to navigate them easily through the appointment process.

The Pre-Enrollment Website provides a list of Enrollment Centers that can be easily searched by region or zip code. As shown in Figure 10, applicants will see the hours of operation and appointments available at each West Virginia Enrollment Center and will be able to scroll through the timeline to locate an appointment that fits their calendar.



West Virginia Concealed Carry Pre-enroll

Step 8 of 9: Select Appointment Location

* Required fields

Enter a Postal Code, City or Airport Code to 'Search' for a location to schedule your appointment. Use the 'Select Options' dropdown to filter your search. After selecting a location, click 'Next' to continue or 'Cancel' to exit.

Huntington, WV

Number of Results 5

Select the location row. Then click 'Next' to continue.

Houston, TX	1.1 mi
South Charleston, WV	36.0 mi
Parkersburg, WV	73.9 mi
Columbus, OH	119.7 m
Highland Heights, KY	120.4 mi

IdentoGO
4510 Terrace Avenue
Huntington, WV 25705-1754

Location ID:8310

Hours:
Monday - Friday: 08:00 AM - 05:00 PM

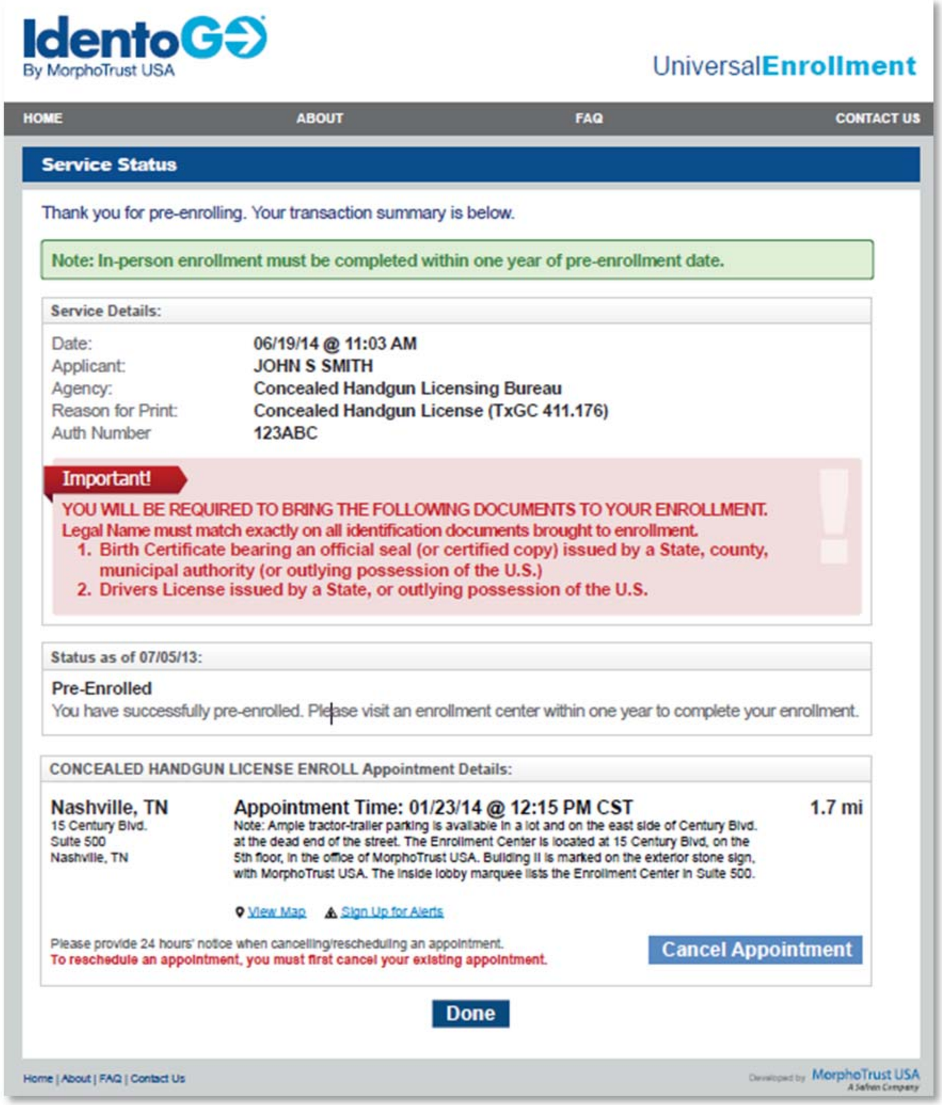
Note: Note: Tractor-trailer parking is available 60 feet from the front door.

View Map Sign Up for Alerts

Figure 10: Selecting an Appointment Location from the List of Enrollment Centers

The Pre-Enrollment Website lists MorphoTrust's fingerprint Enrollment Centers in West Virginia by region or zip code, shows available appointments, provides directions, and links to an online map. Applicants can book a fingerprinting appointment and cancel or change a scheduled appointment without additional rescheduling cost.

After the applicant has scheduled an appointment, a confirmation page (shown in Figure 11) lists the appointment details and reminders to help the applicant prepare for a successful visit to a fingerprinting Enrollment Center.



Service Status

Thank you for pre-enrolling. Your transaction summary is below.

Note: In-person enrollment must be completed within one year of pre-enrollment date.

Service Details:

Date:	06/19/14 @ 11:03 AM
Applicant:	JOHN S SMITH
Agency:	Concealed Handgun Licensing Bureau
Reason for Print:	Concealed Handgun License (TxGC 411.176)
Auth Number	123ABC

Important!

YOU WILL BE REQUIRED TO BRING THE FOLLOWING DOCUMENTS TO YOUR ENROLLMENT.
Legal Name must match exactly on all identification documents brought to enrollment.

1. Birth Certificate bearing an official seal (or certified copy) issued by a State, county, municipal authority (or outlying possession of the U.S.)
2. Drivers License issued by a State, or outlying possession of the U.S.

Status as of 07/05/13:

Pre-Enrolled
You have successfully pre-enrolled. Please visit an enrollment center within one year to complete your enrollment.

CONCEALED HANDGUN LICENSE ENROLL Appointment Details:

Nashville, TN
15 Century Blvd.
Suite 500
Nashville, TN

Appointment Time: 01/23/14 @ 12:15 PM CST — 1.7 mi

Note: Ample tractor-trailer parking is available in a lot and on the east side of Century Blvd. at the dead end of the street. The Enrollment Center is located at 15 Century Blvd, on the 5th floor, in the office of MorphoTrust USA. Building II is marked on the exterior stone sign, with MorphoTrust USA. The inside lobby marquee lists the Enrollment Center in Suite 500.

Please provide 24 hours' notice when cancelling/rescheduling an appointment.
To reschedule an appointment, you must first cancel your existing appointment.

Figure 11: Appointment Confirmation

The confirmation page provides appointment details, payment information, address of the Enrollment Center, details for preparing for the appointment, and a link to an online map.

Onsite Identification Process

Currently, the Enrollment Agent reviews the applicant's valid photo identification prior to capturing fingerprints, in accordance with state guidelines. The Enrollment Agent ascertains, to the best extent possible, that the person is being fingerprinted for the intended purpose and is the person shown on the ID. Acceptable forms of identification will be required. If an applicant presents an ID that is out of date, the Enrollment Agent informs them that they will need to obtain a valid ID before they can be fingerprinted.

Information about the requirement to present valid identification documents before being printed and what types of identification are acceptable is provided to the applicant at the time they schedule their appointment.

Once our UEP solution is deployed, workstations will be equipped with our proprietary document authentication software and B5000 reader to analyze state or federal government-issued photo identification documents for authenticity. This feature provides improved identity document authentication as compared to the current process.

We have provided additional information on document authentication can be found in Section 4.4.6.1, with the B5000 reader shown in Figure 33

Biographic Data Review

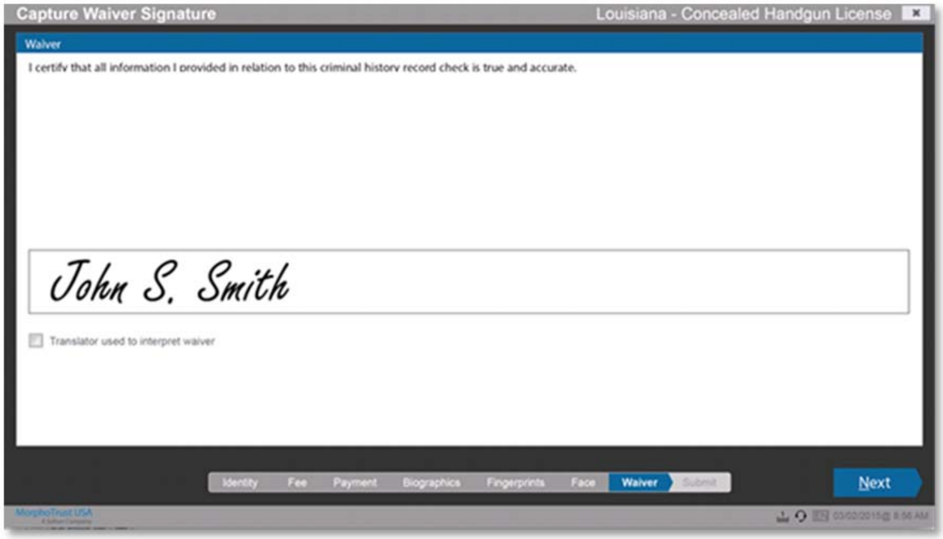
When applicants arrive at the Enrollment Center for their fingerprint appointment, any information provided during pre-enrollment is pre-loaded onto the workstation. However, MorphoTrust employs a double-check system to ensure that applicants are providing truthful and accurate information. If any data provided on the document does not match the information given, the software requires the Enrollment Agent to resolve the conflict.

Payment

As described in our response to 4.4.2.6, MorphoTrust will accept certified check, money order, or credit card as a form of payment.

Release of Record Authorization Process

The Release of Record Authorization Process is accomplished by presenting a waiver on the workstation and collecting the applicant’s signature (shown in Figure 12) using a Topaz signature pad.



Waiver

I certify that all information I provided in relation to this criminal history record check is true and accurate.

John S. Smith

□ Translator used to interpret waiver

Figure 12: Signature Capture

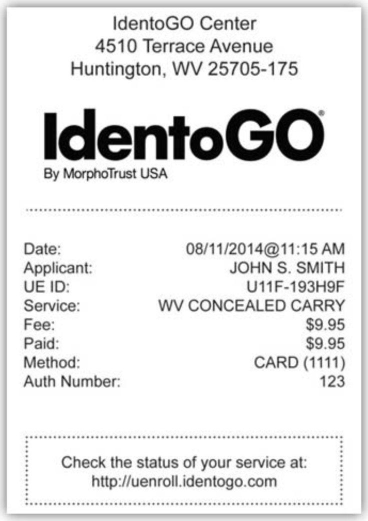
Collection of Digital Fingerprints

Our workstation software is a workflow-driven application that walks both the Enrollment Agent and the applicant through the fingerprint collection process. We recognize that image quality is the most important component of a fingerprint collection system. The workstation software automatically calculates the quality of fingerprint captures, giving real-time feedback to the Enrollment Agent. This fingerprint Quality Assurance process helps eliminate rejects due to of image quality issues.

As an optional feature, our administrative portal provides the ability for agency personnel to investigate their customer’s transactions. Transaction details that may be viewed include service status, steps to fulfill service, and details of the service including the ability to view captured biometrics and documents. This level of detail provides forensic capabilities for the adjudicator for moderate-to-high risk security customers.

4.4.3.4 The Vendor should describe in detail their plan to provide a receipt to each Applicant to verify successful completion of the fingerprinting service.

MorphoTrust currently complies with this requirement and will continue to do so upon contract award. We assign a unique ten-character enrollment identifier to each transaction, which will remain unique for the duration of the contract. We will continue to provide a receipt to each applicant at the conclusion of their enrollment. Figure 13 shows a sample receipt.



IdentoGO Center
4510 Terrace Avenue
Huntington, WV 25705-175

IdentoGO®
By MorphoTrust USA

Date:	08/11/2014@11:15 AM
Applicant:	JOHN S. SMITH
UE ID:	U11F-193H9F
Service:	WV CONCEALED CARRY
Fee:	$9.95
Paid:	$9.95
Method:	CARD (1111)
Auth Number:	123

Check the status of your service at:
http://uenroll.identogo.com

Figure 13: Transaction Receipt

The receipts have been developed to ensure the format and data elements included meet the needs of the State and the applicants. In other MorphoTrust networks, additional data elements include fee paid amount, applicant type, agency, and facility number. Applicants often use these receipts for their own records and/or for submission to their agency for reimbursement or proof of compliance.

As an optional feature with UEP, an applicant may view the status of their transaction online at any time. The online status includes the date of service, method of payment, payment amount, and the Transaction Control Number.

4.4.3.5 The Vendor should describe in detail the time frame of transmitted results.

Fingerprint records are transmitted from the Enrollment Center to the central MorphoTrust process server in real time. For mobile sites or onsite fingerprinting sessions that do not have an internet connection, records are transmitted within 24 hours.

The MorphoTrust central server transmits records as they are received into the WVSP system. Any records that do have not a confirmed payment (such as a check) may be held for up to five business days or until payment is confirmed as valid.

Criminal History Records are electronically forwarded in near real time, once received from the WVSP and/or the FBI. Results electronically delivered, if allowed, will be available in near real time as soon as response is received from the WVSP and/or the FBI. When required, hard copies are printed on a daily basis for all available responses and placed in outgoing USPS mail for delivery. Access to hard copy results are subject to standard USPS mail delivery timelines.

4.4.3.6 The Vendor should describe in detail their plan for electronic submission acceptance requirements.

As the current provider of fingerprinting services in West Virginia, MorphoTrust fully understands and meets the requirements of the technology solution for electronic submission into the WVSP system. Our technology component known as EasyPath will remain in place with the new contract; therefore submissions into WVSP will continue to support the State's requirements.

Should WVSP adopt new interface requirements in the future, WVSP can request a Custom Engineering Change (see Attachment F) and MorphoTrust's technical staff will adapt our solution to meet the new requirements for the systems interface control specification.

As detailed our response to requirement 4.5.3 (d), we agree to maintain a ninety-eight percent (98%) classifiable rate for all Livescan fingerprint submissions digitally collected by MorphoTrust and our partners.

4.4.3.7 The Vendor should describe in detail their plan on fingerprint technician training procedures and curriculum used.

MorphoTrust's training programs are designed to give all personnel and support teams the knowledge, tools, resources and escalation and/or resolution paths needed to provide accurate and high quality service to applicants the first time, so that repeat visits are minimized and the customer experience is positive.

Enrollment Agent Certification Training

All fingerprint technicians (referred to by MorphoTrust as Enrollment Agents) for the West Virginia Enrollment Centers, whether MorphoTrust employee, partner, or subcontractor, are required to complete an internal certification process to ensure the Agent is competent to perform the job responsibilities, functional requirements of operating the equipment, and quality standards of performance. Our professional certification process blends the use of a scripted training manual with supervisory/trainer observation and Enrollment Agents work demonstration.

Our Quality Training Program

Our proven Training Program has been utilized to train over 3,500 Enrollment Agents (fingerprint technicians) to date.

We believe that training is critical to develop a fully qualified Enrollment Agent capable of achieving a 98% classifiability rate, dealing with the general public, and handling equipment issues.

Enrollment Agents hired for this project will go through an orientation and systematic training program that focuses on the West Virginia program requirements. Upon the Enrollment Agent's completion of the onsite training, Certified Trainers use a pre-defined Observed Behaviors Checklist to track the enrollment agent's competency and understanding of all written policies/procedures. The checklist identifies on-the-job behaviors expected of all personnel such as professional customer interaction, professionalism, policy and procedure compliance, system navigation, capturing quality prints and mastery of required skills.

Training Curriculum

Our training program consists of:

- Hardware overview of the Livescan workstation.
- Software overview of the Livescan system. The Enrollment Agent must become skilled in the operation of all Livescan software. This includes how to electronically transfer and receive demographic information, transfer fingerprints to the secure Data Center, and perform all system maintenance and system utility functions. Training is conducted on the identification of pattern type, delta(s), core, and determining the overall quality of the fingerprint
- Technical support overview of diagnostic functions.
- Field training - The Enrollment Agent trainee will be placed with an experienced Enrollment Agent who double-checks the quality of each fingerprint taken, and instructs the trainee on how to capture fingerprints most efficiently and effectively. Enrollment Agents will fingerprint many test applicants prior to completing the on-site training program.
- Best-practice customer service (attitude, dealing with difficult people, escalation processes, MorphoTrust customer service policies)
- Security and Confidentiality (data, personal information, MorphoTrust security protocols)
- Program specifics (Agency information, Applicant types, required forms and information, assisting applicants in obtaining necessary information)

- MorphoTrust Corporate and Enrollment Services general information (who to contact, web links)
- Review of company policies with each Enrollment Agent. Among other topics, this includes instruction on quality standards, security procedures, emergency procedures, privacy policies, personal appearance, identification verification, state fingerprinting laws and requirements, how to interact professionally with the client and how to make the applicant's fingerprinting experience as pleasant as possible.

Training and Operations Manual

Our Enrollment Center policies and procedures address issues such as Enrollment Agent training, security, identification verification and chain of custody of records as recommended in the FBI Identity Verification Program Guide. Each Enrollment Agent is provided a Training and Operations Manual for use during their training and as an ongoing reference. This manual is a living document containing general and network specific information which is updated regularly as changes or additions are made to the network.

Topics covered in the manual include:

- Network Contact Numbers (Scheduling & Customer Service, Operations Management, Technical Troubleshooting and Assistance)
- Overview of MorphoTrust and the Program Network
- MorphoTrust Security Policies and Procedures
- Applicant Registration/Appointment Scheduling
- Program-Specific Contractual Requirements (Acceptable Forms of ID, Photo Capture, Fingerprint Quality, Payment Processing, E-Pay, Receipt Generation)
- Applicant Processing – State to End Workflow (Identification Verification, Fingerprinting, Photo Capture [where used], Save and Transmit, Confirmation and Receipt Printing)
- Troubleshooting (Equipment Power, Missing Applicant Data, ia-Authenticate [where used], Input Forms, Fingerprinting, Photographs, Record Submission, Receipts)
- Frequently Asked Questions
- General MorphoTrust Operating Policies
- General Maintenance and Livescan manual

- Best Practices & Approved Supplies
- Sample Information Form

Computer-Based Training

In addition to the required hands-on training delivery method and user manual, CSRs/Help Desk and Enrollment Agents complete computer-based training via a tailored Learning Management System (LMS). The LMS is a secured platform and can only be accessed by assigned usernames and passwords.

LMS courses are designed to augment and enhance overall learning experience. Courses include job specific training and are used as prerequisite training, for annual recertification of required courses, and as supplement retraining if the need should arise. The LMS allows for tracking of each individuals student record, test scores and completion status of required training.

Our training programs are designed to give Enrollment Agents, CSRs and Help Desk support teams the knowledge, tools, resources and escalation/resolution paths needed to provide accurate and high quality service to applicants the first time, so that repeat visits are minimized and the customer experience is positive.

Performance Evaluations

All new hires also receive a 90-day performance evaluation, regardless of their status as MorphoTrust employee, partner, or subcontractor. The evaluation provides supervisors a formalized process to acknowledge accomplishments, address any learning curve issues, and discuss areas for improvement. Our team remains engaged with all Enrollment Agents throughout their career at MorphoTrust, offering retraining, performance incentives, career development paths, professional development, and supplemental training (i.e., management training, PMP certification, etc.).

4.4.4 Provide automated results processing capability, security and billing system.

4.4.4.1 The Vendor should describe in detail their plan to collect and house Applicant fingerprint submissions including print images, signatures and demographic data on a central server which should at a minimum include their archive retention plan, submission storage format, unplanned outage procedures, re-transmission procedures and backup plan.

MorphoTrust currently provides all results processing, security, and billing systems for the State of West Virginia. Upon contract award, we will continue utilizing the infrastructure in place that meets all RFP requirements.

Collecting and Housing Fingerprint Submissions in UEP

In our UEP solution, MorphoTrust maintains an electronic record of every service provided. This record may be used to track the status of an enrollment that has started but not yet been fulfilled. It also serves as a record of past services provided.

For each record, MorphoTrust maintains (for the duration of the data retention period) all transaction details including:

- The complete demographic data of the applicant
- The fingerprints of the applicant
- The date of their enrollment, the date the record was transmitted to the State, and the date the results were received
- The location where they enrolled
- The identity of the Enrollment Agent who captured their fingerprints
- The service for which the applicant was printed (which includes the Reason for Print, agency, price and other configurable fields)
- The type of identity document provided by the applicant including the document number, issuance date, and expiration date
- The applicant’s signature
- The method of payment and the amount paid by the applicant

Archive Retention Plan

By default, UEP retains all applicant data and submission information for audit purposes. By default, data is purged 365 days following the applicant’s enrollment, but the platform is easily configurable to purge applicant data according to the retention policies of the State. For example, the system may be configured to purge all of an applicant’s data 180 days following their enrollment.

In accordance with CJIS policy, any Criminal History Record Information (CHRI) is purged 30 days after receipt.

Submission Storage Format

UEP is fully EBTS v10.0 compliant and all submissions to the WVSP AFIS will be in the EBTS format. MorphoTrust will use the existing Secure File Transfer Protocol to transmit fingerprint records to the WVSP from our secure Data Center.

Retransmission Procedure

UEP actively seeks an electronic acknowledgement for each submission. If no acknowledgement is received within 24 hours, the record is automatically queued for research and resolution.

The procedure for resolving an unaccepted submission is as follows:

1. If the record was rejected due to formatting issues or biographic issues, a MorphoTrust Support Engineer will attempt to correct the record and resubmit it.
2. If no rejection response was received, a MorphoTrust Support Engineer will attempt to resubmit the record once. Again, if no response is received, the issue will be escalated with the State's AFIS support team.
3. If the submission was rejected due to poor print quality, the applicant will be notified that their prints will need to be recaptured. Once their prints are recaptured, the new record will be submitted to the State.

Backup, Fault Tolerance, and Procedure for Unplanned Outages

UEP is serviced by our Data Center in Franklin, TN. Within this Data Center, our network, storage, and computing devices are deployed in a reductant fashion, which allows for seamless failover when one device fails.

At the data storage layer, our NAS system prevents loss of data, even if a disk fails, by ensuring all data is stored on multiple disks. At the network layer, if a network device fails, a backup device will automatically take over. At the application layer, if an operation fails, the software is programmed to automatically retry.

By providing redundancy at every layer of our solution, we can ensure no data will be lost due to a hardware failure and that data integrity can be maintained during a failover event. Further, in the event of a power outage, our Data Center is provided with diesel-generated power to maintain services.

Our workstations are designed to work on a limited basis in offline mode, so they will continue to function during Data Center or internet outages. When services to the Data Center are restored, the data from the workstations will be uploaded to the Data Center and processing will resume.

If an outage does impact an Enrollment Center causing a closure, UEP has the capability to automatically notify applicants via email and phone.

4.4.4.2 The Vendor should describe in detail their plan to connect their central collection server to the state system in such a way that the information being transmitted is secure and protected.

MorphoTrust will continue to use our proven interface with the State of West Virginia's network, hardware, and software environment. We currently interface with the WVSP AFIS and have successfully sent approximately 220,000 NIST submissions securely through this interface. We will continue to secure and protect the information being transmitted under the new contract.

All enrollment workstations connect to MorphoTrust's Data Center in Franklin, TN via a secure Virtual Private Network (VPN) tunnel. Immediately upon completion of the enrollment, the fingerprints and demographic data are transmitted to the back-end systems via this secure tunnel. Our system then packages and transmits an EBTS compliant record to the Transaction Control Processor housed in the WVSP Data Center over another VPN tunnel, using FBI CJIS Security Policy required encryption standards. From there the data is stored and then forwarded on to the State of West Virginia's AFIS system.

Both our current solution and our proposed UEP system maintain adequate disk capacity to store all fingerprints submissions in the event a communications circuit is not operational. Once the circuit is available again, the system automatically transmits its backlog of records. No records are deleted until the State AFIS has confirmed receipt.

We bring the experience of successfully interfacing to more than 20 State AFIS systems, including 11 MorphoTrak AFIS systems. We currently submit fingerprints to the state and federal AFIS systems shown in Table 12.

Table 12: MorphoTrust's Current State and Federal AFIS Interfaces

MorphoTrust State AFIS Interfaces		
Arkansas (MorphoTrak AFIS)	Massachusetts (MorphoTrak AFIS)	South Carolina* (MorphoTrak AFIS)
California	Michigan	Tennessee* (MorphoTrak AFIS)
Idaho	Minnesota (MorphoTrak AFIS)	Texas*
Illinois	New York* (MorphoTrak AFIS)	Utah
Indiana*	Nevada**	Virginia
Florida (MorphoTrak AFIS)	Oklahoma* (MorphoTrak AFIS)	Washington State*
Maine* (MorphoTrak AFIS)	Oregon (MorphoTrak AFIS)	West Virginia* (MorphoTrak AFIS)
Maryland	Pennsylvania	
**MorphoTrust is the exclusive fingerprint vendor in these states.* ***MorphoTrust is the civil applicant portal to the state.*		
MorphoTrust Federal AFIS/Server Interfaces		
Federal Bureau of Investigation IAFIS*** Transportation Security Administration (TSA) Financial Industry Regulatory Authority (FINRA) American Bankers Association (ABA)		
****MorphoTrust is a certified Federal Bureau of Investigation Channeler*		

4.4.4.3 The Vendor should describe in detail, with examples, their personnel, physical and technical security controls and policies in place that demonstrates their ability to protect the Applicant information.

MorphoTrust's Commitment to Protecting Personally Identifiable Information (PII)

As a U.S. Proxy Corporation, MorphoTrust adheres to stringent National Security Agency (NSA) and Proxy requirements.

We have robust, formalized policies to address all aspects of system security, including those governing the security of user accounts, network, infrastructure, and data. These policies are evaluated and approved by the U.S. Government security oversight committees that monitor our compliance.

Logical Access Security Controls

MorphoTrust enforces strict authentication polices for enrollment workstations and any other software application that accesses Personally Identifiable Information (PII).

No user can access the enrollment workstation software application without first logging in via a username and password. The software requires a password change at initial login and after a reset. In addition to requiring users to change their password, we employ other methods to control the security of the passwords themselves, including:

- A password is never stored in plain-text; it is always stored as a one-way hashed value
- There is no facility in the application to reveal a password
- Users are required to enter a configurable minimum number of characters, numbers, and symbols for their password

- User ID/password management is performed by the System Administrator

MorphoTrust's password rules are compliant with the FBI CJIS 5.3 standard. We require password to:

- Be a minimum length of eight (8) characters on all systems.
- Not be a dictionary word or proper name.
- Not be the same as the User ID.
- Expire within a maximum of 90 calendar days.
- Not be identical to the previous ten (10) passwords.

Furthermore, our systems do not transmit passwords in the clear outside the secure location and do not display passwords when entered.

UEP passwords expire every 90 calendar days and accounts are automatically locked out after three unsuccessful login attempts.

Personnel Security

MorphoTrust follows a successful and repeatable process to vet, onboard, and train personnel. All personnel must be U.S. citizens and must pass a rigorous background check.

MorphoTrust adheres to a strict Training Plan to make sure all personnel working on fingerprint programs are fully trained on standards of performance and operational excellence. These training standards are applicable without bias to MorphoTrust employees, partners, and subcontractors.

Physical Security

Physical access control is provided by the Individual Authorization Request (VAR) process, Closed Circuit Television Cameras (CCTV) surveillance, man-traps, identity validation, cipher locks, access logs, and multi-factor authentication for physical access.

Any person entering the Data Center is considered a visitor. This includes MorphoTrust employees entering to access enrollment systems. If an individual does not have an active electronic card key, the individual must be escorted by an individual with a valid VAR and active electronic card key. If the visitor has a valid VAR and electronic card key, they may enter the lobby by holding the electronic card key near the proximity reader and then entering a valid Personal Identification Number (PIN). This will unlock the door and allow the visitor into the lobby. The Data Center utilizes CCTV to record all individuals outside the door and inside the lobby. All access is automatically logged in the operations center.

A man trap area between the lobby and the Data Center floor requires two factor authentication (electronic card key and PIN). Authorized individuals must hold their valid electronic card key near another proximity reader and enter a valid PIN to enter the man trap. Inside the man trap, a CCTV camera captures all activity. All physical access attempts are logged via the electronic card key reader in the facility operations center. Authorized individuals must then hold their electronic card key near another proximity reader and provide their biometric factor. If authorized, the exit door to the man-trap will unlock and allow access to the Data Center floor. A CCTV camera captures all individuals entering the Data Center floor. CCTV cameras throughout the Data Center capture the movement of visitors within the facility.

Individuals with valid VARs but without electronic card keys must be escorted from the lobby by a VAR-holder with a card key to enter the Data Center floor. All individuals accessing the cabinets containing enrollment systems must sign into the MorphoTrust visitor log book.

The facilities are equipped with gas-based fire suppression systems and by dry-pipe sprinkler systems. Fire suppression systems in the Franklin, TN, Data Center utilize Dual Action Dry Pipe and Halon 1301 Gas Fire Suppression; the Richmond, VA, Data Center utilizes HFC-125 gas fire suppression and dual-zone pre-action dry pipe with VESDA early warning systems. These configurations ensure that fires may be suppressed without damage to the equipment. The sprinkler systems are only used if the gas-based systems prove ineffective during a fire event. The sprinkler systems are zoned to minimize water damage to equipment should water be needed to suppress a fire. In addition, Class C fire extinguishers are located throughout the facilities. Pre-combustion (ion) and combustion (smoke) detectors are located throughout the facilities, and are powered by an electrical circuit that backed by the facility UPS. Fire detection, preparedness, response and evacuation drills are conducted at least annually, in accordance with municipal fire department regulations. The local fire department audits the facilities as required.

Battery backups and diesel generators are in place to supply uninterrupted power in the event of a utility power outage.

Network Security

The UEP network is divided into zones for security and separation of concerns (Figure 14). Workstations, which are connected to the public internet at Enrollment Centers across the nation, exist in an "Untrusted" network zone.

Through a Virtual Private Network (VPN) tunnel, the workstations gain access to a "Semi-Trust" network zone. In this zone, requests for allowed services are proxied through to the "Trust" network zone hosting the desired service. There are multiple Trust Zones, properly partitioned for separation of concerns.

Finally, a "Secure" network zone hosts all persistent storage of Personally Identifiable Information (PII). Only the Trust Zone for the UEP application tier has access to this Secure Zone.

When information is exchanged between networks, it is always through an encrypted channel.

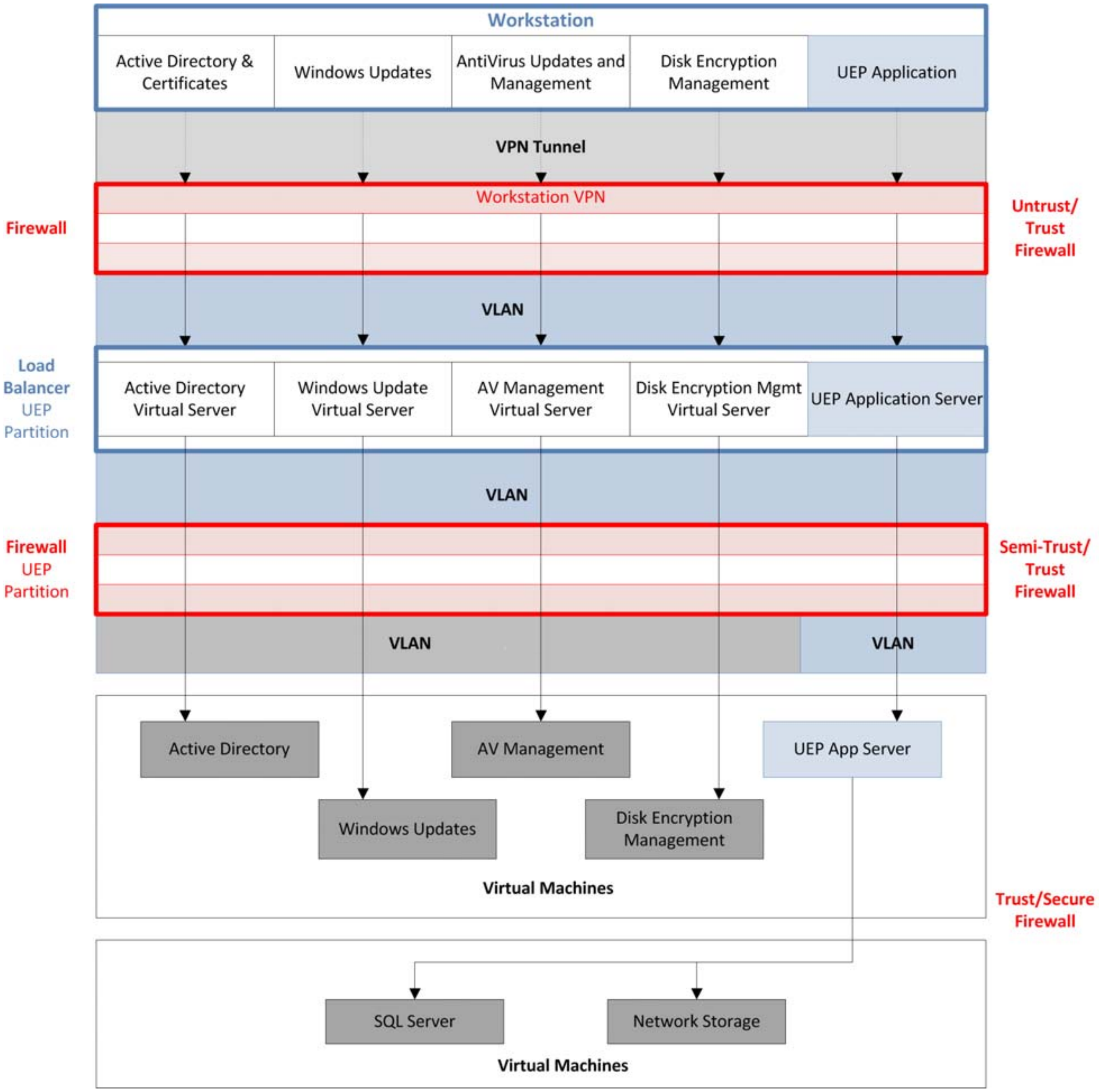


Figure 14: UEP Workstation Network Topography

Multiple tiers of "Trust Zones" protect Personally Identifiable Information from the point of collection to secure submission.

Auditing

For auditing of solution access and key data changes, the system architecture includes Security Information and Event Management (SIEM) capability, which provides complete auditing of events across the solution components. Key user access audit capabilities include:

- Log-on attempts (successful and unsuccessful)

- Password change attempts (successful and unsuccessful)
- User account creation, deletion, and permissions changes Attempts to create, modify, or delete system files and directories (successful and unsuccessful)

4.4.4.4 The Vendor should describe in detail their plan to provide a central results server which would house the Applicant background results and be responsible for making results available and providing notification to the appropriate submitting agencies as well as reporting capabilities. This plan should include at a minimum the physical location of the server, technical and security controls required to meet the current CJIS Security Policy, the method an agency will use to retrieve their results, what information an agency will have available to them from this server and the method the state will use to transmit the results to this central results server.

By continuing to use the centralized results server (aka Transaction Control Processor (TCP)) already installed in the WVSP Data Center, MorphoTrust will continue to receive, store, process, and deliver results with no interruption of service. This solution already operates under WVSP oversight and is compliant with FBI CJIS Security Policies.

Figure 15 provides a solution overview including the central results server. We have provided additional detail about our Results Processor in our response to requirement 4.5.4.

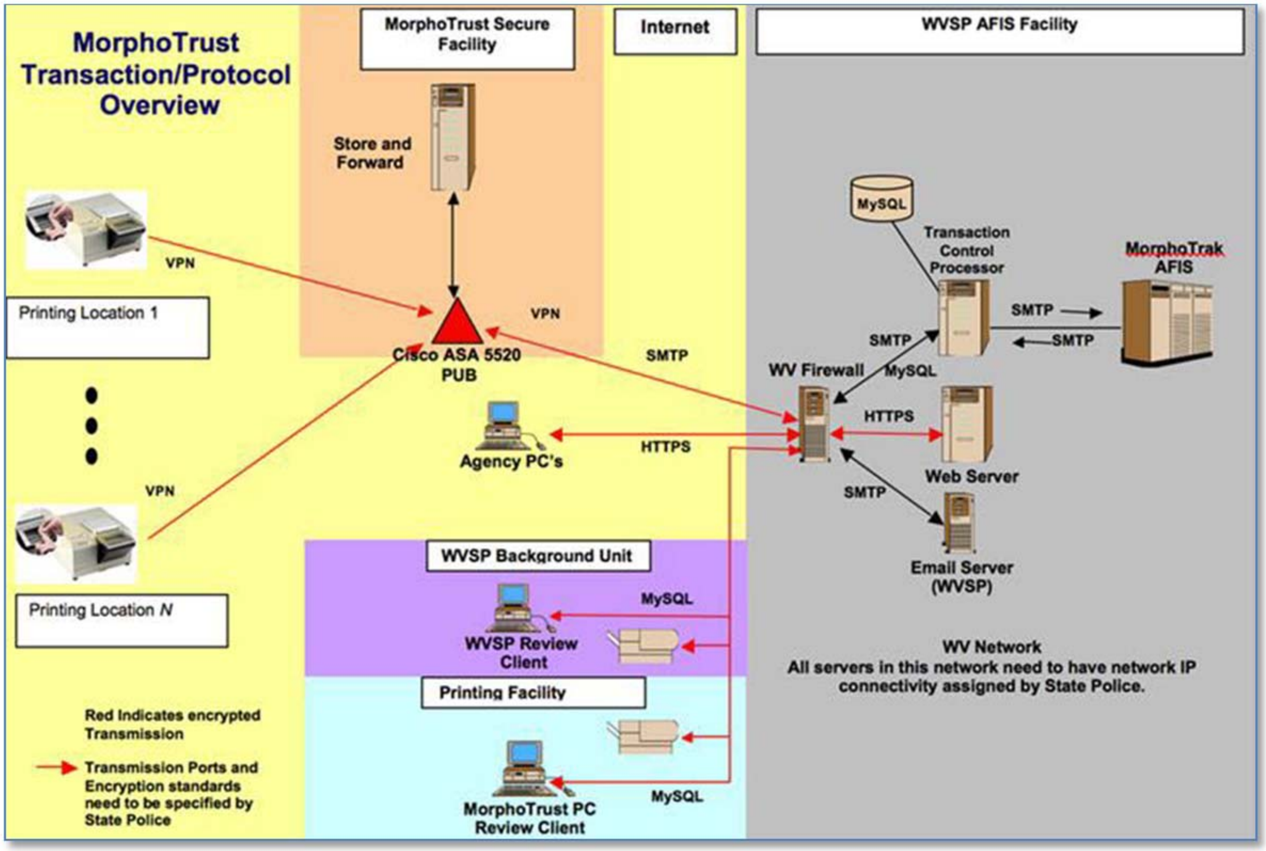

MorphoTrust Transaction/Protocol Overview
MorphoTrust Secure Facility
Internet
WVSP AFIS Facility
Store and Forward
VPN
Printing Location 1
VPN
Cisco ASA 5520 PUB
SMTP
VPN
Printing Location N
Agency PC's
HTTPS
MySQL
Transaction Control Processor
MorphoTrak AFIS
SMTP
SMTP
SMTP
WV Firewall
MySQL
HTTPS
Web Server
SMTP
Email Server (WVSP)
WVSP Background Unit
MySQL
WVSP Review Client
Printing Facility
MySQL
MorphoTrust PC Review Client
WV Network
All servers in this network need to have network IP connectivity assigned by State Police.
Red Indicates encrypted Transmission
Transmission Ports and Encryption standards need to be specified by State Police

Figure 15: Overview of MorphoTrust Technical Solution

This solution already operates under WVSP oversight, using a central results server located in the WVSP Data Center, and is compliant with FBI CJIS Security Policies.

Data Storage

NIST submissions received from the MorphoTrust Central Server, including information such as fingerprints, digital signature, and other status information, are stored on the Transaction Control Processor (TCP) as shown in the preceding Figure 15. From the TCP central server, the NIST submissions are sent to the WVSP AFIS for processing.

State and FBI Result Collection

Returned State and FBI AFIS results are delivered to the TCP via email. The TCP automatically retrieves the results, opens the responses, and attaches the results to the corresponding applicant record. Based upon the response, the TCP performs the following steps:

1. Updates the record status.

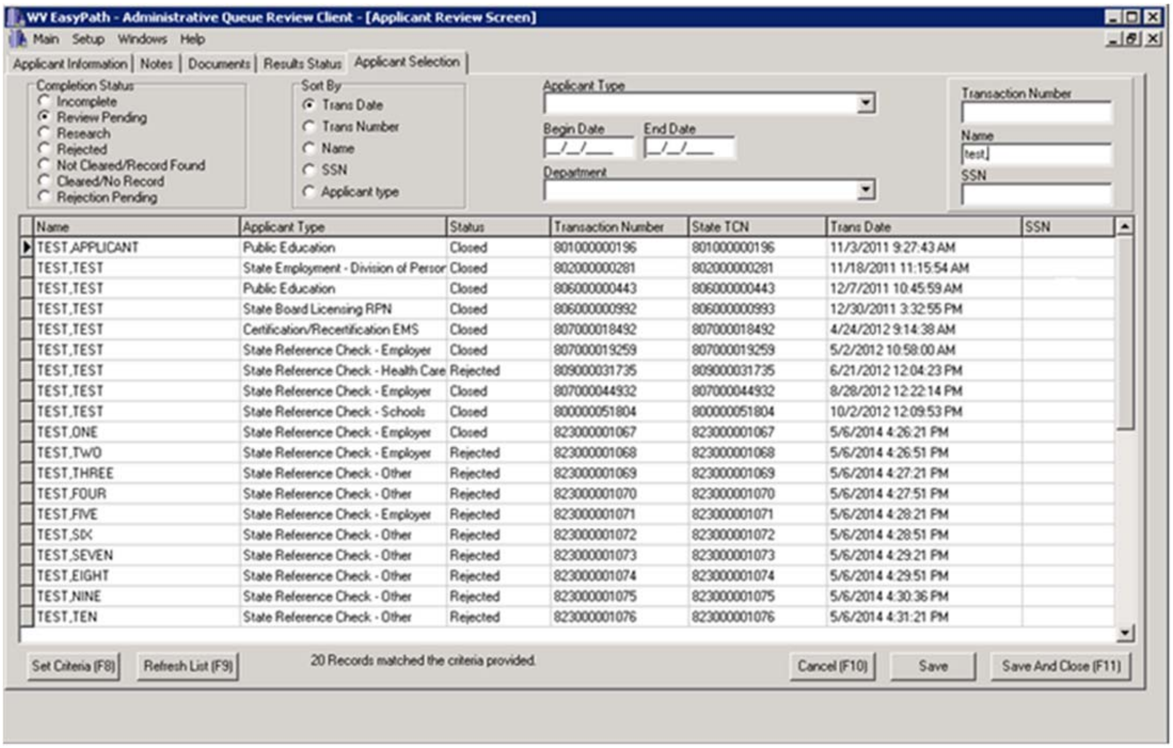
2. Based upon the transaction type submitted, auto-generates email notification to the authorized entity or the individual when no record is found.

Results Notification and Access

MorphoTrust's Review Client application, the front-end user interface for the TCP, includes the following functionality to ensure efficient processing of applicants for West Virginia employing and licensing agencies:

- ***Automated Adjudication Decisions*** – On average, 80% of adjudication decisions are made without human intervention. These decisions are made based upon the criminal history responses received and the pre-specified adjudication criteria (typically, no indication of a criminal record). The result is shorter turnaround times for responses to employing and licensing agencies and minimal effort by State of West Virginia employees to process applicants.
- ***Redaction*** - One or more specific sections of text can be redacted before results are delivered to an agency and/or the applicant. Only non-redacted text is included in denial letters provided to the applicant. The original (full) response is retained within the Review Client for future reference and use by authorized state employees.
- ***Collaboration*** – Notes and attachments can be added to an applicant record as necessary to provide the necessary support information for the final adjudication decision.
- ***Disposition Assignment*** – Authorized personnel can assign a final disposition, which triggers response generation, based upon their permissions.

Figure 16 through Figure 18 show screenshots from MorphoTrust's Review Client application currently provided as part of our West Virginia solution.



Completion Status
- ○ Incomplete
- ● Review Pending
- ○ Research
- ○ Rejected
- ○ Not Cleared/Record Found
- ○ Cleared/No Record
- ○ Rejection Pending

Sort By
- ● Trans Date
- ○ Trans Number
- ○ Name
- ○ SSN
- ○ Applicant type

Applicant Type:

Begin Date: __/__/____ End Date: __/__/____

Department:

Transaction Number:

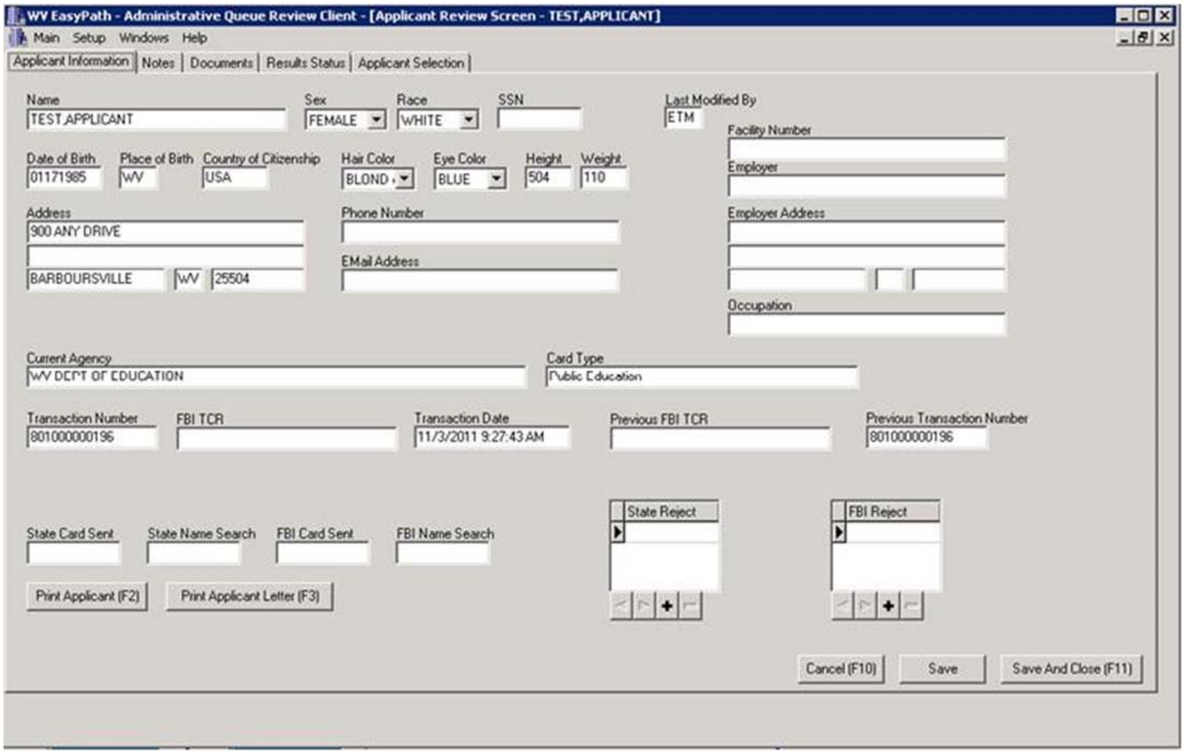
Name: test

SSN:

Name	Applicant Type	Status	Transaction Number	State TCN	Trans Date	SSN
TEST,APPLICANT	Public Education	Closed	801000000196	801000000196	11/3/2011 9:27:43 AM	
TEST,TEST	State Employment - Division of Persor	Closed	802000000281	802000000281	11/18/2011 11:15:54 AM	
TEST,TEST	Public Education	Closed	806000000443	806000000443	12/7/2011 10:45:59 AM	
TEST,TEST	State Board Licensing RPN	Closed	806000000992	806000000993	12/30/2011 3:32:55 PM	
TEST,TEST	Certification/Recertification EMS	Closed	807000018492	807000018492	4/24/2012 9:14:38 AM	
TEST,TEST	State Reference Check - Employer	Closed	807000019259	807000019259	5/2/2012 10:58:00 AM	
TEST,TEST	State Reference Check - Health Care	Rejected	809000031735	809000031735	6/21/2012 12:04:23 PM	
TEST,TEST	State Reference Check - Employer	Closed	807000044932	807000044932	8/28/2012 12:22:14 PM	
TEST,TEST	State Reference Check - Schools	Closed	800000051804	800000051804	10/2/2012 12:09:53 PM	
TEST,ONE	State Reference Check - Employer	Closed	823000001067	823000001067	5/6/2014 4:26:21 PM	
TEST,TWO	State Reference Check - Employer	Rejected	823000001068	823000001068	5/6/2014 4:26:51 PM	
TEST,THREE	State Reference Check - Other	Rejected	823000001069	823000001069	5/6/2014 4:27:21 PM	
TEST,FOUR	State Reference Check - Other	Rejected	823000001070	823000001070	5/6/2014 4:27:51 PM	
TEST,FIVE	State Reference Check - Employer	Rejected	823000001071	823000001071	5/6/2014 4:28:21 PM	
TEST,SIX	State Reference Check - Other	Rejected	823000001072	823000001072	5/6/2014 4:28:51 PM	
TEST,SEVEN	State Reference Check - Other	Rejected	823000001073	823000001073	5/6/2014 4:29:21 PM	
TEST,EIGHT	State Reference Check - Other	Rejected	823000001074	823000001074	5/6/2014 4:29:51 PM	
TEST,NINE	State Reference Check - Other	Rejected	823000001075	823000001075	5/6/2014 4:30:36 PM	
TEST,TEN	State Reference Check - Other	Rejected	823000001076	823000001076	5/6/2014 4:31:21 PM	

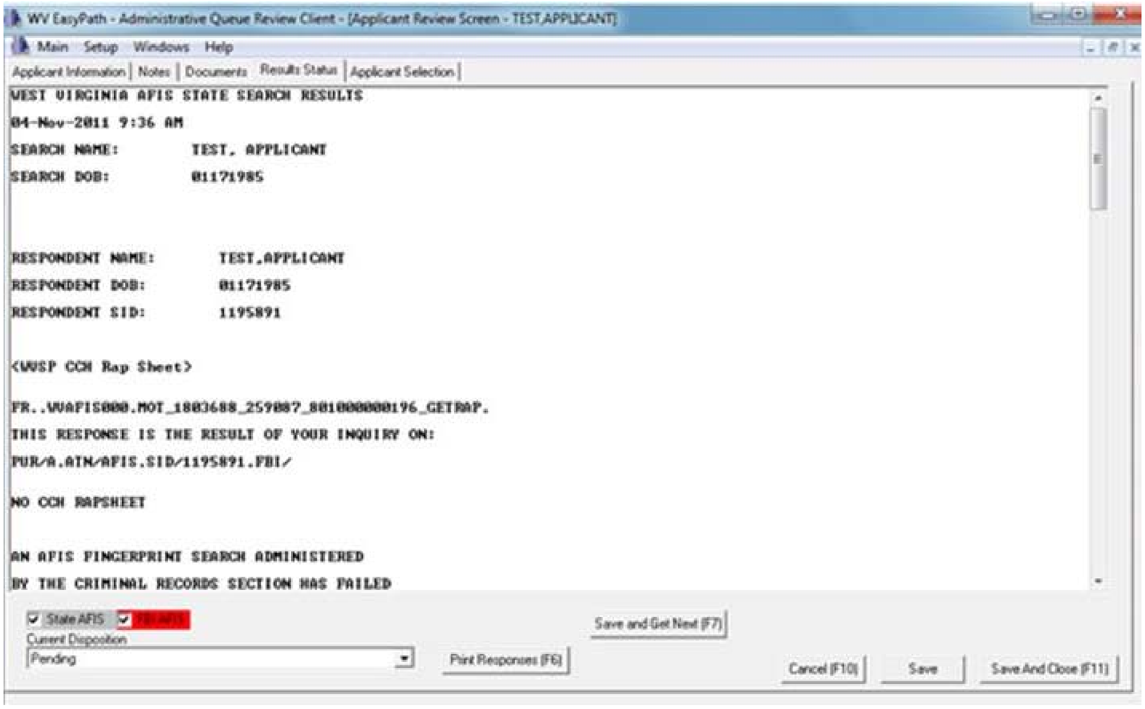
20 Records matched the criteria provided.

Figure 16: Search Records and View Real-Time Transaction Status



Name: TEST,APPLICANT
Sex: FEMALE
Race: WHITE
SSN:
Last Modified By: ETM
Facility Number:
Employer:
Date of Birth: 01171985
Place of Birth: WV
Country of Citizenship: USA
Hair Color: BLOND
Eye Color: BLUE
Height: 504
Weight: 110
Address: 900 ANY DRIVE
BARBOURSVILLE WV 25504
Phone Number:
EMail Address:
Employer Address:
Occupation:
Current Agency: WV DEPT OF EDUCATION
Card Type: Public Education
Transaction Number: 801000000196
FBI TCR:
Transaction Date: 11/3/2011 9:27:43 AM
Previous FBI TCR:
Previous Transaction Number: 801000000196
State Card Sent:
State Name Search:
FBI Card Sent:
FBI Name Search:

Figure 17: View Applicant Detail - Includes demographic and transactional data


WV EasyPath - Administrative Queue Review Client - [Applicant Review Screen - TEST,APPLICANT]
Main Setup Windows Help
Applicant Information | Notes | Documents | Results Status | Applicant Selection |
☑ State AFIS ☑ FBI AFIS
Current Disposition
Pending
Print Responses (F6)
Save and Get Next (F7)
Cancel (F10)
Save
Save And Close (F11)

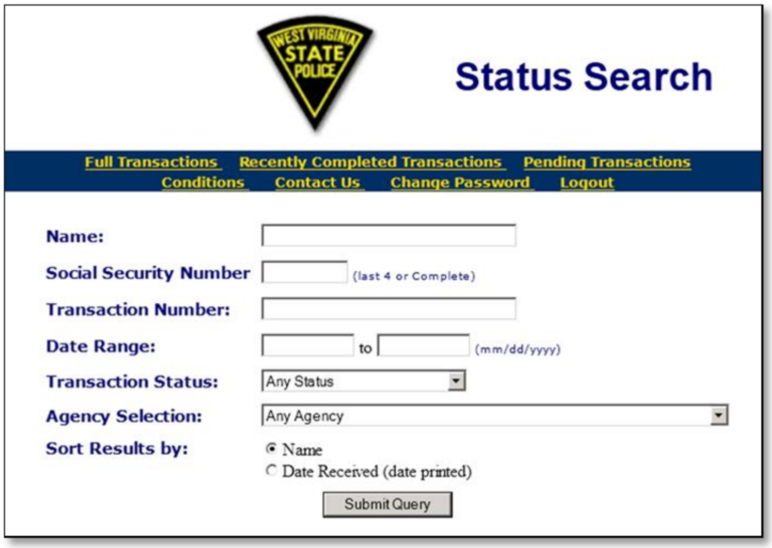
```
WEST VIRGINIA AFIS STATE SEARCH RESULTS
04-Nov-2011 9:36 AM
SEARCH NAME:        TEST, APPLICANT
SEARCH DOB:         01171985


RESPONDENT NAME:       TEST,APPLICANT
RESPONDENT DOB:        01171985
RESPONDENT SID:        1195891

<WVSP CCH Rap Sheet>

FR..WVAFIS000.MOT_1803688_259087_801000000196_GETRAP.
THIS RESPONSE IS THE RESULT OF YOUR INQUIRY ON:
PUR/A.ATN/AFIS.SID/1195891.FBI/

NO CCH RAPSHEET


AN AFIS FINGERPRINT SEARCH ADMINISTERED
BY THE CRIMINAL RECORDS SECTION HAS FAILED
```

Figure 18: View AFIS Responses (State and FBI) - Authorized users can make status changes as needed.

Reporting Capabilities

Authorized Review Client users can access data through the Administrative Web Portal. This allows users to generate ad-hoc reports containing data for their applicants, as well as export the data to an Excel spreadsheet.

Figure 19 and Figure 20 show an example screen of an applicant status search and search results using the Review Client tool.



Name:

Social Security Number (last 4 or Complete)

Transaction Number:

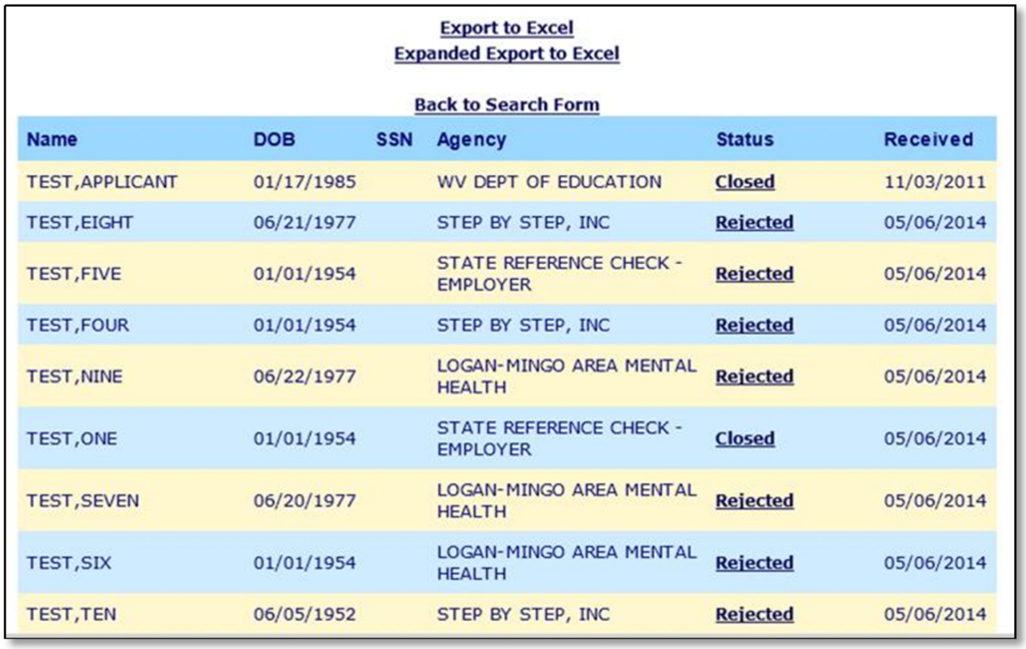
Date Range: to (mm/dd/yyyy)

Transaction Status: Any Status

Agency Selection: Any Agency

Sort Results by: ● Name ○ Date Received (date printed)

Figure 19: Applicant Status Search using Administrative Web Portal



Name	DOB	SSN	Agency	Status	Received
TEST,APPLICANT	01/17/1985		WV DEPT OF EDUCATION	Closed	11/03/2011
TEST,EIGHT	06/21/1977		STEP BY STEP, INC	Rejected	05/06/2014
TEST,FIVE	01/01/1954		STATE REFERENCE CHECK - EMPLOYER	Rejected	05/06/2014
TEST,FOUR	01/01/1954		STEP BY STEP, INC	Rejected	05/06/2014
TEST,NINE	06/22/1977		LOGAN-MINGO AREA MENTAL HEALTH	Rejected	05/06/2014
TEST,ONE	01/01/1954		STATE REFERENCE CHECK - EMPLOYER	Closed	05/06/2014
TEST,SEVEN	06/20/1977		LOGAN-MINGO AREA MENTAL HEALTH	Rejected	05/06/2014
TEST,SIX	01/01/1954		LOGAN-MINGO AREA MENTAL HEALTH	Rejected	05/06/2014
TEST,TEN	06/05/1952		STEP BY STEP, INC	Rejected	05/06/2014

Figure 20: Results of Applicant Status Search

Physical Location

The TCP and Web Portal systems are located in the secure Data Center of the WVSP so WVSP maintains access control. The only MorphoTrust users with access to these systems are the authorized support personnel that have been cleared and approved by WVSP.

Security and Controls

The software and systems are FBI CJIS Security policy compliant in their access control, logging, and encryption policies. User access, password policies, physical access, and other controls are under direct control of WVSP personnel.

While MorphoTrust's network boundary houses all servers, data, and equipment necessary to collect the biometric and biographic data, this data must still be sent to the State's AFIS. Data sent to (and retrieved from) the State will be transmitted over a secure Virtual Private Network (VPN) tunnel.

To maintain compliance with CJIT-ITS v5.3, MorphoTrust uses physical separation of system boundaries for systems that process Criminal History Record Information (CHRI) versus those systems that only transmit the PII needed to initiate the search. To minimize audit (and thus, applicant) costs, MorphoTrust installs the Adjudication, Redaction, and Rap Sheet processing software within the State's boundary, which is already subject to FBI CJIS security controls and audits.

Figure 14 on page 57 shows that all prints are captured in the field and transmitted to the central server over a secure Virtual Private Network (VPN). Prints, along with the demographic data, are transmitted to the Transaction Control Processor (TCP), located within the State's boundary.

The TCP tracks all prints submitted to the State's AFIS from MorphoTrust, and forwards the requests to the AFIS. Responses from the AFIS are returned to the TCP, where they can be accessed and processed via multiple channels, including:

- ***The Review Client*** - used to view applicant details, add notes, and redact results
- ***The Agency portal*** – used by User Agencies to retrieve results and adjudicate their clients
- ***Email server*** – used to notify agency contacts and/or applicants with the status of a relevant transaction
- ***Printer*** - used to print hard copy response notifications

4.4.5 Provide billing system and reports

4.4.5.1 The Vendor should describe in detail their plan to provide a billing system with the public/agencies and between the Vendor and the state. The plan should detail the reconciliation process and escrow accounts establishments, the fee structure and points of contact for discrepancies with billing issues.

Both agencies and employers in West Virginia currently have the option of establishing billing accounts with MorphoTrust. All policies and processes will remain in effect for the new contract period.

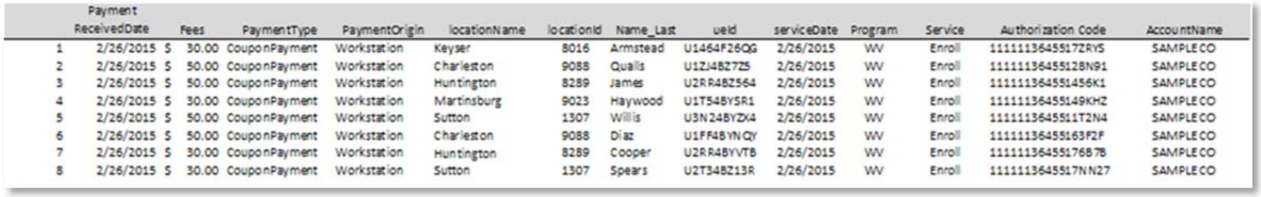
MorphoTrust maintains a Tennessee-based Billing Department with 8:00 A.M. to 5:00 P.M. Central Standard Time support to assist with any invoice or billing account inquiries. Applicants may contact the Customer Service Center for assistance in account reconciliation, discrepancies, or usage questions.

Once UEP is deployed, agencies will have additional options. An agency may provide a specific one-time use Authorization Code that the applicant is required to use. Alternatively, agencies may allow all applicants processed under a specific Service Code to be billed without use of a unique Authorization Code.

Likewise, non-governmental entities will have the option of placing a credit card on file, which will be charged at the time of transaction whenever an Authorization Code is utilized. This reduces the opportunity for fraud via use of shared universal billing account numbers and eliminates the need for employers to maintain a pre-paid balance.

The Customer Service Center provides assistance in utilizing authorization codes.

No enrollment is invoiced to a credit billing account until the applicant transmission is successful. All invoices are accompanied by a detail of activity inclusive of Payment Date, Fees, Location, Last Name, UEID (Enrollment ID number), Service Date, & Authorization Code (unique one-time use code). Figure 21 shows an example of the billing details for all invoicing activity.



	Payment ReceivedDate	Fees	PaymentType	PaymentOrigin	locationName	locationId	Name_Last	ueid	serviceDate	Program	Service	Authorization Code	AccountName
1	2/26/2015	$ 30.00	CouponPayment	Workstation	Keyser	8016	Armstead	U1464F26QG	2/26/2015	WV	Enroll	1111113645517ZRYS	SAMPLECO
2	2/26/2015	$ 50.00	CouponPayment	Workstation	Charleston	9088	Qualls	U1ZJ4BZ7Z5	2/26/2015	WV	Enroll	11111136455128N91	SAMPLECO
3	2/26/2015	$ 50.00	CouponPayment	Workstation	Huntington	8289	James	U2RR4BZ564	2/26/2015	WV	Enroll	111111364551456K1	SAMPLECO
4	2/26/2015	$ 30.00	CouponPayment	Workstation	Martinsburg	9023	Haywood	U1T54BYSR1	2/26/2015	WV	Enroll	11111136455149KHZ	SAMPLECO
5	2/26/2015	$ 50.00	CouponPayment	Workstation	Sutton	1307	Willis	U3N24BYZX4	2/26/2015	WV	Enroll	11111136455511T2N4	SAMPLECO
6	2/26/2015	$ 50.00	CouponPayment	Workstation	Charleston	9088	Diaz	U1FF4BYNQY	2/26/2015	WV	Enroll	11111136455163F2F	SAMPLECO
7	2/26/2015	$ 30.00	CouponPayment	Workstation	Huntington	8289	Cooper	U2RR4BYVTB	2/26/2015	WV	Enroll	111111364551768 7B	SAMPLECO
8	2/26/2015	$ 30.00	CouponPayment	Workstation	Sutton	1307	Spears	U2T34BZ13R	2/26/2015	WV	Enroll	1111113645517NN27	SAMPLECO

Figure 21: Invoicing Activity Report

At no additional cost, MorphoTrust offers a billing account administration portal that allows billing account managers to establish accounts, distribute authorization codes via email, verify redemption status, and run reports for the purpose of reconciliation.

4.4.5.2 The Vendor should describe in detail their plan on providing and developing standard and ad-hoc reports for use in reconciliation and other program objectives. The plan should detail how the state and user agencies will access the reports. The Vendor will discuss the server for this database and provide screen shot of these reports:

Monthly/ Annual Summary

Monthly/ Annual Detail

Fee Collection/Billing Reconciliation (for State access only)

MorphoTrust leverages Microsoft's SQL Server Reporting Services (SSRS) for report generation and delivery services. The SSRS database server is deployed in a cluster, which allows for continuous operation when any one node in the cluster either fails or is taken offline for maintenance.

The network and reporting tools currently in use in West Virginia will continue to be in place upon contract award. Reports are based on information stored on the Transaction Control Processor, already in place today within the WVSP Data Center. Examples of current reports are included on the following pages.

Reports are available in real time to the State via a secure extranet reporting module. Approved contacts are provided a username and access to the secure module.

Authorized users can generate ad-hoc reports using a number of parameters, such as date range, applicant type, status, employer and name. All reports available through the extranet module can be viewed, printed or downloaded in a spreadsheet format. Reports are also available through daily emails for requesting agencies. Reports for applicants printed, transaction information, and status are delivered to the approved contacts by email.

Once our UEP solution is deployed, additional reporting capabilities will become available. UEP delivers reporting capabilities proven to successfully meet the needs of large state agencies and federal programs requiring applicant fingerprint services. These robust self-service reporting capabilities allow authorized state personnel to access reports as needed to understand their applicant activity.

The solution provides significant reporting flexibility, including:

- Multiple report formats, including XML, CSV, PDF, and XLS
- Ability to specify the desired reporting date range
- Ability to specify the agency(s) included in the report

Our standard reports include Operational Reports, Financial Reports, and Incident Support Reports. Details for each type of report follow:

Operational Reporting

Operational Reporting includes applicant volume statistics by agency as well as by location (Figure 24), with many operational reports available. Key operational reports include:

- ***Services By Location*** – shows the number of applicants processed by program as well as by location during the time period specified by the user
- ***Submissions*** – shows average time between print capture and submission to FBI as well as statistics on FBI fingerprint quality rejections by program
- ***Appointment Availability*** – shows, by location, the appointments available and the appointments already scheduled

Financial Reporting

Financial Reporting provides information about payment collection, refunds issued, and fund remittance. Key financial reports include:

- ***Payments*** – shows details (date, amount, program, location, payment method, etc.) of payments collected during the time period specified by the user
- ***Refunds*** – shows details, including reason, for all refunds processed within the time period specified by the user

Incident Support Reporting

Incident Support Reporting provides information about support tickets opened (by purpose or by agency) as well as average incident resolution time. Key support reports include:

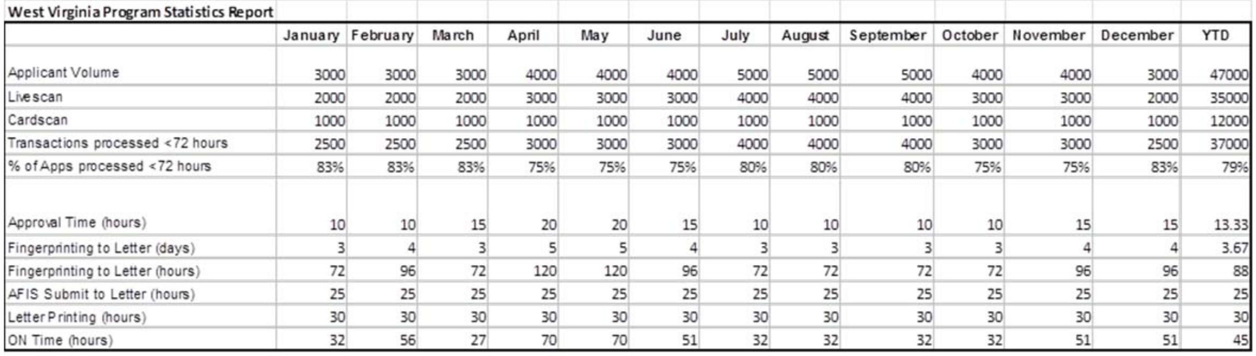
- ***Daily Status*** – shows several Key Performance Indicators (KPIs) used to ensure overall health of the solution and the quality of service being provided. KPIs include support issues by program, fingerprint rejection rates, appointment availability, etc.
- ***Ticketing Statistics*** – shows a count of tickets by program as well as average resolution times and the support inquiry purposes.

Report Examples

Figure 22 through Figure 28 show screen captures of Monthly/Annual Summary, Monthly/Annual Detail, and Fee Collection/Billing Reconciliation reports. The screen captures include:

- Sample reports from the current solution (Figure 22 and Figure 23), which will remain operational on contract award
- Samples of the reports available with the upgrade to UEP (Figure 24 through Figure 28)

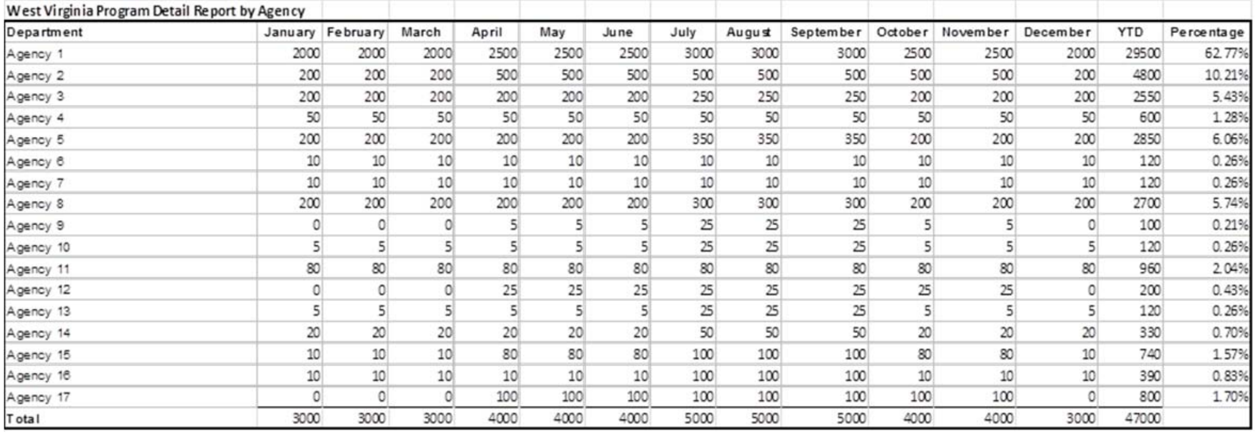
The screen captures were sanitized to remove applicant data.



West Virginia Program Statistics Report

	January	February	March	April	May	June	July	August	September	October	November	December	YTD
Applicant Volume	3000	3000	3000	4000	4000	4000	5000	5000	5000	4000	4000	3000	47000
Livescan	2000	2000	2000	3000	3000	3000	4000	4000	4000	3000	3000	2000	35000
Cardscan	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	12000
Transactions processed <72 hours	2500	2500	2500	3000	3000	3000	4000	4000	4000	3000	3000	2500	37000
% of Apps processed <72 hours	83%	83%	83%	75%	75%	75%	80%	80%	80%	75%	75%	83%	79%
Approval Time (hours)	10	10	15	20	20	15	10	10	10	10	15	15	13.33
Fingerprinting to Letter (days)	3	4	3	5	5	4	3	3	3	3	4	4	3.67
Fingerprinting to Letter (hours)	72	96	72	120	120	96	72	72	72	72	96	96	88
AFIS Submit to Letter (hours)	25	25	25	25	25	25	25	25	25	25	25	25	25
Letter Printing (hours)	30	30	30	30	30	30	30	30	30	30	30	30	30
ON Time (hours)	32	56	27	70	70	51	32	32	32	32	51	51	45

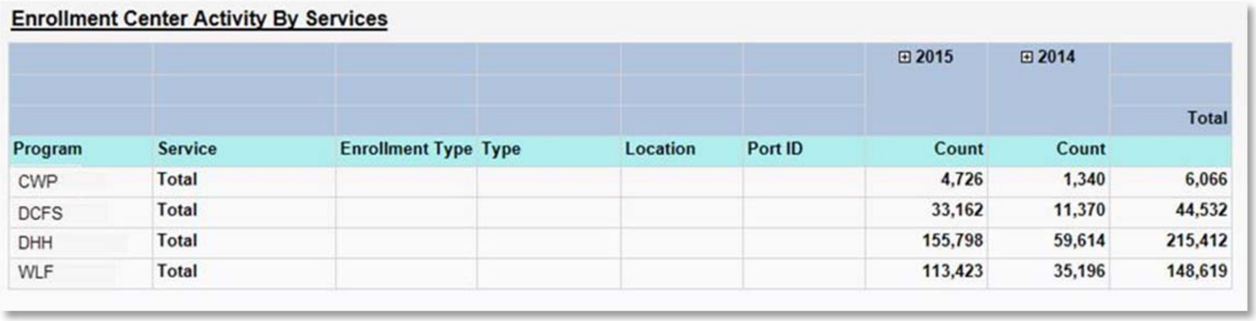
Figure 22: Monthly/Annual Summary Report (Current Solution)



West Virginia Program Detail Report by Agency

Department	January	February	March	April	May	June	July	August	September	October	November	December	YTD	Percentage
Agency 1	2000	2000	2000	2500	2500	2500	3000	3000	3000	2500	2500	2000	29500	62.77%
Agency 2	200	200	200	500	500	500	500	500	500	500	500	200	4800	10.21%
Agency 3	200	200	200	200	200	200	250	250	250	200	200	200	2550	5.43%
Agency 4	50	50	50	50	50	50	50	50	50	50	50	50	600	1.28%
Agency 5	200	200	200	200	200	200	350	350	350	200	200	200	2850	6.06%
Agency 6	10	10	10	10	10	10	10	10	10	10	10	10	120	0.26%
Agency 7	10	10	10	10	10	10	10	10	10	10	10	10	120	0.26%
Agency 8	200	200	200	200	200	200	300	300	300	200	200	200	2700	5.74%
Agency 9	0	0	0	5	5	5	25	25	25	5	5	0	100	0.21%
Agency 10	5	5	5	5	5	5	25	25	25	5	5	5	120	0.26%
Agency 11	80	80	80	80	80	80	80	80	80	80	80	80	960	2.04%
Agency 12	0	0	0	25	25	25	25	25	25	25	25	0	200	0.43%
Agency 13	5	5	5	5	5	5	25	25	25	5	5	5	120	0.26%
Agency 14	20	20	20	20	20	20	50	50	50	20	20	20	330	0.70%
Agency 15	10	10	10	80	80	80	100	100	100	80	80	10	740	1.57%
Agency 16	10	10	10	10	10	10	100	100	100	10	10	10	390	0.83%
Agency 17	0	0	0	100	100	100	100	100	100	100	100	0	800	1.70%
Total	3000	3000	3000	4000	4000	4000	5000	5000	5000	4000	4000	3000	47000	

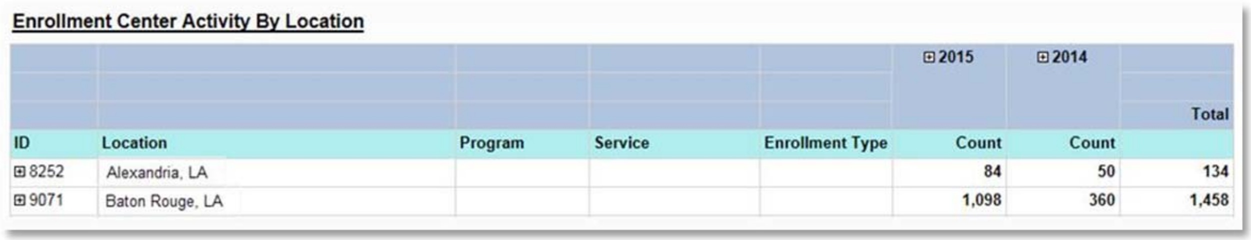
Figure 23: Monthly/Annual Detail Report (Current Solution)



Enrollment Center Activity By Services

						⊞ 2015	⊞ 2014	Total
Program	Service	Enrollment Type	Type	Location	Port ID	Count	Count	
CWP	Total					4,726	1,340	6,066
DCFS	Total					33,162	11,370	44,532
DHH	Total					155,798	59,614	215,412
WLF	Total					113,423	35,196	148,619

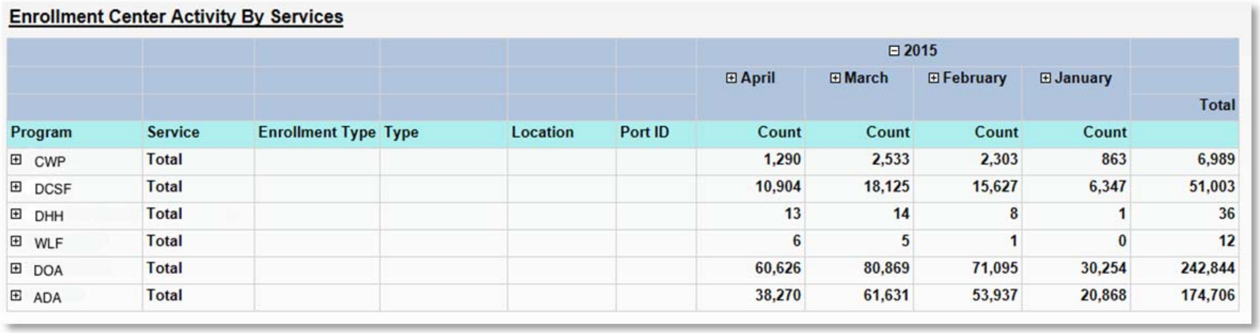
Figure 24: Annual Report of Enrollment Center Activity by Service (UEP Solution)



Enrollment Center Activity By Location

					⊞ 2015	⊞ 2014	Total
ID	Location	Program	Service	Enrollment Type	Count	Count	
⊞ 8252	Alexandria, LA				84	50	134
⊞ 9071	Baton Rouge, LA				1,098	360	1,458

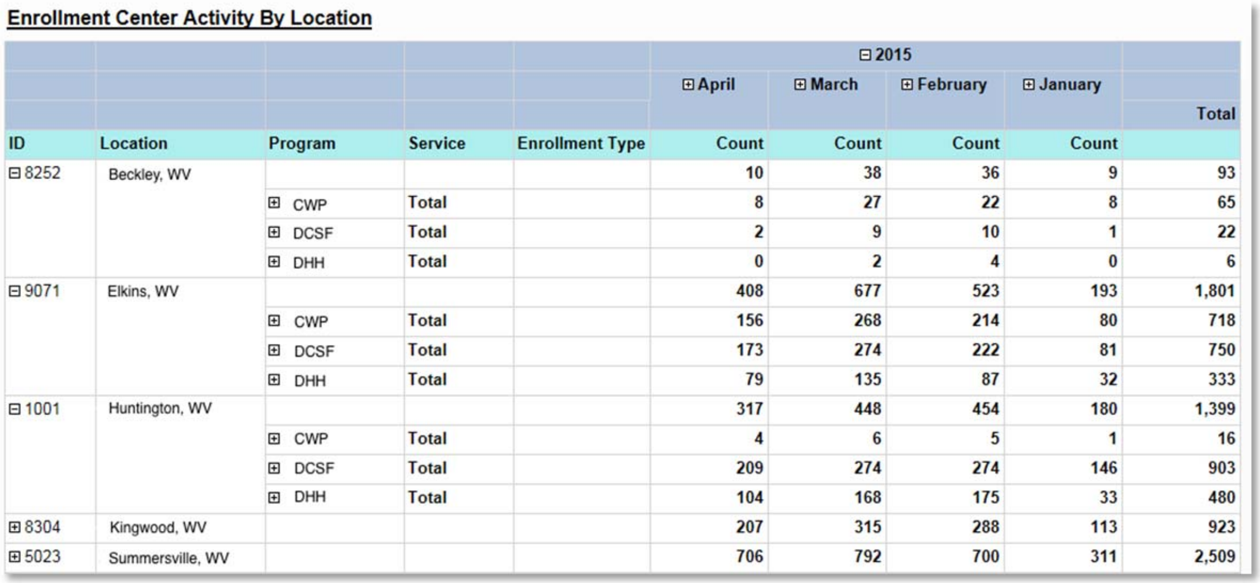
Figure 25: Annual Report of Enrollment Center Activity by Location (UEP Solution)



Enrollment Center Activity By Services

						⊟ 2015				
						⊞ April	⊞ March	⊞ February	⊞ January	Total
Program	Service	Enrollment Type	Type	Location	Port ID	Count	Count	Count	Count	
⊞ CWP	Total					1,290	2,533	2,303	863	6,989
⊞ DCSF	Total					10,904	18,125	15,627	6,347	51,003
⊞ DHH	Total					13	14	8	1	36
⊞ WLF	Total					6	5	1	0	12
⊞ DOA	Total					60,626	80,869	71,095	30,254	242,844
⊞ ADA	Total					38,270	61,631	53,937	20,868	174,706

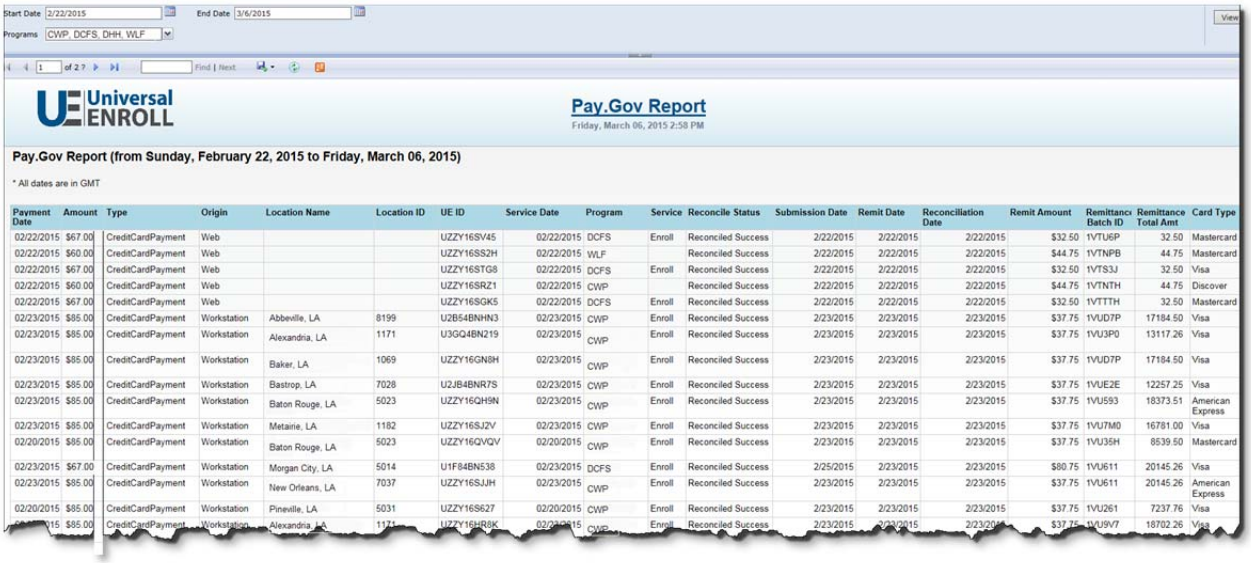
Figure 26: Monthly Report of Enrollment Center Activity by Service (UEP Solution)



Enrollment Center Activity By Location

					⊟ 2015				
					⊞ April	⊞ March	⊞ February	⊞ January	Total
ID	Location	Program	Service	Enrollment Type	Count	Count	Count	Count	
⊟ 8252	Beckley, WV				10	38	36	9	93
		⊞ CWP	Total		8	27	22	8	65
		⊞ DCSF	Total		2	9	10	1	22
		⊞ DHH	Total		0	2	4	0	6
⊟ 9071	Elkins, WV				408	677	523	193	1,801
		⊞ CWP	Total		156	268	214	80	718
		⊞ DCSF	Total		173	274	222	81	750
		⊞ DHH	Total		79	135	87	32	333
⊟ 1001	Huntington, WV				317	448	454	180	1,399
		⊞ CWP	Total		4	6	5	1	16
		⊞ DCSF	Total		209	274	274	146	903
		⊞ DHH	Total		104	168	175	33	480
⊞ 8304	Kingwood, WV				207	315	288	113	923
⊞ 5023	Summersville, WV				706	792	700	311	2,509

Figure 27: Monthly Report of Enrollment Center Activity by Location (UEP Solution)



Start Date 2/22/2015 End Date 3/6/2015

Programs CWP, DCFS, DHH, WLF

Pay.Gov Report

Friday, March 06, 2015 2:58 PM

Pay.Gov Report (from Sunday, February 22, 2015 to Friday, March 06, 2015)

* All dates are in GMT

Payment Date	Amount	Type	Origin	Location Name	Location ID	UE ID	Service Date	Program	Service	Reconcile Status	Submission Date	Remit Date	Reconciliation Date	Remit Amount	Remittance Batch ID	Remittance Total Amt	Card Type
02/22/2015	$67.00	CreditCardPayment	Web			UZZY16SV45	02/22/2015	DCFS	Enroll	Reconciled Success	2/22/2015	2/22/2015	2/22/2015	$32.50	1VTU6P	32.50	Mastercard
02/22/2015	$60.00	CreditCardPayment	Web			UZZY16SS2H	02/22/2015	WLF		Reconciled Success	2/22/2015	2/22/2015	2/22/2015	$44.75	1VTNPB	44.75	Mastercard
02/22/2015	$67.00	CreditCardPayment	Web			UZZY16STG8	02/22/2015	DCFS	Enroll	Reconciled Success	2/22/2015	2/22/2015	2/22/2015	$32.50	1VTS3J	32.50	Visa
02/22/2015	$60.00	CreditCardPayment	Web			UZZY16SRZ1	02/22/2015	CWP		Reconciled Success	2/22/2015	2/22/2015	2/22/2015	$44.75	1VTNTH	44.75	Discover
02/22/2015	$67.00	CreditCardPayment	Web			UZZY16SGK5	02/22/2015	DCFS	Enroll	Reconciled Success	2/22/2015	2/22/2015	2/22/2015	$32.50	1VTTTH	32.50	Mastercard
02/23/2015	$85.00	CreditCardPayment	Workstation	Abbeville, LA	8199	U2B54BNHN3	02/23/2015	CWP	Enroll	Reconciled Success	2/23/2015	2/23/2015	2/23/2015	$37.75	1VUD7P	17184.50	Visa
02/23/2015	$85.00	CreditCardPayment	Workstation	Alexandria, LA	1171	U3GQ4BN219	02/23/2015	CWP	Enroll	Reconciled Success	2/23/2015	2/23/2015	2/23/2015	$37.75	1VU3P0	13117.26	Visa
02/23/2015	$85.00	CreditCardPayment	Workstation	Baker, LA	1069	UZZY16GN8H	02/23/2015	CWP	Enroll	Reconciled Success	2/23/2015	2/23/2015	2/23/2015	$37.75	1VUD7P	17184.50	Visa
02/23/2015	$85.00	CreditCardPayment	Workstation	Bastrop, LA	7028	U2JB4BNR7S	02/23/2015	CWP	Enroll	Reconciled Success	2/23/2015	2/23/2015	2/23/2015	$37.75	1VUE2E	12257.25	Visa
02/23/2015	$85.00	CreditCardPayment	Workstation	Baton Rouge, LA	5023	UZZY16QH9N	02/23/2015	CWP	Enroll	Reconciled Success	2/23/2015	2/23/2015	2/23/2015	$37.75	1VU593	18373.51	American Express
02/23/2015	$85.00	CreditCardPayment	Workstation	Metairie, LA	1182	UZZY16SJ2V	02/23/2015	CWP	Enroll	Reconciled Success	2/23/2015	2/23/2015	2/23/2015	$37.75	1VU7M0	16781.00	Visa
02/20/2015	$85.00	CreditCardPayment	Workstation	Baton Rouge, LA	5023	UZZY16QVQV	02/20/2015	CWP	Enroll	Reconciled Success	2/23/2015	2/23/2015	2/23/2015	$37.75	1VU35H	8539.50	Mastercard
02/23/2015	$67.00	CreditCardPayment	Workstation	Morgan City, LA	5014	U1F84BN538	02/23/2015	DCFS	Enroll	Reconciled Success	2/25/2015	2/23/2015	2/23/2015	$80.75	1VU611	20145.26	Visa
02/23/2015	$85.00	CreditCardPayment	Workstation	New Orleans, LA	7037	UZZY16SJJH	02/23/2015	CWP	Enroll	Reconciled Success	2/23/2015	2/23/2015	2/23/2015	$37.75	1VU611	20145.26	American Express
02/20/2015	$85.00	CreditCardPayment	Workstation	Pineville, LA	5031	UZZY16S627	02/20/2015	CWP	Enroll	Reconciled Success	2/23/2015	2/23/2015	2/23/2015	$37.75	1VU261	7237.76	Visa
[illegible]15	$85.00	CreditCardPayment	Workstation	Alexandria, LA	1171	UZZY16HR8K	02/23/2015	CWP	Enroll	Reconciled Success	2/23/2015	2/23/2015	2/23/20	$37.75	1VU9V7	18702.26	Visa

Figure 28: Sample Report for Fee Collection and Billing Reconciliation (UEP Solution)

4.4.6 Equipment

4.4.6.1 The Vendor should describe in detail how they will capture Applicant fingerprints digitally. Included in the plan, the Vendor should discuss the Livescan device, ID Authentication plan, the manual fingerprint process, digital signatures, central server/store and forward configuration, and card scan conversions process.

As the current provider of the West Virginia fingerprinting network, MorphoTrust will continue to operate all current and expanded sites with all hardware, software, and processes remaining the same. This will ensure zero risk to the network at contract start, allowing for services to continue for the residents of West Virginia while the network is prepared for update. The update to the Universal Enrollment Platform will be a collaborative effort by MorphoTrust with the West Virginia State Police.

Digital Fingerprint Capture

Both our current software solution and proposed UEP workstation software are workflow-driven applications that walk the Enrollment Agent and the applicant through the fingerprint collection process. The workstation software automatically calculates the quality of fingerprint captures, giving real-time feedback to the Enrollment Agent and helping to eliminate rejects due to image quality issues.

Fingerprint scanners are calibrated daily, as a part of the overall maintenance of the equipment. In addition, our workstation software automatically detects dirt, residual oils, and other platen imperfections that would require cleaning and recalibration of the scanner.

Our workstation solution also provides automatic, real-time sequence checking (Figure 29) that verifies that the same hand was not scanned twice and compares the 10 rolled fingerprint images to the four-finger slap and the flat thumb images, using minutiae matching to verify the images are captured and stored correctly. This helps prevent any further processing of inaccurate image data based on finger numbering, such as omitting or inadvertently substituting a fingerprint.

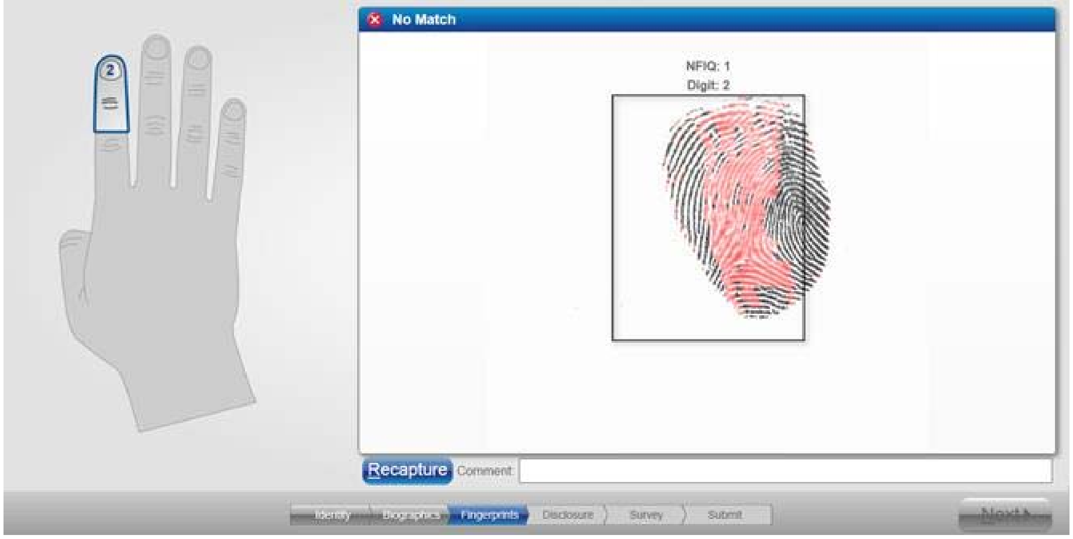


Figure 29: UEP Workstation Fingerprint Error Detection

During the ten-print capture workflow, each fingerprint is captured twice—once as a rolled print and once as a flat print. The workstation automatically detects when the rolled fingerprint does not match the corresponding flat fingerprint and directs the Enrollment Agent to correct the mistake.

Livescan Systems

At the start of the contract, MorphoTrust will continue to utilize our TouchPrint™ 5100 (TP-5100) system for the West Virginia network. ***Please see Appendix E for our FBI letter stating that the TP-5100 is FBI Appendix F certified for type 14 prints at 1000 dpi.***

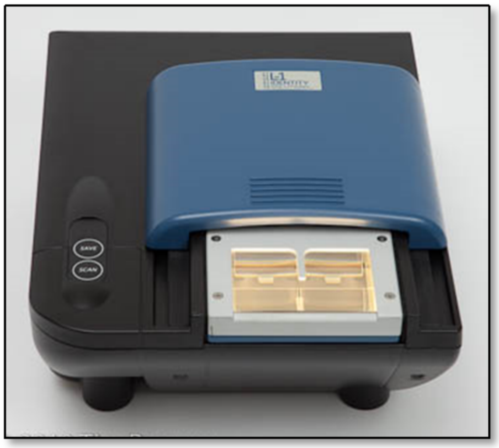


Figure 30: TP-5100 Livescan System

The TP-5100 (Figure 30) provides the image clarity needed to prevent artifacts and capture important friction ridge detail. The high dynamic range sensor results in maximum contrast and gray scales, bringing out the minutiae and pore detail in the fingerprint image with virtually no distortion, which makes the image ideal for latent print comparison.

The patented optics ignores moisture, dirt and latent prints left behind on the platen, making it easier to capture high quality images – consistently – regardless of the challenges faced, such as dry or sweaty fingers or an unclean platen.

The TP-5100 is a completely sealed unit, making it impervious to dust and dirt. It contains a single, large non-coated platen and no moving parts. With fewer parts to break and no need to replace platen coatings, the scanner is less costly to maintain and more reliable than other Livescans.

For the proposed updated UEP solution, both our TP-4100 (Figure 31) and our TP-5300 (Figure 32) Livescan systems capture standard ten print fingerprint roll and four (4) slap images. Both are of sturdy construction, and intuitive operations make them a sound choice for high volume fingerprint capture use.

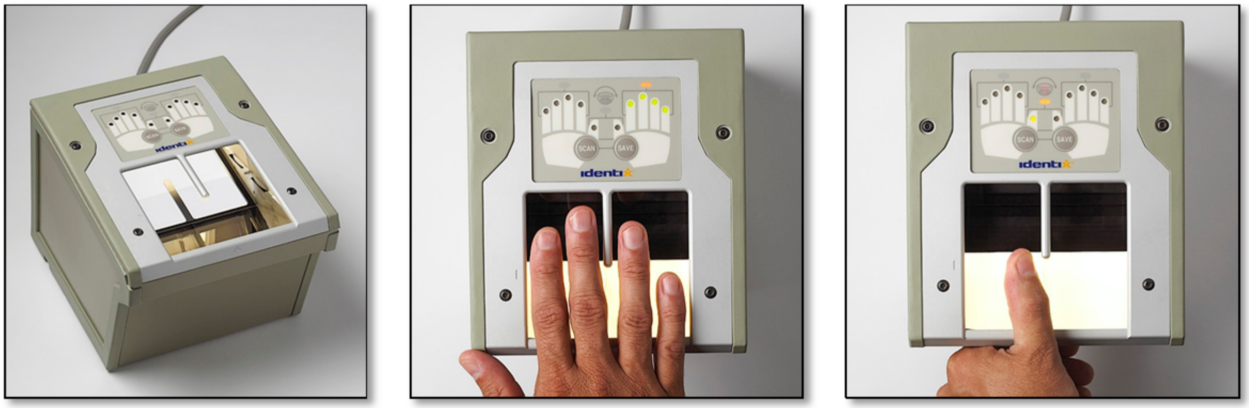


Figure 31: TP-4100 Livescan System

Both devices are certified by the FBI as tested and in compliance with the FBI's Next Generation Identification (NGI) initiatives and IAFIS Image Quality Specifications (IQS). The review of the test data was conducted by the FBI Criminal Justice Information Services Division, Biometric Services Section, as part of Biometric Center of Excellence. The Livescan system fully supports the EBTS standard.

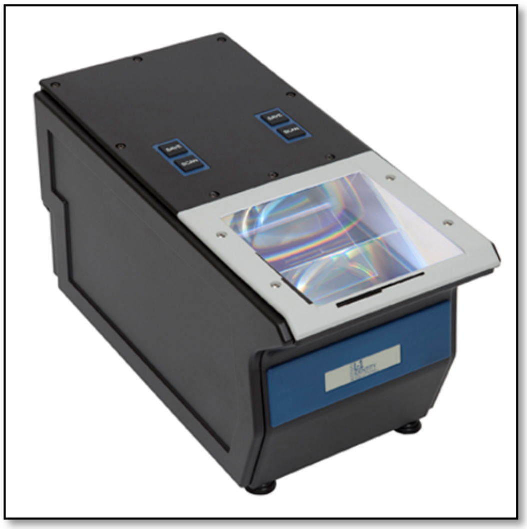


Figure 32: TP-5300 Livescan System

Please see Appendix E for our FBI letters stating that the TP-4100 is FBI Appendix F certified for type 14 prints at 500 dpi and the TP-5300 is FBI Appendix F certified for type 14 prints at 500 and 1000 dpi.

The TP-4100 device captures prints at a resolution 500 dpi and is the standard device used on the Universal Enrollment Platform.

The TP-5300 device captures prints at 1000 dpi and is offered for compliance with the 1000 dpi requirements of the RFP.

MorphoTrust will comply with the 1000 dpi requirement, either through use of the current TP-5100 system or the proposed TP-5300 system. However, we encourage WVSP to consider the TP-4100 device and accept 500 dpi fingerprints as new, cutting-edge fingerprint scanners are often first available in 500 dpi resolution. MorphoTrust is actively evaluating new fingerprint capture devices that require less cleaning, capture better ridge detail, and capture prints faster. However, we cannot make these devices available in West Virginia if 1000 dpi resolution is required.

Authentication of Identification Credentials

For the current solution, the Enrollment Agent reviews each applicant's valid photo identification prior to the fingerprinting session. In accordance with state guidelines, the Enrollment Agent ascertains to the best extent possible that the person is being fingerprinted for the purpose intended and is the person shown on the ID. Acceptable forms of personal identification must be current and valid and will include driver licenses issued by any state, passport, military ID, and photo identification card issued by a municipality, county or state in lieu of a driver's license.

With our UEP solution, the workstation software displays the list of acceptable identification documents to the Enrollment Agent. While this list can be configured specifically for West Virginia requirements, we recommend accepting only photo IDs issued by a state, United States territory, or the federal government.

When presented with an identification document, the Enrollment Agent will do their best to determine if the document is authentic and that the photo reasonably matches the applicant. MorphoTrust's Enrollment Agent training program includes a dedicated section that details how to determine that the offered ID is genuine and valid. Our Enrollment Agents will also use the document to verify the biographic data provided during enrollment.

As an added security feature, MorphoTrust proposes our Identity Proofing Solution, which leverages our industry-leading iA-thenticate® authentication software and B5000 Document Reader. The B5000, shown in Figure 33, will analyze state and federal government-issued photo identification documents including driver licenses, government-issued ID cards, military IDs, or Passports.

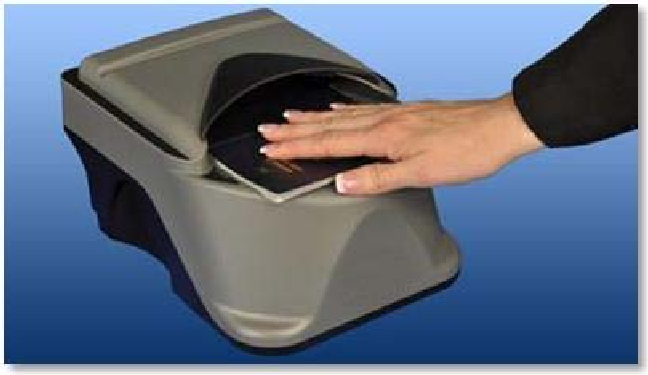


Figure 33: MorphoTrust B5000 Document Authentication Reader

Enrollment Agents will use the B5000 to examine state or federal government-issued photo IDs before capturing an applicant's fingerprints. The B5000 is certified under the SAFETY Act by the U.S. Department of Homeland Security.

The Enrollment Agent will scan the document utilizing the B5000 Document Reader. Our Identity Proofing Solution knows which document it is expecting and will alert the Enrollment Agent if the document authenticated is not the correct document. If the document is the expected document, then diagnostics will be run against it ensuring it is valid.

With the B5000, the Enrollment Agent lays the identification document on the scanner platen. If the ID is a driver's license, the Enrollment Agent will insert the license into the reader and then lay it on the platen to scan it. If the document is dual-sided, the system will ask the Enrollment Agent to scan the opposite side.

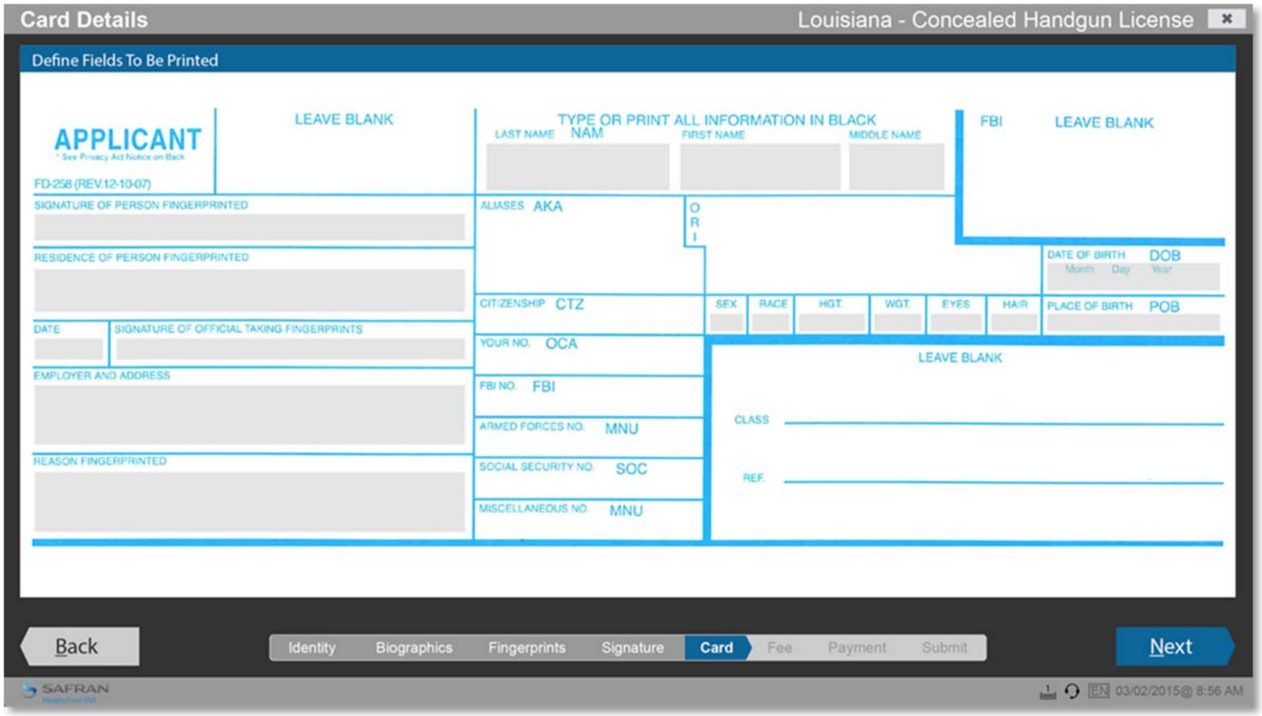
Once the B5000 scans the document and performs the authentication process, the software provides the Enrollment Agent with a status or requests further clarifying information. For instance, if the document is dirty, the software asks the Enrollment Agent if they are able to visually identify a specific piece of information in a specific location of the document and provide a diagram of where the information should be printed. If the information is found, the Enrollment Agent confirms and the process continues.

If the iA-thenticate device identifies a discrepancy, the Enrollment Agent is notified not to accept the document and the Enrollment Agent will follow the State of West Virginia's protocols regarding un-authenticated identification documents. MorphoTrust will not fingerprint an applicant who is unable to provide the required valid ID documents.

Our UEP Livescan software will be configured to require that a valid identity document is verified by the B5000 before allowing the record to be submitted from the Enrollment Workstation to our Central Server. In addition, the data from the authentication event will be embedded into the applicant record so the verification event details will persist for the life of the transaction.

Manual Fingerprint Process

In the current solution as well as the proposed UEP solution, MorphoTrust offers a universal "Print and Go" capability that allows any applicant to have a physical FD-258 hard card produced from their fingerprints that were collected electronically on our Livescan systems. All applicant data and fingerprints are captured using the same software interfaces used for records that are submitted electronically. However, a FD-258 hard card (Figure 34) is produced instead of the electronic record, for the applicant to take with them from the Enrollment Center.



APPLICANT
* See Privacy Act Notice on Back
FD-258 (REV.12-10-07)
LEAVE BLANK
TYPE OR PRINT ALL INFORMATION IN BLACK
LAST NAME NAM
FIRST NAME
MIDDLE NAME
FBI
LEAVE BLANK
SIGNATURE OF PERSON FINGERPRINTED
ALIASES AKA
ORI
RESIDENCE OF PERSON FINGERPRINTED
DATE OF BIRTH DOB
Month Day Year
DATE
SIGNATURE OF OFFICIAL TAKING FINGERPRINTS
CITIZENSHIP CTZ
SEX
RACE
HGT.
WGT.
EYES
HAIR
PLACE OF BIRTH POB
YOUR NO. OCA
LEAVE BLANK
EMPLOYER AND ADDRESS
FBI NO. FBI
CLASS
ARMED FORCES NO. MNU
REASON FINGERPRINTED
SOCIAL SECURITY NO. SOC
REF.
MISCELLANEOUS NO. MNU

Figure 34: FD-258 Fingerprint Hard Card

The hard card is printed using a Lexmark MS810n or T600 series printer (Figure 35). These printers have printed thousands of hard cards while deployed in West Virginia and other states.

Figure 35: Lexmark Printer

Lexmark printers have printed thousands of hard cards in West Virginia and other states.

Figure 36: Topaz Signature Capture Pad

Topaz signature pad has been used within the Universal Enrollment Platform for more than 3.5 million applicants.

Digital Signatures

Both the current and proposed UEP solutions offer the ability for applicant digital signatures. After an applicant provides their demographic data and the fingerprints are captured, the enrollment workstation requires the applicant to attest that the information they have provided is true and accurate. The applicant acknowledges the data is true and accurate by signing on a Topaz electronic signature pad (Figure 36).

Signatures are submitted in the Type 8 record of the NIST record. The Topaz signature pad has been used within the Universal Enrollment Platform for more than 3.5 million applicants.

Cardscan Conversion

Hard cards may be mailed to MorphoTrust's central facility where we will digitize them and submit them to the State AFIS just like a Livescan submission. Figure 37 illustrates the Cardscan conversion process.

Our proven centralized Cardscan Center converts and digitally submits more than 100,000 paper fingerprint cards annually in support of numerous statewide networks as well as FBI Channels.

Our card scanning service employs commercial off-the-shelf (COTS) Card Scanning Workstations, which are FBI-certified to the IAFIS IQS Appendix F Scanner Requirements.

To improve the tracking and payment management for Cardscan submissions, MorphoTrust requires pre-enrollment for all Cardscan submissions. During pre-enrollment, applicants are required to pay fees, which are non-refundable. A printed copy of the applicant's pre-enrollment must be mailed with the Cardscan submission.

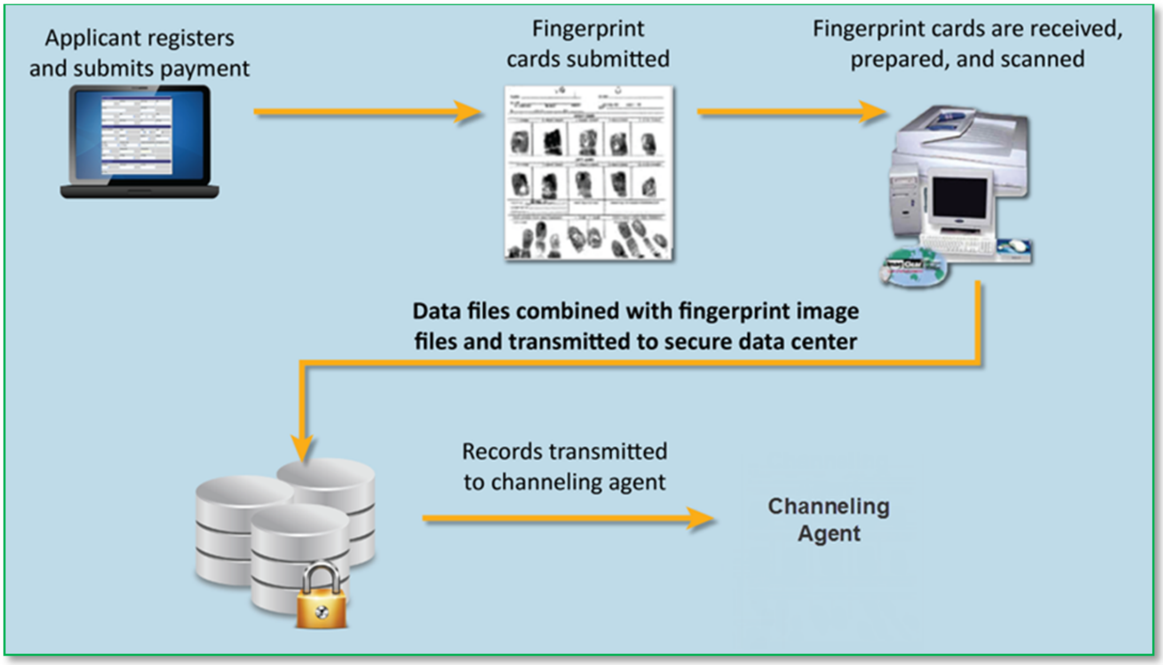

Applicant registers and submits payment
Fingerprint cards submitted
Fingerprint cards are received, prepared, and scanned
Data files combined with fingerprint image files and transmitted to secure data center
Records transmitted to channeling agent
Channeling Agent

Figure 37: Cardscan Conversion Process

Paper fingerprint cards are converted and digitally submitted from our centralized Cardscan Center.

The steps in the fingerprint Card Scan conversion process are as follows:

1. ***Applicant Pre-Enrolls and Submits Payment*** – The applicant registers with MorphoTrust using either our secure website or Call Center and pays for the transaction. Because personal information is collected securely, the applicant needs to enter only their full name, the Registration ID provided at the end of the registration process, and payment confirmation number when submitting the fingerprint card to MorphoTrust. This process limits the amount of personal information being sent by mail. The applicant is provided instructions for submitting fingerprint cards to the MorphoTrust Processing Center.

2. ***Fingerprint Cards Received*** – We receive FBI (FD-258) fingerprint cards from applicants in accordance with instructions provided to applicants at time of registration.

3. ***Fingerprint Cards Reviewed and Prepared*** – A MorphoTrust staff member opens each package, applies a barcode label to each card, reviews the card for completeness and legibility of demographic data, and logs the record in. If the applicant has not completed the registration process but has provided

contact information, the applicant is contacted and assisted with the registration and payment process, and the card is put back into the processing queue. If no contact information is provided, the cards are returned to the applicant with instructions on how to complete the registration/payment process. The applicant will complete the process and re-submit the cards to MorphoTrust.

4. ***Cards Scanned*** - The Cardscan Technician scans the cards in batches and then combines the images with the correct registration entry. MorphoTrust software automatically converts the fingerprint card to a digital image in preparation to building the NIST file for submission to the WVSP AFIS.
5. ***Records submitted*** – The data files are combined with the fingerprint images and transmitted to our secure Data Center.
6. ***Transmission to Channeling Agent*** – Records are transmitted to WVSP AFIS in accordance with specifications.

Central Server/Store and Forward Configuration

Upon contract award, MorphoTrust will continue to operate the existing central servers and submission channels in place today. Ours is the only no-risk solution available that will allow continued transmissions and uninterrupted service to applicants through the transition to the new contract. Testing and deploying the current system will provide additional experience with the current AFIS so we are well-prepared for the upgrade to UEP.

MorphoTrust's UEP system consists of four major software components and the hardware that hosts them. One of the software components, the "workstation," exists at the Enrollment Center site; the other three are hosted on servers at our UEP Data Center. These components include a public web portal, an application server, and an administrative web portal.

Our secure Data Center currently submits approximately five million fingerprint records per year to more than 20 state AFIS systems, including 11 MorphoTrak AFIS systems. We are certified FBI Channeler.

4.4.7 Project Management

4.4.7.1 The Vendor will be required to utilize a formalized approach to project management.

MorphoTrust fully understands the level of effort required to deliver and operate the West Virginia program. Implementing the State's defined needs requires a thorough understanding of the basic processes for scheduling and fingerprinting applicants as well as the peripheral support required to ensure success. The technical solution requires compliance with West Virginia State Police requirements for the electronic acquisition, transmission, and storage of fingerprint images and associated demographic data.

Responsibility for MorphoTrust's contract administration and project management plan resides with the Program Manager, Denny Wear. Mr. Wear is empowered to make decisions and commitments on behalf of MorphoTrust and communicate those decisions and commitments to the designated representative of the state of West Virginia. He is responsible for the project management and tracking the progress of each defined task, maintaining the project schedule, identifying any potential problem areas or risks, and communicating all of the activity status with the State’s Contract Manager and Agency Program Managers.

The project management follows the Project Management Institute (PMI®) industry standard process groups of Initiation, Planning, Execution, Monitoring and Control, and Closing.

MorphoTrust utilizes a baseline set of project management software tools that are familiar to our customers. Microsoft Office 2010 and its suite of applications are the standard means of monitoring, controlling, tracking and communication of project tasks and deployments. Microsoft Word, Visio, Outlook, Excel, PowerPoint, and Project are the tools of choice. Any documents or deliverables shared with the state of West Virginia can be converted to Microsoft Office 2007 or PDF files where needed.

We have provided additional information about our Project Plan in our response to requirement 4.5.9 (b) and a preliminary project schedule in Appendix B.

4.4.7.2 The Vendor should describe in detail the plan on how status updates will be provided on the overall progression of the project at each phase of development.

Lowest-Risk Transition to Improved Fingerprinting Services for West Virginia Applicants

MorphoTrust will use existing infrastructure, current key processes, and existing project staff in West Virginia for the program.

We are in the best position of any vendor to accomplish all implementation tasks without an interruption in services.

MorphoTrust realizes that the best planning is based on effective communications. With this in mind, our Program Manager will continue to be the primary point-of-contact from contract negotiations through the life of the program. He will maintain regular communications with West Virginia’s designated counterpart, ranging from routine in-person and telephone contact to regularly scheduled status meetings and other communication.

The Program Manager will present a Preliminary Project Plan at the initial kick-off meeting. We follow a structured procedure for the review and updating of the Program Management Plan. To ensure success, a complete Work Breakdown Structure (WBS) for the Contract Management will be presented to and signed-off by West Virginia. This WBS defines the deliverables dates for all components and tasks, providing a step-by-step process to move from contract award to the implementation of Full Operational Capability (FOC).

Shortly after contract award, MorphoTrust will initiate the Universal Enrollment Platform (UEP) implementation project by piloting the UEP solution in an Enrollment Center. The purpose of the pilot will be to test the integration between UEP and the state’s systems and to gather feedback on the enrollment process from West Virginia State Police and related agencies. This pilot approach will allow us to quickly discover any changes to the existing process, while making the project real and concrete for all stakeholders, including the many agencies.

During this pilot phase, we will also establish and test our ongoing project communication plan. We will hold regular project status meetings and establish project tracking artifacts such as issue-tracking lists.

MorphoTrust will adapt our approach based on any lessons learned during the pilot phase, and apply those learnings to subsequent phases.

Development Timeline and Rollout Plan

Since MorphoTrust currently operates the existing West Virginia applicant-processing network, we will approach the new functionality required in this RFP incrementally, while not disrupting current operational activities.

With a phased approach, we can deliver value quickly, demonstrate new capabilities within weeks of being awarded this contract, roll out additional features each month until full operational compliance is met, adapt to stakeholder feedback, and minimize operational risk to applicants.

As such, MorphoTrust will roll out the UEP functionality in phases. During each phase, we will completely develop, test, deploy, and begin to utilize a new set of functionality. MorphoTrust will not move onto a new phase until all requirements have been successfully delivered in the current phase.

A description of each phase and the work to be completed in each phase is listed in Appendix B, along with tentative timelines.

4.4.8 Maintenance

4.4.8.1 The Vendor should describe in detail the maintenance levels that will be provided for each of the elements of the network, including how the State would request maintenance and what the Vendor will do to mitigate disruption of service to the Applicant.

Levels of Maintenance

MorphoTrust addresses maintenance of all systems at several levels: Enrollment Agent, Technical Help Desk, and Field Service Engineering. Most maintenance requests are initiated through a call to our toll free Customer Service Center, and may be escalated according to the Escalation Procedure described in our response to requirement 4.4.8.3.

All Enrollment Agents are trained in basic maintenance and troubleshooting techniques for the systems. The perform daily maintenance functions such as calibrating the scanners and ensuring the platen is cleaned and surge protectors are used on the systems at all times. For systems that are transported, Enrollment Agents use a specially manufactured heavy duty Pelican case, which provides a protected environment for both the scanner and accompanying laptop computer.

MorphoTrust is qualified to provide all maintenance for our Enrollment Workstations without subcontracting with the manufacturer, therefore if the Enrollment Agent encounters a problem they are unable to troubleshoot, our Technical Help Desk is contacted. This Technical Help Desk employs trained, experienced technicians that provide technical support for Enrollment Agents in the field as well as support for state agencies for issues such as web-based scheduling support, server issues, fingerprint transmissions, etc. We provide the same high level of maintenance in support of each of our existing statewide networks. A toll-free phone number is provided for customer operational support.

In addition to the Technical Help Desk staff, MorphoTrust employs a team of certified Field Service Engineers (FSEs) to support and maintain our equipment. The FSEs have the ability to access each system with secure remote access to perform an array of diagnostic tests. Based on the remote diagnostic results, the FSE will walk the Enrollment Agent through the steps required to correct the error.

If a service visit is required, an FSE will be dispatched to the location to field-service the device. FSEs carry spare units to swap for disabled equipment if field-repair cannot be completed within an acceptable timeframe. In addition to servicing the device, FSEs ensure that all mission-critical equipment at the location is fully operational prior to their departure.

Approximately 80% of trouble tickets are resolved in under half an hour. The maximum time for fingerprinting center outage would entail the delivery of a replacement scanner or computer no later than start of business the next business day. Maximum outage applies to less than 1% of trouble tickets.

MorphoTrust has monitoring software in place that continually monitors the availability of all switches, VPN connections, servers, and firewalls. This monitoring software will notify the appropriate person via email and page and the issue will be addressed immediately. All network components are kept on a current vendor support contract, each support contract requiring same day response.

When issues arise that require additional assistance, our technical team is available 24x7 to provide necessary support. MorphoTrust will maintain an ample quantity of spare parts and systems to ensure rapid replacement when necessary.

Minimal Disruption to Applicants

We minimize disruption to customers, both state users and applicants, by planning maintenance to ensure downtime windows are as small as possible, by providing visibility into the planned maintenance schedule, and by robustly communicating when emergency maintenance or system failures occur. Key aspects of our maintenance policies include:

- ***Planned maintenance*** – Security patches, operating system updates, software updates, and other maintenance tasks are performed once a month during low-volume activity periods. Fingerprint device calibration occurs daily.
- ***Unscheduled outages*** – When these occur, all stakeholders are notified as soon as the outage has been confirmed and updates are provided at a minimum of once every two hours if the outage is system-wide.
- ***Redundancy*** – Critical systems, such as database systems, are deployed in clustered pairs allowing one server to be patched while the other continues to provide services. Using this failover strategy, most critical systems can be patched without any service disruption.

MorphoTrust attempts to provide advanced notification to all stakeholders in the event of an emergency, unplanned outage and defers non-emergency maintenance until the next planned maintenance window.

All network components are kept on a current vendor support contract, each support contract requiring same day response. Routine monthly patching also occurs to ensure software operating system updates are applied to both the workstations in the field and the central server technology stack.

4.4.8.2 The Vendor should describe in detail the expected response time for maintenance for each element of the services infrastructure, i.e. livescan failure, server downtime, web site disruption of service, etc.

MorphoTrust's uptime for Universal Enrollment was 99.3% in 2014.

Table 13 summarizes the expected maintenance response activities and duration for our current solution and UEP.

Table 13: Maintenance Response Times

Infrastructure Element	Action	Response Time	Impact
Live Scan Failure	Enrollment Agent conducts onsite troubleshooting	5-15 minutes	Wait time
	Field Service Engineer dials in to perform further troubleshooting	5 min-1 hour	Wait time or reschedule appointment
	Equipment is replaced	Next day start of business	Reschedule appointment - affected applicants contacted to reschedule
Server Downtime	Immediate trouble ticket issued and resources released to address issue as Top Priority	5-15 minutes	No disruption to enrollment customers – records queued on Livescan for submission when lines are re-established
Website disruption of service	Immediate trouble ticket issued and resources released to address issue as Top Priority	5-15 minutes	Applicants cannot pre-register online, but Enrollment Centers are operational on a walk-in basis and the Customer Service Center is available to provide directions to Enrollment Centers and answer questions
Communication lines disruption of service	Immediate trouble ticket issued and resources released to address issue as Top Priority	5-15 minutes	No disruption to customers – records queued on Livescan for submission when lines are re-established

Workstations

Our workstations are designed to work in offline mode, so they continue to function in the event of a server outage. When services to the Data Center are restored, the data from the workstations is uploaded to the Data Center and processing will resume.

MorphoTrust is qualified to provide all maintenance for our Enrollment Workstations without subcontracting with the manufacturer, therefore if the Enrollment Agent encounters a problem they are unable to troubleshoot, our Technical Help Desk is contacted. The Technical Help Desk employs trained, technicians that provide technical support for Enrollment Agents in Enrollment

Centers. A Tech Help Desk agent has the ability to access each system with secure remote access to perform an array of diagnostic tests to troubleshoot technical problems. Based on the remote diagnostic results, the agent will walk the Enrollment Agent through the steps required to correct the error.

If replacement equipment is required, the agent will order a replacement device shipped out to the site as soon as possible (typically next-day air), and a trained person will install the new device. The Technical Help Desk is available to our Enrollment Centers as a toll-free phone number. MorphoTrust also maintains critical spares in select high volume locations to ensure operational downtime is minimized should a critical device fail like the CPU or the fingerprint scanner.

Server Outages

To ensure system uptime, MorphoTrust has monitoring software in place that continually monitors the availability of all major networking components under the control of MorphoTrust such as switches, VPN connections, servers, and firewalls. This monitoring software will notify the appropriate person the issue will be addressed immediately.

When issues arise that require additional assistance, our technical team is available 24x7 to provide necessary support.

Any server outage is considered critical and receives an immediate response and active troubleshooting until resolved

4.4.8.3 The Vendor should describe in detail the call escalation procedure with the name, title, area of responsibility and phone number for each level starting with the state program manager up to the top official in the company.

All significant issues should be reported directly to the Program Manager, Denny Wear. Mr. Wear's contact information is:

Denny Wear
Director – Program Management
Office phone: (217) 547-2116
Cell phone: (615) 946-7947
dwear@morphotrust.com

In the unlikely event that a problem must be escalated, it should be reported to Mr. Wear's supervisor, Kent Schmitt. Mr. Schmitt's contact information is:

Kent Schmitt
Program Executive
Office Phone: (202) 688-4826
Cell Phone: (615) 347-4627

kschmitt@morphoTrust.com

In the unlikely event that a problem must be escalated, it should be reported to Mr. Schmitt's supervisor, Charles Carroll. Mr. Carroll's contact information is:

Charles Carroll
Senior Vice-President
Office Phone: (615) 778-5752
Cell Phone: (937) 604-6595
ccarroll@morphoTrust.com

Issue Escalation

Most day-to-day operational issues would typically be escalated in the following manner:

- ***Step One*** – Most problems should be reported to our toll free Customer Service Center which will be open 7:00 A.M - 4:00 P.M. CST Monday through Friday. All Customer Service Representatives assigned to this program will have a thorough knowledge of the program.
- ***Step Two*** - Problems that cannot be solved or addressed by a Customer Service Representative are forwarded to the West Virginia Customer Service Supervisor or our Technical Support Center for resolution.
- ***Step Three*** – Problems that cannot be solved or addressed by the Customer Service Supervisor or Technical Support will be forwarded to the Operations Manager.
- ***Step Four*** – If a problem cannot be solved by the Operations Manager, the issue will be escalated to the Project Manager, Denny Wear. Mr. Wear's contact information is included above.
- ***Step Five*** - In the unlikely event that a problem must be escalated above the Project Manager level, the Program Executive, Kent Schmitt, should be contacted. Mr. Schmitt's contact information is included above.
- ***Step Six*** - In the unlikely event that a problem must be escalated above the Program Executive level, the Senior Vice-President, Charles Carroll, should be contacted. Mr. Carroll's contact information is included above.

This page intentionally left blank.

Mandatory Specification Checklist (Attachment B)

By signing and dating Attachment B: Mandatory Specification Checklist, MorphoTrust acknowledges that we meet or exceed each of these specifications as outlined in 4.5 of Section Four: Project Specifications.

Authorized Signature:

Robert Eckel
CEO and President

May 11, 2015

Date

Section 4, Subsection 4.5: Mandatory Requirements

4.5 The following mandatory requirements must be met by the Vendor as a part of the submitted proposal. Failure on the part of the Vendor to meet any of the mandatory specifications shall result in the disqualification of the proposal. The terms "must", "will", "shall", "minimum", maximum", or "is/are required" identify a mandatory item or factor. Decisions regarding compliance with any mandatory requirements shall be at the sole discretion of the Purchasing Division.

MorphoTrust meets all requirements in Subsection 4.5 – *Mandatory Requirements.* Where applicable, we have provided additional detail describing how our solution meets the requirement.

Our Applicant Fingerprinting Services solution is already in place in West Virginia, allowing us to be up and running within weeks of contract award with a system that meets all mandatory requirements of the RFP. Our response details how we will tailor our existing infrastructure and proven processes to

deliver new capabilities while providing continuous service to the residents of West Virginia.

Furthermore, we propose a no-risk upgrade our advanced technology Universal Enrollment Platform (UEP) during the first year of the contract. Our response details how UEP meets all mandatory requirements of the RFP while offering many benefits for West Virginia agencies and applicants.

4.5.1 Customer Service Center

The Vendor must provide a customer service center to serve as a single point of contact for all Applicant needs. The service center must have the following capabilities:

a) Call Center

Vendor must provide a toll-free phone number for Applicants and/or agencies to schedule, change or cancel appointments, provide demographic data, pay fees, request information and track their transaction. The call center must be physically present within the continental United States and be available from 9am to 5pm local time, Monday through Friday. The Vendor must provide live operators to assist Applicants with appointment scheduling and other program questions as needed.

The Vendor must provide contact information for its current call center so that the State can verify its existence and test its performance.

The Vendor must provide statistics on the number of calls accepted by its call center annually.

MorphoTrust meets the requirements.

We operate a centralized, scalable Customer Service Center (CSC), which currently serves the State of West Virginia and other statewide networks. The CSC accepts over two million calls per year, including 50,000 calls from West Virginia citizens. We welcome the State to verify its existence and test its performance by calling the toll free number at 855-766-7746.

The CSC offers an uninterrupted, proven single point of contact to speak with a live operator. Our Customer Service Representatives (CSR) will assist the applicant to provide demographic information to complete their registration; schedule, change, or cancel) an appointment; process payment; and ask questions about the process. West Virginia applicants and agencies will be able to access the CSC conveniently from anywhere in the United States via a single, toll-free, program-specific telephone number.

Our knowledgeable, experienced, and multi-lingual staff is available Monday through Friday, 7:00 A.M. – 4:00 P.M. Central Standard Time (9:00 A.M. to 5:00 P.M. West Virginia local time). The CSC currently employs more than 150 CSRs including an established team of CSRs who currently serve the needs of West Virginia applicants. In addition to the CSRs who are dedicated to this project, all CSRs are cross-trained so that they can be utilized during peak periods if needed.

Housed in multiple U.S. cities (specifically Springfield, IL and Des Moines, IA) to minimize outages due to disaster, weather, or telecommunications issues, our CSC has sufficient telephone system capacity to handle the estimated volume of calls served by this contract.

We have provided additional detail about our Customer Service Center in our response to requirement 4.4.2.1.

b) Web Scheduling

Vendor must provide a secure web site where Applicants and/or agencies can schedule, change or cancel appointments, provide demographic data, pay fees and retrieve directions to fingerprinting centers. The web site must be available 24 hours a day, seven days a week with minimal downtime for regular maintenance. All scheduled maintenance must be scheduled during off-peak times. All interaction with this web site that includes provision of personal or financial information shall be encrypted using industry standard encryption algorithms such as Secure Sockets Layer protocol (SSL).

The Vendor must provide a link to its existing web scheduling application so that the State can verify its existence and test its performance.

The Vendor must provide statistics on the number of appointments scheduled via web-based application annually.

MorphoTrust meets the requirements.

We will continue to provide our secure web site that is already in use by West Virginia applicants to schedule, change or cancel appointments, provide demographic data, pay fees and retrieve directions to Enrollment Centers.

The current website is currently active for verification and testing at the following URL:
https://wv.l1enrollment.com/OpenNetworkPortal/spring/customer?execution=e1s1

We propose to upgrade during the first year of the contract to our secure UEP Pre-Enrollment Website. The UEP website simplifies the registration process and makes it even more intuitive, improving the online experience for applicants.

The simpler online registration process also reduces the volume of calls to our Customer Service Center, thereby speeding the phone registration time. The reduction in the registration processing time will directly affect the number of calls that can be processed within a given period. Today, the average call wait time in our West Virginia program is four minutes, compared to the wait times of less than 30 seconds in our Universal Enrollment Services program, which uses the UEP website. Customers of our TSA Universal Enrollment Services program self-register for appointments or walk-in service at a rate of 98%.

Our UEP web pre-enrollment and scheduling solution is also phone and tablet friendly. The UEP Pre-Enrollment Website can be tested at the following URL:

https://universalenroll.dhs.gov

In our response to requirement 4.4.2.5 on page 32, we provided additional instructions for testing performance of both web sites.

Both web sites are available 24 hours a day, seven days a week, 365 days a year, with minimal downtime for maintenance that is scheduled during off-peak times. Both web sites safeguard the applicant's personal and financial information using a Secure Socket Layer protocol (SSL) following industry standards for encryption.

Secure Infrastructure in Place

MorphoTrust already has infrastructure in place for the secure transmission and storage of personal and financial information of West Virginia applicants.

More than two million applicants per year register with us online, including 55,000 applicants from the West Virginia program.

c) Fee Collection

Vendor must collect all Applicant fees including State and FBI fees. Vendor must accept a) the following forms of payment online: e-check and credit card (at least Visa and MasterCard) and b) the following forms of payment at the fingerprinting location: personal check, credit card (at least Visa and MasterCard) and money order and c) prepaid and/or credit billing accounts for private agencies and employers and d) credit billing accounts for governmental agencies.

The Vendor must provide statistics on the number of Applicant fingerprinting payment transactions processed annually by payment type.

The Vendor must ensure that Applicant appointments are scheduled in a timely manner within 10 business days from the time the Applicant makes initial inquiry unless the Applicant requests an appointment beyond the 10 days.

The customer service center must, at a minimum, provide scheduling of appointments, answer Applicant questions and provide directions. Merely registering Applicants does not meet the requirements of this RFP.

MorphoTrust meets the requirements.

Applicant Fees

MorphoTrust will collect all applicant fees including State and FBI fees, through multiple payment options. We agree to accept all required forms of payment, as listed in Table 14, but we recommend that payment is rendered at the time of processing as a best practice.

Table 14: Forms of Payment

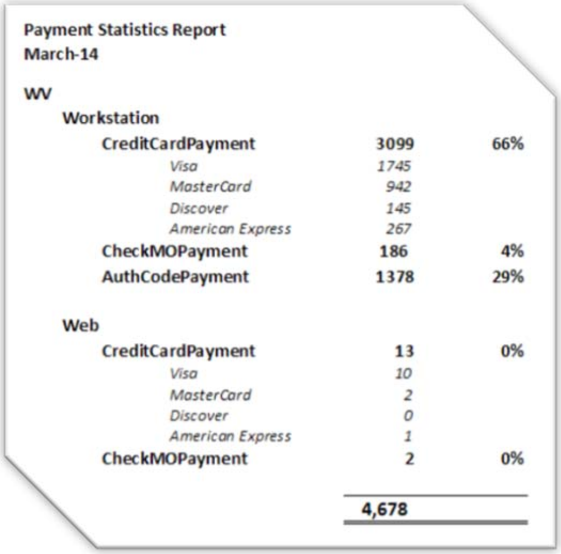
Transaction Type	Current WV Platform	UEP Platform
Online Payment by Applicant	e-check Credit Card (V/M/D/A)	e-check : *Not Recommended* Credit Card (V/M/D/A)
Payment at Enrollment Center by Applicant	Personal check Corporate Check Money Order	Personal check: *Not Recommended* Corporate Check Money Order Credit Card (V/M/D/A)
Private Agencies and Employers	Prepaid and/or Credit Billing Accounts	Credit Billing Accounts *(Credit Pending)* Credit Card Backed Accounts
Governmental Agencies	Credit Billing Accounts	Credit Billing Accounts

We have provided additional details of our plan for collecting fees from applicants in our response to requirement 4.4.2.6.

Payment Statistics

MorphoTrust's UEP system provides payment statistics in real time or per scheduled report distribution (daily, monthly, or annually). Figure 38 is an example of a monthly payment statistics report.

Enrollment level itemized detail supporting each value is also available for download in CSV format.



Payment Statistics Report
March-14

WV		
Workstation		
CreditCardPayment	3099	66%
Visa	*1745*	
MasterCard	*942*	
Discover	*145*	
American Express	*267*	
CheckMOPayment	186	4%
AuthCodePayment	1378	29%
Web		
CreditCardPayment	13	0%
Visa	*10*	
MasterCard	*2*	
Discover	*0*	
American Express	*1*	
CheckMOPayment	2	0%
	4,678	

Figure 38: Monthly Payment Statistics Report

Appointment Scheduling

MorphoTrust will provide adequate Enrollment Center locations and appointment capacity to ensure that applicants have access to locations and appointment slots so that they can be fingerprinted within 10 business days.

As part of our Quality Assurance Surveillance Plan (QASP), we routinely monitor appointment availability. Our program management and regional operations teams evaluate Enrollment Center capacity and utilization on a recurring schedule to assess and remediate recurring issues related to appointment availability.

Customer Service Center

MorphoTrust's Customer Service Center acts as a central point of information and assistance for applicants and User Agencies. In addition to providing scheduling services for appointments, CSRs assist applicants with program information, answer their questions about the process and status of their background checks, and provide directions to sites.

4.5.2 Equipment

Vendor will be required to capture Applicant fingerprints digitally.

a) Live Scan Device

All live scan or card scan equipment used to support the Applicant Fingerprinting Service project must be certified according to the FBI Image Quality Standards (IQS), Appendix F Standards. The Vendor must provide a copy of the FBI certification letter in their response.

Live scan equipment must be able to build and submit records at 1000 ppi in compliance with the state Interface Control Document (ICD), state National Institute of Standards and Technology (NIST) definitions including records Type 1 (State), Type 2 (State), Type 8 (Signature), and Type 14 (flat and rolled). This ICD document can be found in Appendix A.

The live scan device must be capable of capturing 1000 ppi 4, 4, 2 slap only capture.

The Livescan device will assign a transaction control number (TCN) which will be unique and used to track all submissions throughout the fingerprinting process. The format of the TCN is shown in the ICD document in Appendix A.

The live scan device must provide necessary data fields required to process the transaction through the State's AFIS System. Unique data fields are required to be transmitted within the NIST file and can be found in Appendix A. The Vendor will be required to contract with the State AFIS Vendor for the development and testing of this interface.

Interface with WVSP AFIS

As the current provider of fingerprinting services in West Virginia, MorphoTrust has successfully engineered an interface between our fingerprinting technology and the WVSP AFIS. ***We are fully compliant with the State's AFIS system and will continue to be compliant going forward.***

Furthermore, because MorphoTrak is a sister company to MorphoTrust, we can work closely together to resolve any issues that arise between our systems.

MorphoTrust meets the requirements.

The proposed 1000 dpi Livescan devices comply with the Interface Control Document provided in RFP Appendix A. The scanner meets National Institute of Standards and Technology (NIST) definitions including records Type 1 (State), Type 2 (State), Type 8 (Signature), and Type 14 (flat and rolled). The proposed devices feature 1000 ppi 4, 4, 2 slap-only capture.

While MorphoTrust proposes a 1000 dpi scanner as required by the RFP, we also propose an alternative 500 dpi scanner. We have provided a detailed equipment description in our response to requirement 4.4.6.

All proposed Livescan devices meet FBI Image Quality Standards (IQS), Appendix F Standards and we have provided FBI certification letters in Appendix E.

Our Livescan solution will assign the unique transaction control number and required data fields as specified in the Interface Control Document, which will be transmitted the NIST file to the WVSP AFIS. MorphoTrust already has an established interface between our fingerprinting technology and the WVSP AFIS. We will work with MorphoTrak on any additional development and testing that may be required.

b) ID Authentication

The Vendor personnel must require the Applicant to provide valid governmental photo identification for proof of identity at the fingerprinting session using the most current ID Verification guide from the Compact Council.

MorphoTrust meets the requirements.

While the Compact Council guidelines do allow for forms of identification that do not contain a photo, MorphoTrust recommends requiring a Photo ID issued by a U.S. State, U.S. Territory, or a U.S. Government agency.

Enrollment Agents will require a valid governmental photo identification for proof of identity before the applicant is fingerprinted. Our training program prepares Enrollment Agents to determine that the ID is genuine and valid.

As an added security feature, MorphoTrust proposes our Identity Proofing Solution, which leverages our industry-leading iA-thenticate® authentication software and B5000 Document Reader. The B5000 analyzes state and federal government-issued photo identification documents including driver licenses, government-issued ID cards, military IDs, or Passports. We have described this solution in detail in our response to requirement 4.4.6.1.

c) Manual Process

The Vendor shall have the capability to provide an Applicant with a completed manual inked or electronically printed FBI standard fingerprint card if requested.

MorphoTrust meets the requirements.

Our solution includes "Print and Go" capability that allows any applicant to have a physical FD-258 hard card produced from their fingerprints. After collecting the applicant data and capturing the fingerprints, the Enrollment Agent prints a FD-258 hard card instead of submitting an electronic record. Hard cards are printed using a Lexmark MS810n or T600 series printer.

We have described the manual process in more detail our response to requirement 4.4.6.1.

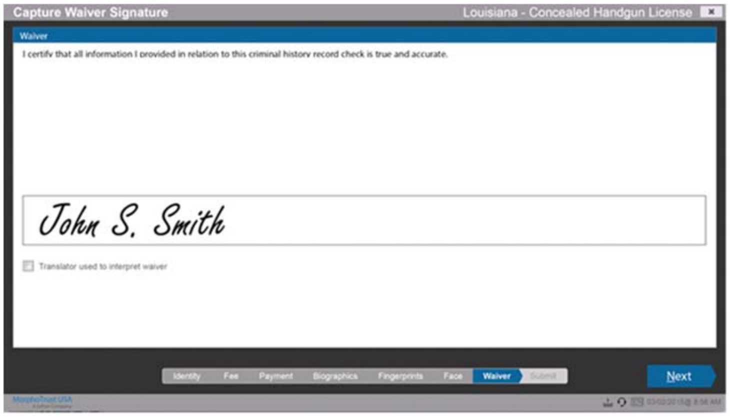
d) Digital Signatures

The Vendor is required to collect a digital signature from each Applicant at the time of fingerprinting following the Applicant's review and acknowledgement of terms and conditions related to the release of the Applicant's criminal record.

The Vendor must provide an example of where it has used signature capture devices in an Applicant fingerprint network and statistics on the number of Applicants processed utilizing this equipment.

MorphoTrust meets the requirements.

After applicants complete the fingerprinting process, the Enrollment Agent requests that they review the terms and conditions related to the release of their criminal record. Applicants acknowledge by providing their signature on an electronic signature pad. The signature is captured by the UEP workstation software (Figure 39) and saved with the applicant's record.



Capture Waiver Signature

Louisiana - Concealed Handgun License

Waiver

I certify that all information I provided in relation to this criminal history record check is true and accurate.

John S. Smith

□ Translator used to interpret waiver

Figure 39: Captured Signature

We currently provide signature capture devices in the West Virginia Enrollment Centers, where we have provided fingerprinting services for more than 220,000 applicants.

MorphoTrust also captures signatures for our TSA Pre✔® program, in which the applicant is required to read a waiver provided by TSA and apply their signature using an LED touchpad. We provide fingerprinting services for more than one million TSA Pre✔® applicants per year.

e) Central Server/Store and Forward

The Vendor must provide a central server configuration that will receive and process electronic demographic, signature and fingerprint image information from the remote fingerprint capture locations. This component must include a secure communication line from the central server to the state network and equipment allowing for submission to the State's AFIS system for transaction processing. This interface requirement is defined in the State ICD document.

The Central Server must have adequate disk storage to retain a month's worth of fingerprint submissions in the event a communications circuit is not operational. Upon restoration of communication, the information must be sent to the criminal records repository without the need to re-fingerprint the Applicants.

All fingerprint images, signature images, and demographic data shall be archived by the Vendor and shall remain the sole property of the State. The fingerprint image, signature image, and demographic data shall be stored in a non-proprietary EFTS format, meeting all State and FBI standards. The Vendor shall store these existing fingerprint images and demographic data with the ability to retrieve and transmit to the State. The database shall be purged of all transactions after one year from the date of submission. A Backup copy of the database will be written to an external location on the WVSP network daily.

The archive may be used for the subsequent transmission of archived data for statutory re-licensing issues. The archive may also be used for the re-transmission of any unsuccessful transmission.

The Vendor must develop a re-transmission procedure with individual user agencies to ensure that the correct records are submitted for re-transmission and that the accompanying demographic data is correct.

A Network share on this server will be created so that the Staff of the WVSP and Vendor may exchange sensitive data in a secure manner.

An administrator account will be provided to the WVSP for audit purposes on the server.

The Vendor must disclose its annual volume of Applicant fingerprint transactions processed through existing central servers.

MorphoTrust meets the requirements.

Our current Central Server meets these RFP requirements and our UEP solution will continue to meet the requirements. We currently produce a database backup on the WVSP network daily and we propose to continue this process under the new contract for fingerprinting services.

Additionally, a network share on the TCP server is currently available, which the WVSP staff and MorphoTrust use to exchange sensitive data in a secure manner. WVSP has an administrator account on the TCP and Web Portal server with full access to all data, logs, and other system configuration information.

We meet all State and FBI standards for archiving all fingerprint images, signature images, and demographic data in a non-proprietary EFTS format. All archived data remains the sole property of the State and is purged from the database according to the required schedule.

We maintain adequate disk storage for more than one month of fingerprint submissions. In the event of a communications failure, submissions are sent to the criminal records repository upon restoration of communication, without the need to re-fingerprint applicants.

The following statistics demonstrate the annual volume of transactions processed through our central servers in state and federal programs:

- *More than five million fingerprint enrollments per year at more than 1,200 Enrollment Centers in 26 U.S. states.*
- *More than one million TSA Pre✔® applicants per year.*
- *70,000 West Virginia applicants per year*

In our response to requirement 4.4.4.1, we have provided additional details on our plan for collecting and housing fingerprint submissions.

f) Card Scan Conversion

User agencies' Applicants using manual "ink and roll" fingerprint cards will forward fingerprint cards to the Vendor. The Vendor shall conduct a technical examination of the fingerprint images to ensure a successful conversion into the electronic medium at 1000 ppi. Fingerprint images that do not pass the Vendor's technical examination shall be returned to the Applicant with a request for the bad prints to be re-rolled. The criterion for defining an "acceptable" quality fingerprint will be agreed upon by the Vendor and the State.

The Vendor shall convert data, signature and acceptable flat and rolled "ink and roll" fingerprint cards into an electronic medium whereby they may be transmitted electronically per the ICD found in Appendix A. This conversion and electronic transmission to the State must occur within 48 hours of receipt by the Vendor.

Following conversion, the Vendor shall document the transaction number of the electronic submission on the manual card and store the electronic record of the card and record release authorization on the State Central Repository.

The Vendor must provide an example of where it has performed card scanning in an Applicant fingerprinting network and statistics on the number of Applicants processed utilizing this equipment.

MorphoTrust meets the requirements.

Fingerprint cards may be mailed to our central facility, where we digitize them and submit them today at 1000 ppi to the State AFIS, in the same manner as a Livescan submission. Our card scanning service employs commercial off-the-shelf (COTS) Card Scanning Workstations, which are FBI-certified to the IAFIS IQS Appendix F Scanner Requirements.

All incoming fingerprint cards are reviewed for completeness and quality prior to processing for submission to the State. Any cards that do not meet the minimum requirements (i.e. all fingerprint images collected properly, unless noted as AMP; all applicant demographic data; all pertinent agency and submission information) are returned to the applicant with notations regarding the missing data and instructions on what is needed, including any necessary re-rolls for bad prints. This process is in place today and will continue to be utilized.

Our proven centralized Cardscan Center converts and digitally submits more than 100,000 paper fingerprint cards annually in support of numerous statewide networks as well as FBI Channels. We provide Cardscan services for both state and federal civil applicants and state criminal backlog conversion.

Our Cardscan customers include:

- South Carolina Law Enforcement Division
- Texas Department of Public Safety
- Florida Department of Law Enforcement
- New York Department of Criminal Justice Systems
- Indiana State Police
- Michigan State Police
- Tennessee Bureau of Investigation
- Oklahoma State Bureau of Investigation

We will convert and electronically transmit manual "ink and roll" fingerprint cards to the State within 48 hours of receipt, in accordance with the Interface Control Document provided in RFP Appendix A, and will document the transaction number of the electronic submission.

We have described our conversion process in our response to requirement 4.4.6.1. Figure 37 on page 77 illustrates the conversion process.

4.5.3 Electronic Fingerprint Capture Service

a) Fingerprinting Sites

All fingerprinting sites must be ADA compliant.

Fingerprinting sites must be established and staffed in such a manner as to ensure meeting the 10 business day scheduling requirement. No Applicant should have to travel more than a maximum of 35 miles (one way) to access fingerprinting services. The Vendor will provide at a minimum, mandatory site locations in the Charleston, Huntington, Martinsburg, Morgantown, Beckley, Elkins, Wheeling, Logan, Princeton and Parkersburg areas. Fingerprint sites must be staffed by personnel that are approved by the West Virginia State Police.

Communications, facility and any other expenses required to perform the fingerprinting services as specified in this contract will be the responsibility of the Vendor.

The Vendor shall provide a receipt in a format approved by the State to each Applicant as evidence of successful completion of the fingerprinting, including the identifying State Control Number assigned and submitted with the electronic submission.

The Vendor may work with user agencies to provide convenient fingerprinting sites as long as they meet the requirements above.

MorphoTrust meets the requirements.

Site Assessment and ADA Compliance

MorphoTrust requires all potential Enrollment Center locations to pass a rigorous Readiness Assessment, which requires the Site Assessor to evaluate over 50 qualities of the facility, including compliance with ADA laws. All sites are reviewed against the following ADA requirements:

- ADA accessible entrances:
  - Doors have a minimum 32 inch width clearance
  - External entrance is accessible directly from ground level, or easily accessible via accessibility ramp if located above ground level
  - Internal entrance (if applicable) is accessible directly from ground level, or easily accessible via elevator if located above or below ground level
  - Elevators if building is multiple levels
  - Hallways have a minimum 36 inch width clearance
- ADA marked parking spaces for disabled individuals at a 1:8 ratio (i.e.: one handicapped parking space to every eight parking spaces)

Enrollment Center Locations

MorphoTrust proposes 27 Enrollment Center locations in West Virginia, which have been identified, established and staffed in such a manner to meet the availability requirement that all applicants will be fingerprinted within 10 business days of request.

In our response to requirement 4.4.3.1, we described the proposed locations. Table 10 on page 35 lists the locations and hours of operations and the map in Figure 7 shows the statewide distribution.

Our current and proposed locations for Enrollment Centers provide geographic coverage so that no applicant will have to travel more than a maximum of 35 miles (one way) from their place of home or work to access fingerprinting services. An Enrollment Center is available in all of the major West Virginia locations noted in the RFP: Charleston, Huntington, Martinsburg, Morgantown, Beckley, Elkins, Wheeling, Logan, Princeton and Parkersburg areas. In addition to the locations required by the RFP, we propose additional Enrollment Centers to fulfill the 35 mile travel requirement.

We will work with all West Virginia agencies to fulfill their needs for Enrollment Centers, within the requirements described above. All Enrollment Center Agents will be subject to approval by the West Virginia State Police.

MorphoTrust bears all communication, facility and other expenses related to the operation of the Enrollment Centers.

Receipts

MorphoTrust provides a receipt to each customer upon completion of the in-person enrollment process that meets the RFP requirements including the State Control Number. We have described the receipt in our response to requirement 4.4.3.4 and shown the proposed receipt in Figure 13.

b) On-site Fingerprinting Services

Vendor must provide on-site fingerprinting services for groups of 25 or more Applicants. The location must be at the convenience of the requesting agency. The Vendor must provide a point of contact for agencies wishing to use this service. The service may be negotiated between the Vendor and the requesting agency.

MorphoTrust meets the requirements.

We will provide on-site mobile fingerprinting anywhere in the state for groups of 25 or more. Based on our experience with the demand for onsite services in other states, we are initially planning to have three mobile fingerprinting units throughout the state for the convenience of requesting agencies, although additional resources can be added if the demand for mobile services supports an expansion.

MorphoTrust typically requests that such sessions be scheduled at least two weeks in advance. We respond to all requests in a timely manner and work with the requestor to identify the most convenient, available option for the on-site session. Full instructions and guidance are provided to the customers during the schedule setup, including technical and space requirements for the site, sample advanced communication and notifications to applicants, and expectations during the on-site visit.

We have provided additional detail about our on-site fingerprinting services in our response to requirement 4.4.3.2.

c) Applicant Appointment

1) Applicant Identification

The Applicant must present a valid form of photo ID at the time of fingerprinting. Acceptable forms of photo identification are drivers licenses issued by any state, passport, photo identification card issued by a municipality, county or state in lieu of a driver's license or a military ID.

2) Collect payment where not paid at the time of appointment scheduling, if applicable.

3) Verify Applicant demographic data.

4) Provide the release for record check authorization, provide a copy of the challenge process for the state and federal process as outlined in 28 CFR 50.12(b), and collect digital fingerprints and a signature.

5) The Vendor shall provide a receipt in a format approved by the State to each Applicant as evidence of successful completion of the fingerprinting, including the identifying State Control Number assigned and submitted with the electronic transmission.

6) Records must be transmitted in a timely manner within 24 hours from collection.

MorphoTrust meets the requirements.

Table 15 summarizes the steps in the process for an applicant's visit to an Enrollment Center. We have described the process in more detail in our response to requirement 4.4.3.3 and illustrated the steps in Figure 9 on page 40.

Table 15: Steps in the Applicant Appointment Process

Appointment Scheduling	• Applicant schedules appointment either online or by calling Customer Service Center • Applicant can opt to pay fees by a variety of methods • Applicant receives appointment tracking number and confirmation information • If an email address is provided, appointment information is emailed to the applicant along with a link to an online mapping of appointment location
In Person at Enrollment Center	• Applicant's record is loaded on Livescan from the MorphoTrust Central Server • Applicant's photo ID is authenticated • Applicant's ID is checked against the demographic data supplied at time of appointment scheduling • Applicant is asked to verify all demographic information • Applicant is asked to review terms and conditions and provide signature through signature pad device • Applicant is fingerprinted • Applicant pays fee if not paid at time of appointment scheduling • Applicant is provided with a receipt of the transaction. Receipt includes the State Control Number, date, applicant type, amount paid and signature of Enrollment Agent
After Appointment	• Records are transmitted in real time from fixed sites • Records are transmitted within 24 hours for mobile sites or onsite fingerprinting sessions without an internet connection

Please note that our solution transmits records from the Enrollment Centers in real time, more than meeting the State's requirement for transmission within 24 hours from collection.

d) Electronic Submission Acceptance Requirements

The Vendor must be able to achieve and maintain acceptability rates of more than 98%.

MorphoTrust will meet the requirements.

We agree to maintain a ninety-eight percent (98%) classifiable rate for all Livescan fingerprint submissions digitally collected by MorphoTrust and our partners. We cannot warrant the quality of Cardscan submissions where fingerprints were physically collected by a third party.

We provided additional information about our plan for fingerprint acceptance in our response to requirement 4.4.3.6.

e) Fingerprint Technician Training

The Vendor shall provide well-trained personnel to take fingerprints. The responsibility and costs for training these personnel is entirely with the Vendor. The Vendor must include a narrative explaining the curriculum used for training/certifying fingerprint personnel.

MorphoTrust meets the requirements.

We will staff Enrollment Centers with certified Enrollment Agents who are fully trained in all aspects of the fingerprinting process. We understand that all costs related to training Enrollment Agents rest with us and we will assume responsibility for training and all associated costs.

In addition to the following description of our curriculum used for training/certifying fingerprint personnel, we have described our Training and Operations Manual, Computer-Based Training, and Performance Evaluations in our response to requirement 4.4.3.7.

Enrollment Agent Certification Training

All fingerprint technicians (referred to by MorphoTrust as Enrollment Agents) for the West Virginia Enrollment Centers, whether MorphoTrust employee, partner, or subcontractor, are required to complete an internal certification process to ensure the Agent is competent to perform the job responsibilities, functional requirements of operating the equipment, and quality standards of performance. Our professional certification process blends the use of a scripted training manual with supervisory/trainer observation and Enrollment Agents work demonstration.

Enrollment Agents hired for this project will go through an orientation and systematic training program that focuses on the West Virginia program requirements. Upon the Enrollment Agent's completion of the onsite training, Certified Trainers use a pre-defined Observed Behaviors Checklist to track the enrollment agent's competency and understanding of all written policies/procedures. The checklist identifies on-the-job behaviors expected of all personnel such as professional customer interaction, professionalism, policy and procedure compliance, system navigation, capturing quality prints and mastery of required skills.

Training Curriculum

Our proven Training Program has been utilized to train over 3,500 Enrollment Agents to date. We believe that training is critical to develop a fully qualified Enrollment Agent capable of achieving a 98% classifiability rate, dealing with the general public, and handling equipment issues.

Our training program consists of:

- Hardware overview of the Livescan workstation.
- Software overview of the Livescan system. The Enrollment Agent must become skilled in the operation of all Livescan software. This includes how to electronically transfer and receive demographic information, transfer fingerprints to the secure Data Center, and perform all system maintenance and system utility functions. Training is conducted on the identification of pattern type, delta(s), core, and determining the overall quality of the fingerprint
- Technical support overview of diagnostic functions.
- Field training - The Enrollment Agent trainee will be placed with an experienced Enrollment Agent who double-checks the quality of each fingerprint taken, and instructs the trainee on how to capture fingerprints most efficiently and effectively. Enrollment Agents will fingerprint many test applicants prior to completing the on-site training program.
- Best-practice customer service (attitude, dealing with difficult people, escalation processes, MorphoTrust customer service policies)
- Security and Confidentiality (data, personal information, MorphoTrust security protocols)
- Program specifics (Agency information, Applicant types, required forms and information, assisting applicants in obtaining necessary information)
- MorphoTrust Corporate and Enrollment Services general information (who to contact, web links)
- Review of company policies with each Enrollment Agent. Among other topics, this includes instruction on quality standards, security procedures,

emergency procedures, privacy policies, personal appearance, identification verification, state fingerprinting laws and requirements, how to interact professionally with the client and how to make the applicant's fingerprinting experience as pleasant as possible.

4.5.4 Results Processor

In order to a) create a single source of result delivery and b) create a secure automated method of processing and reporting these transaction results, the Vendors must provide the State with Automated Results Processing capability.

The results processor must be capable of processing the returned results as specified in the example returns as found in Appendix A.

In order to accomplish this functionality, all transactions submitted from livescan devices must be processed at a Central Transaction Switch. This hardware and software solution, which will be provided by the Vendor, but remain under the physical control and security of the State, serves as the central point of receipt, return, and coordination of all transaction results for any fingerprint or supporting name based transactions. The Central Transaction Switch must:

- Utilize a database that records transactional data, search results, Applicant information, transaction configurations, and other information necessary for the proper tracking, execution, and result dissemination of all transactions and system function.
- Be easily customizable by the State
- Be capable of programmatically creating and delivering results to authorized entities by email or paper letter, or a combination of both. Provide a Web Server for electronic access to the results over the Internet with the proper security in place to meet the current CJIS Security Policy. This server will show the current status of all transactions in the system.
- Allow the State direct access to the information contained in the database for each transaction, including Applicant information, transaction tracking information, transaction status, and all results data via client software provided to the State for use as a part of the Applicant fingerprinting solution. Access from this software must be controlled by User id and password. Authorized users must be allowed to change transaction status, reprint results and perform follow up inquires to appropriate data sources to complete tasks necessary to adjudicate the transaction. All necessary configuration information including agency and ORI information must be table driven and able to be updated by the State.

MorphoTrust meets the requirements.

We have successfully implemented automated results processing and reporting functions in West Virginia. Our solution is already proven and fully operational in the WVSP environment, so the State of West Virginia can be confident of continued service with no disruption.

Figure 40 provides a solution overview including the central results server.

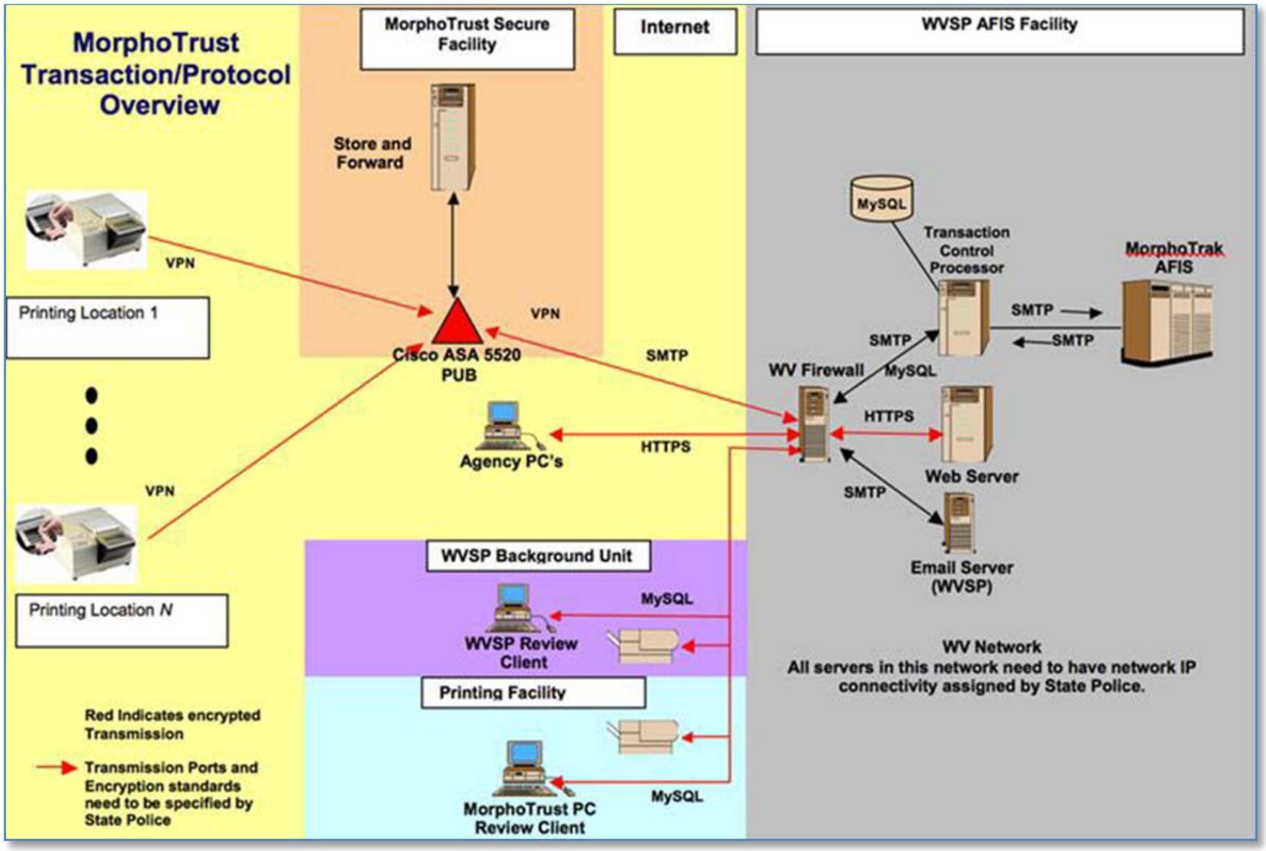

MorphoTrust Transaction/Protocol Overview
MorphoTrust Secure Facility
Internet
WVSP AFIS Facility
Store and Forward
VPN
Printing Location 1
VPN
Cisco ASA 5520 PUB
SMTP
VPN
Printing Location N
Agency PC's
HTTPS
MySQL
Transaction Control Processor
MorphoTrak AFIS
SMTP
SMTP
SMTP
WV Firewall
MySQL
HTTPS
Web Server
SMTP
Email Server (WVSP)
WVSP Background Unit
MySQL
WVSP Review Client
Printing Facility
MorphoTrust PC Review Client
MySQL
WV Network
All servers in this network need to have network IP connectivity assigned by State Police.
Red Indicates encrypted Transmission
Transmission Ports and Encryption standards need to be specified by State Police

Figure 40: Solution Overview including Results Processing

MorphoTrust's automated results processing solution will return results as specified in Appendix A of the RFP. All transactions submitted from Livescan devices will be processed at a Central Transaction Switch.

Automated Results Processing

As described in our response to requirement 4.4.4.4, MorphoTrust has already provided West Virginia with a robust solution for automated result processing. We will continue to provide a single source of result delivery and secure automated method of processing and reporting these transaction results.

Our solution uses a combination of automated transaction processing software, consolidated administrative result review and letter processing, and a secure user review website for query-only users. The results processing hardware and software will remain under the physical control and security of the State.

The solution reduces disposition workloads by 80% or more by:

- *Automatically dispositioning and reporting results that have no indication of a criminal record*

- ***Providing a single point of disposition processing from the user desktop, to efficiently process the remaining transactions for automated disposition and reporting to User Agencies***

Our fingerprint processing solution automates and streamlines the processing of state and FBI criminal record results. Any record reporting "no record" or "all clear" results from all data sources can be processed with no human intervention. Results for all other records are consolidated into a combined result record, allowing for more efficient processing by the authorized reviewing entity.

Result Notification

Our result processing solution can provide the following additional functions:

- Send email notification of transaction completion to employing or licensing agencies
- Allow for review and processing of transactions that may require or allow adjudication by the authorized entity
- Provide for secure web access to applicant transaction status and data by authorized entities

Notification types include:

- ***Applicant & Agency Notifications*** – result letters bearing the WVSP letterhead are automatically generated for all approved applicants and printed out for mailing. All result letters contain only the appropriate results as necessary and permissible by State and FBI rules. Upon transaction completion, email notifications are sent to employing or licensing agencies.
- ***Automated Renewal Required Notifications*** – for credentials that have expiration dates (ex: Concealed Weapon Permit), notification letters are generated prior to the expiration advising the credential holder of the steps required to complete the renewal process.

Generation of Response Letters

MorphoTrust's Review Client solution provides batch processing of letters and/or emails as an integral step of adjudication processing. Configurable result processing rules govern how letter processing occurs, based upon factors such as agency and applicant type. Key results processing capabilities of the solution include:

- Only personnel authorized by State of West Virginia can generate response letters

- From the list of applicants for whom an adjudication decision has been made, authorized personnel can specify whether to print letters for all applicants (batch) or selectively indicate one or more applicants for whom to generate a response letter
- Checklist of applicants for whom letters will be produced, so authorized personnel can verify that all letters are printed and can reprint any letters lost to printer jams, toner outage, etc.
- Letter formatting aligns the applicant name and mailing address to appear in the envelope window
- Electronic image of the result letter is retained in the database for future review and reprinting

User Access Controls

Review Client users are assigned permissions so they can only perform the activities for which they are authorized. For example, only designated Review Client users can assign a final disposition or redact results, while other Review Client users can add notes or attachments to an applicant record.

State Access to Data via Administrative Queue Review

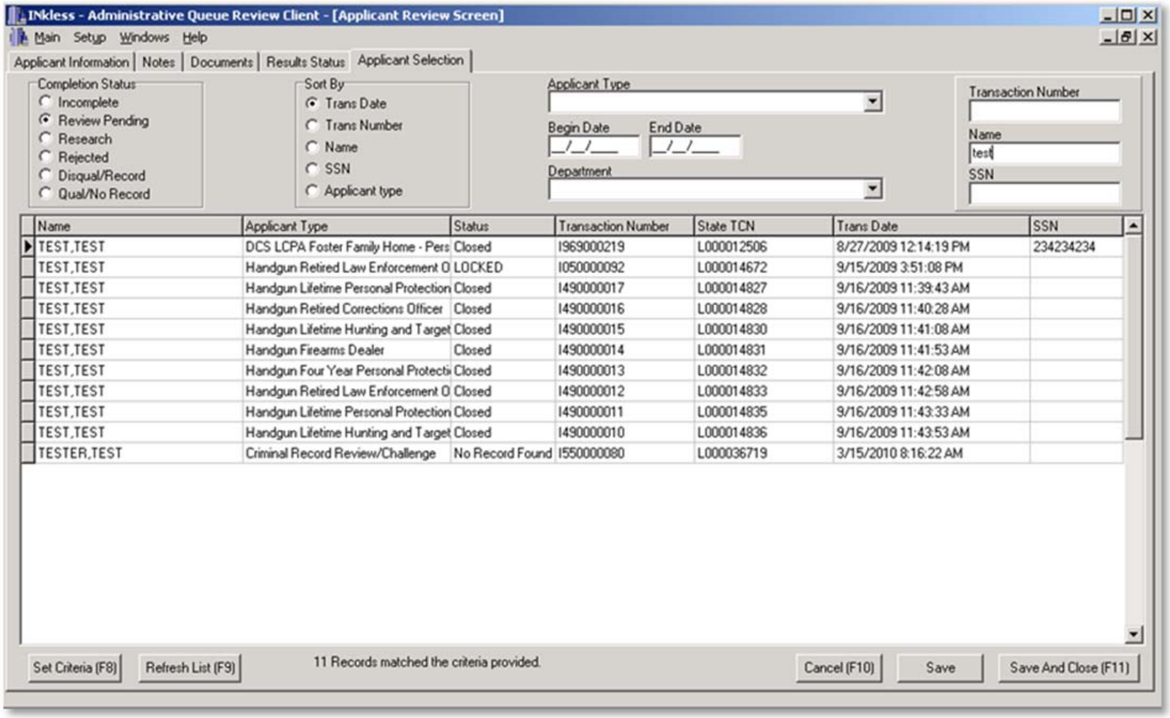
The Administrative Queue Review Client presents a single source for operator review of all transaction result and applicant information and permits the authorized user to adjudicate the results of transactions. This function is accessible to multiple simultaneous users that have a proper login name and password. The Client accesses the Database Server for all transaction data and status.

Transaction and user information is accessed by an authorized user through the Applicant Selection Screen, a single screen with several options for searching. The demographic data and all returned query responses are presented when an operator selects a transaction to review and process. The demographic data is displayed on the Applicant Information Screen and the WVSP and FBI response data is displayed in the Query Response Screen.

The following pages provide an overview of the process for searching and retrieving applicant information using the Administrative Queue Review Client. Figure 41 through Figure 43 are screen shots of the application.

Applicant Selection

The applicant selection screen, shown in Figure 41, is used to search for applicants and transactions using various search criterion and transaction status values. Authorized personnel can search for an individual applicant by fields such as name or SSN, or they can generate a list of applicants by fields such as date range, applicant type, or transaction status.



Completion Status
○ Incomplete
● Review Pending
○ Research
○ Rejected
○ Disqual/Record
○ Qual/No Record

Sort By
● Trans Date
○ Trans Number
○ Name
○ SSN
○ Applicant type

Applicant Type:
Begin Date: __/__/____ End Date: __/__/____
Department:

Transaction Number:
Name: test
SSN:

Name	Applicant Type	Status	Transaction Number	State TCN	Trans Date	SSN
TEST,TEST	DCS LCPA Foster Family Home - Pers	Closed	I969000219	L000012506	8/27/2009 12:14:19 PM	234234234
TEST,TEST	Handgun Retired Law Enforcement O	LOCKED	I050000092	L000014672	9/15/2009 3:51:08 PM	
TEST,TEST	Handgun Lifetime Personal Protection	Closed	I490000017	L000014827	9/16/2009 11:39:43 AM	
TEST,TEST	Handgun Retired Corrections Officer	Closed	I490000016	L000014828	9/16/2009 11:40:28 AM	
TEST,TEST	Handgun Lifetime Hunting and Target	Closed	I490000015	L000014830	9/16/2009 11:41:08 AM	
TEST,TEST	Handgun Firearms Dealer	Closed	I490000014	L000014831	9/16/2009 11:41:53 AM	
TEST,TEST	Handgun Four Year Personal Protecti	Closed	I490000013	L000014832	9/16/2009 11:42:08 AM	
TEST,TEST	Handgun Retired Law Enforcement O	Closed	I490000012	L000014833	9/16/2009 11:42:58 AM	
TEST,TEST	Handgun Lifetime Personal Protection	Closed	I490000011	L000014835	9/16/2009 11:43:33 AM	
TEST,TEST	Handgun Lifetime Hunting and Target	Closed	I490000010	L000014836	9/16/2009 11:43:53 AM	
TESTER,TEST	Criminal Record Review/Challenge	No Record Found	I550000080	L000036719	3/15/2010 8:16:22 AM	

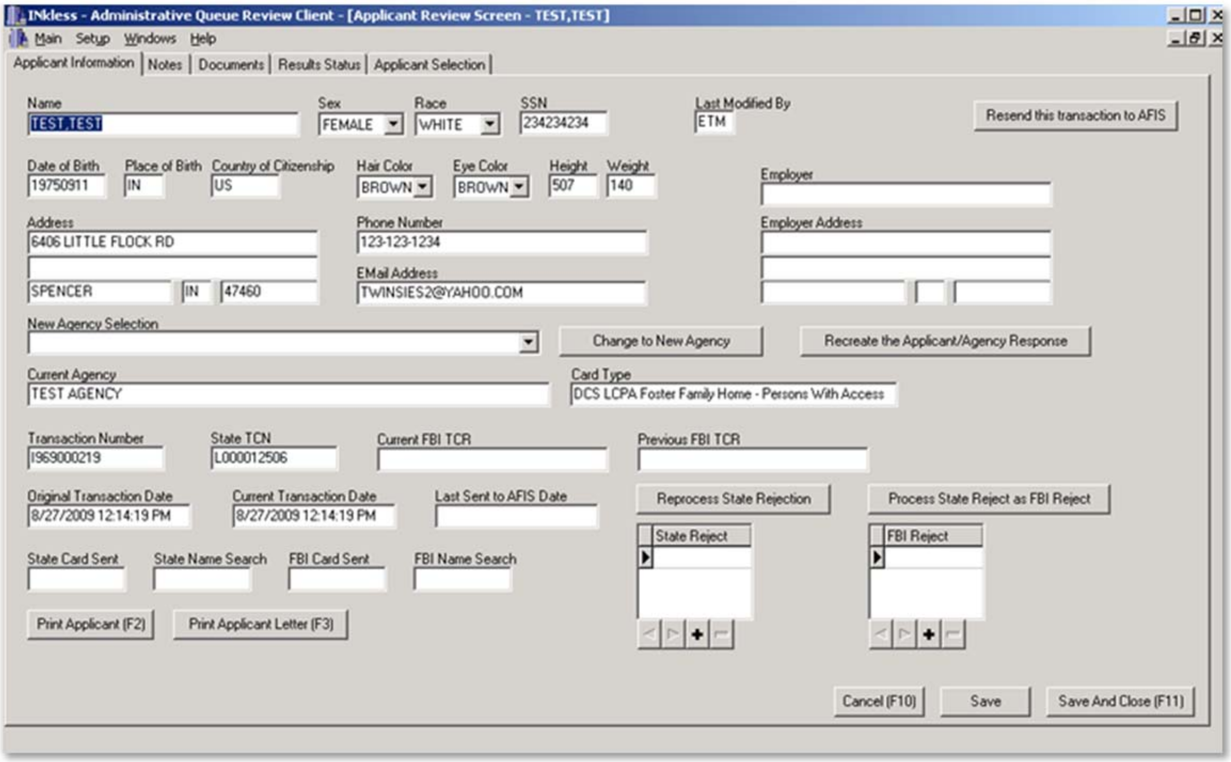
11 Records matched the criteria provided.

Figure 41: Administrative Queue Review – Searching Applicants for Review

Applicant Information

The Applicant Information screen (shown in Figure 42) allows authorized personnel to review the information submitted as a part of the selected applicant's transaction. Additional information on this screen includes the history of a transaction that was rejected by the WVSP or FBI and the mailing date for paper versions of the cards.

Other available functions include resending fingerprint transactions to the WVSP AFIS, reprinting results letter for a transaction, and printing applicant information.



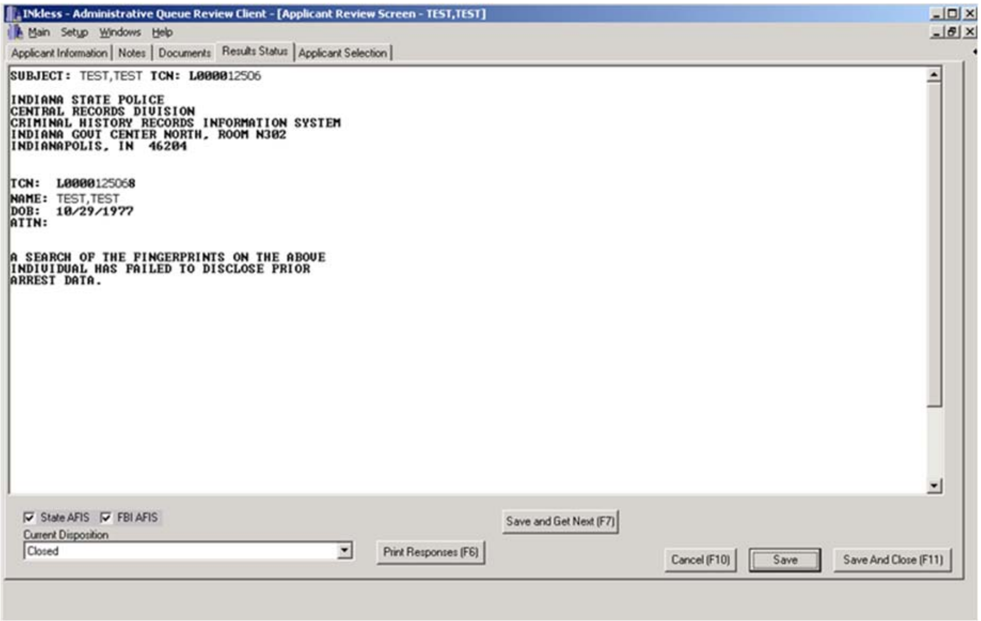
Name: TEST,TEST
Sex: FEMALE
Race: WHITE
SSN: 234234234
Last Modified By: ETM
Date of Birth: 19750911
Place of Birth: IN
Country of Citizenship: US
Hair Color: BROWN
Eye Color: BROWN
Height: 507
Weight: 140
Address: 6406 LITTLE FLOCK RD
SPENCER IN 47460
Phone Number: 123-123-1234
EMail Address: TWINSIES2@YAHOO.COM
Current Agency: TEST AGENCY
Card Type: DCS LCPA Foster Family Home - Persons With Access
Transaction Number: I969000219
State TCN: L000012506
Original Transaction Date: 8/27/2009 12:14:19 PM
Current Transaction Date: 8/27/2009 12:14:19 PM

Figure 42: Administrative Queue Review – Reviewing Applicant Information

Results Status Screen

The Results Status Screen (Figure 43) presents the query responses for review and allows for efficient processing of all transactions ready for adjudication. It also provides control buttons and function keys to re-send an individual query or the full set of queries (for optional data sources beyond the state and FBI AFIS).

Response indicators are displayed at the bottom of the screen to indicate that responses have been received and special highlighted indications when responses indicate that they are not automatically determined by the system to be “No Hit.” The operator can examine the response text to make the proper adjudication decision. The operator can also print all responses for a transaction by clicking the Print Responses key or button.



INkless - Administrative Queue Review Client - [Applicant Review Screen - TEST,TEST]
Main Setup Windows Help
Applicant Information | Notes | Documents | Results Status | Applicant Selection

```
SUBJECT: TEST,TEST TCN: L000012506

INDIANA STATE POLICE
CENTRAL RECORDS DIVISION
CRIMINAL HISTORY RECORDS INFORMATION SYSTEM
INDIANA GOVT CENTER NORTH, ROOM N302
INDIANAPOLIS, IN  46204


TCN:  L0000125068
NAME: TEST,TEST
DOB:  10/29/1977
ATTN:


A SEARCH OF THE FINGERPRINTS ON THE ABOVE
INDIVIDUAL HAS FAILED TO DISCLOSE PRIOR
ARREST DATA.
```

☑ State AFIS ☑ FBI AFIS

Current Disposition: Closed

Figure 43: Administrative Queue Review – Results Status Screen

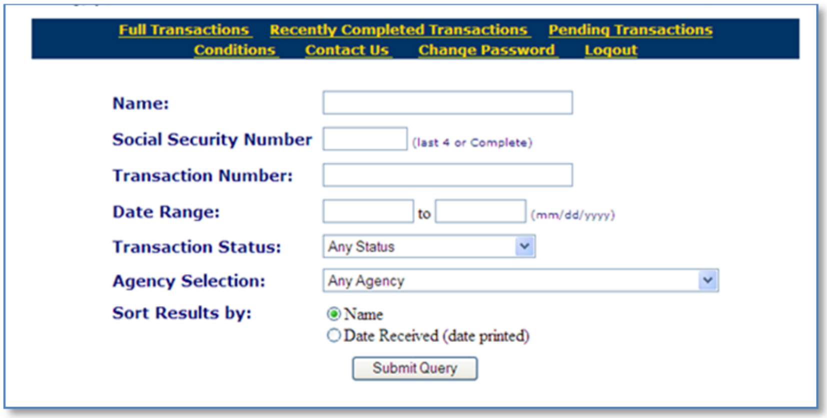
Other Client Functions

MorphoTrust's Review Client software provides a robust transaction management and documentation solution. In addition to the features described above, the client software provides system support tools for creation and setup of result letters, setting up details of each transaction type processed, user management and security, and maintenance of submitting agency tables. As seen in Figure 43, tabs across the top of the screen access functionality to add processing notes to the transaction, attach scanned support documents to the transaction, and resend result notifications to agencies.

State Access to Data via Secure Administrative Web Portal

Approved agency users and internal WVSP users can also our secure web portal to access transaction and applicant information. The main search screen, shown in Figure 44 and Figure 45, allows a variety of search options to allow users to find transactions and applicant status.

In states where MorphoTrust provides access to our Administrative Web Portal for agencies, the number of calls to the central records processing agency has been greatly reduced.



Name:

Social Security Number (last 4 or Complete)

Transaction Number:

Date Range: to (mm/dd/yyyy)

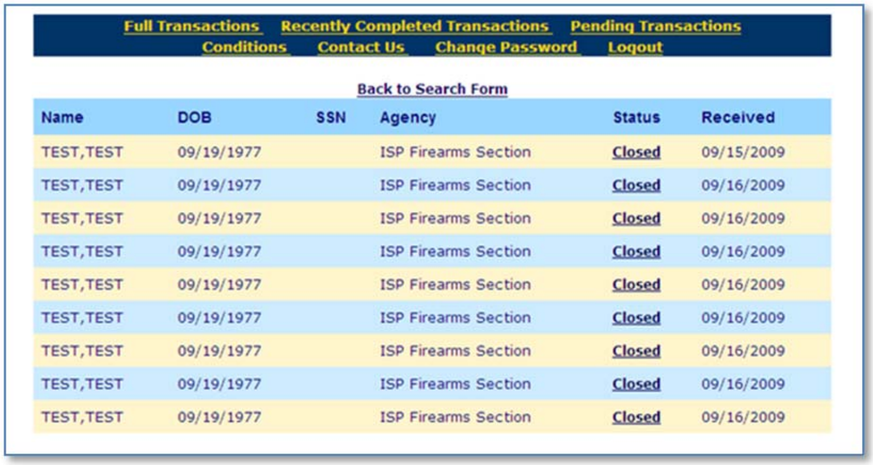
Transaction Status: Any Status

Agency Selection: Any Agency

Sort Results by: ● Name ○ Date Received (date printed)

Figure 44: Administrative Web Portal – Applicant Search

Access for users is limited to data for their own agency only.



Name	DOB	SSN	Agency	Status	Received
TEST,TEST	09/19/1977		ISP Firearms Section	Closed	09/15/2009
TEST,TEST	09/19/1977		ISP Firearms Section	Closed	09/16/2009
TEST,TEST	09/19/1977		ISP Firearms Section	Closed	09/16/2009
TEST,TEST	09/19/1977		ISP Firearms Section	Closed	09/16/2009
TEST,TEST	09/19/1977		ISP Firearms Section	Closed	09/16/2009
TEST,TEST	09/19/1977		ISP Firearms Section	Closed	09/16/2009
TEST,TEST	09/19/1977		ISP Firearms Section	Closed	09/16/2009
TEST,TEST	09/19/1977		ISP Firearms Section	Closed	09/16/2009
TEST,TEST	09/19/1977		ISP Firearms Section	Closed	09/16/2009

Figure 45: Administrative Web Portal – Applicant Search Results

The web portal provides only information about the transaction status and applicant data. No criminal record data is available.

4.5.5 Security

The FBI and the State have computer security requirements, including connection to the internet by any computer connected to State local area networks or mainframe system. The successful Vendor, including employees and subcontractors working on this project, will be required to comply with current CJIS and National Crime Prevention and Privacy Compact Council Security requirements and policies throughout the duration of this contract award and will sign appropriate agreements and abide by these security requirements.

The successful Vendor personnel, including employees and subcontractors assigned to this project or performing activities related to this project must be approved by the West Virginia State Police.

All software and hardware systems utilized by the Vendor in the performance of this contract must be secured to prevent unauthorized access. The Vendor must provide the State with its IT Security Policy. This policy must encompass all industry standard security measures to ensure access to personal and financial information and systems is limited to those personnel requiring access to perform the duties necessary to accomplish this contract. At a minimum, the IT Security Policy must address:

- Physical security
- Access security
- Monitoring and auditing capability
- Data encryption
- Internet security
- Communication security
- Intrusion protection
- Virus protection

The personal information obtained from Applicants will not be utilized in any way by the Vendor outside of the performance of this contract. Information obtained from the Applicant cannot be resold, disseminated to any entity, business, or individual. The contractor will be required to sign a nondisclosure agreement. This agreement is contained in Appendix B.

The Vendor must provide the State with its Personal Data Privacy Policy.

MorphoTrust meets the requirements.

In our response to requirement 4.4.4.3, we have described our approach to security including logical access, personnel security, physical security, and network security.

In addition, Appendix A provides the following MorphoTrust policies:

- ***Privacy Policy (POL-00144-A)*** – Describes our policies for safeguarding the private information of our customer's citizens (Personal Data Privacy Policy).
- ***Cyber Security Plan (PLN-00091-A-02)*** – Describes our policies for ensuring the security and protection of the sensitive data and the information systems that transmit or store the data from cyber-attacks (IT Security Policy).

MorphoTrust will not use the personal information obtained from applicants in any way outside of the performance of this contract.

We meet all documented Information Security program requirements. We are experienced with both Federal Security Authorization (SA) processes and State government audits. We have a strong record of designing and building fully FISMA-compliant security controls. Moreover, our history also demonstrates our ability to identify, analyze and close findings to remain compliant with FISMA and Department of Homeland Security requirements.

The scope of MorphoTrust information security program includes information systems and technologies, personnel security, physical and environmental security for facilities that house our information systems, and business process security. We employ a team of information system security engineers who are knowledgeable and experienced in delivering FISMA-compliant security programs.

MorphoTrust's Unique Security Mandate

MorphoTrust is one of a rare few companies governed by U.S. Proxy and National Security Agreements and is mandated to follow the highest standards of security to protect all personally identifiable information.

We may employ and subcontract with only U.S. citizens who are thoroughly vetted and have successfully passed a background check, drug test, financial review, and security threat assessment.

We include SA requirements from our conceptual system design forward. Our Risk Management Framework includes the full NIST workflow consisting of the following processes: System Categorization, Selection of Security Controls, Implementation of Security Controls, Assessment of Security Controls, System Authorization, and Monitoring of Security Controls.

Security Awareness Training is a key component of NIST/FISMA information security controls, and MorphoTrust conducts information security awareness training for all employees who serve our biometric enrollment customers. We work to mitigate the threat of social engineering by requiring social engineering training for each employee when they join the company, and annually thereafter. Additionally, we conduct unannounced social engineering awareness exercises throughout each calendar year for all biometric services employees. We also have strict annual security awareness training requirements imposed upon us by the U.S. Federal Government as a result of our federal contracts.

The security and integrity of our network solutions, including all components, data transmissions, and physical facilities are of the utmost importance to MorphoTrust. We understand the critical importance of protecting all personal and financial information of our customers. As such, we provide industry standard security measures throughout our network solution to protect this sensitive information and infrastructure to ensure that only those persons needing access to the information have it, and when they do, that each access is controlled and logged appropriately.

All MorphoTrust staff and subcontractors assigned to or performing duties related to this project will be submitted for approval by WVSP and we will provide a signed nondisclosure agreement to the State.

4.5.6 Reports

The Vendor will be required to develop a number a standard and ad-hoc reports for use in reconciliation and other program objectives. These reports must be available for the State and User Agencies to access via a secure web site using a Vendor-assigned user name and password. The State will work with the Vendor to identify required data elements for each report. The Vendor will provide the database structure of the store and forward server.

At a minimum, the Vendor will be required to produce the following reports:

a) Monthly/Annual Summary

b) Monthly/Annual Detail

c) Fee Collection/Billing Reconciliation (for State access only)

d) Ad-hoc Reports - 5 free reports to be developed at the mutual agreement of Vendor and the State.

Vendor must provide screen shot samples of each report listed above which have had any actual Applicant data sanitized from view or replaced with fictitious data.

MorphoTrust meets the requirements.

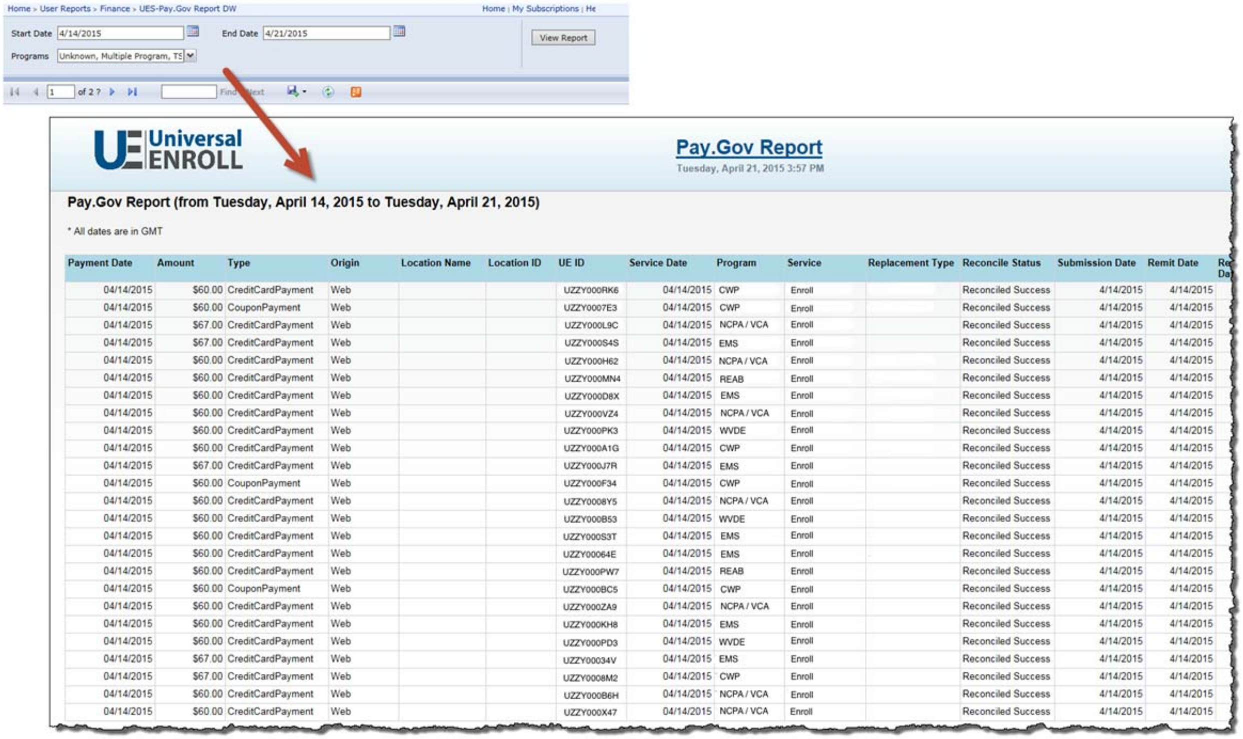
We produce a variety of reports for our customers using any of the data elements collected during the appointment scheduling process and encompassing any date range. These reports are available in real time to the State via a secure extranet reporting module. Authorized users can generate reports using a number of parameters, such as date range, applicant type, status, employer and name. All reports available through the extranet module can be viewed, printed or downloaded in a spreadsheet format.

At a minimum, we will work with the State of West Virginia to develop monthly and annual summary reports, monthly and annual detail reports, fee collection and reconciliation reports and ad-hoc reports, as needed.

We have described our billing system and reports in our response to requirement 4.4.5 and have provided screen captures of Monthly/Annual Summary, Monthly/Annual Detail, and Fee Collection/Billing Reconciliation reports in Figure 24 through Figure 28 on pages 68 – 70. The screen captures were sanitized to remove applicant data.

MorphoTrust will develop five additional reports as required. We leverage Microsoft's SQL Server Reporting Services (SSRS) for report generation and delivery services. The SSRS database server is deployed in a cluster, which allows for continuous operation when any one node in the cluster either fails or is taken offline for maintenance.

The following Figure 46 shows the ad-hoc search capability used to produce reports in real time.


Home > User Reports > Finance > UES-Pay.Gov Report DW
Home | My Subscriptions | He
View Report
1 of 2 ?
Find Next
Universal ENROLL

Start Date 4/14/2015
End Date 4/21/2015
Programs Unknown, Multiple Program, TS

Pay.Gov Report
Tuesday, April 21, 2015 3:57 PM

Pay.Gov Report (from Tuesday, April 14, 2015 to Tuesday, April 21, 2015)

* All dates are in GMT

Payment Date	Amount	Type	Origin	Location Name	Location ID	UE ID	Service Date	Program	Service	Replacement Type	Reconcile Status	Submission Date	Remit Date	Re Da
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000RK6	04/14/2015	CWP	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CouponPayment	Web			UZZY0007E3	04/14/2015	CWP	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$67.00	CreditCardPayment	Web			UZZY000L9C	04/14/2015	NCPA / VCA	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$67.00	CreditCardPayment	Web			UZZY000S4S	04/14/2015	EMS	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000H62	04/14/2015	NCPA / VCA	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000MN4	04/14/2015	REAB	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000D8X	04/14/2015	EMS	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000VZ4	04/14/2015	NCPA / VCA	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000PK3	04/14/2015	WVDE	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000A1G	04/14/2015	CWP	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$67.00	CreditCardPayment	Web			UZZY000J7R	04/14/2015	EMS	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CouponPayment	Web			UZZY000F34	04/14/2015	CWP	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY0008Y5	04/14/2015	NCPA / VCA	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000B53	04/14/2015	WVDE	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000S3T	04/14/2015	EMS	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY00064E	04/14/2015	EMS	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000PW7	04/14/2015	REAB	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CouponPayment	Web			UZZY000BC5	04/14/2015	CWP	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000ZA9	04/14/2015	NCPA / VCA	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000KH8	04/14/2015	EMS	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000PD3	04/14/2015	WVDE	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$67.00	CreditCardPayment	Web			UZZY00034V	04/14/2015	EMS	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$67.00	CreditCardPayment	Web			UZZY0008M2	04/14/2015	CWP	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000B6H	04/14/2015	NCPA / VCA	Enroll		Reconciled Success	4/14/2015	4/14/2015	
04/14/2015	$60.00	CreditCardPayment	Web			UZZY000X47	04/14/2015	NCPA / VCA	Enroll		Reconciled Success	4/14/2015	4/14/2015	

Figure 46: Ad-Hoc Search Capability

4.5.7 Billing

a) Fee Structure

The Vendor will be responsible for collecting the entire Applicant fingerprinting fee from either the Applicant or the Applicant's sponsoring agency/business. The fee is comprised of:

State fee: $20.00

State Authorized Central Abuse Fee, if applicable: $10.00

FBI fee: $14.75

FBINCPA/VCA Volunteer fee: $13.50

NCPANCA State fee: $10.00

Vendor Electronic Rolling/Submission fee: TBD

Vendor Manual Rolling Fee: TBD

Vendor Card Conversion/Submission Fee: TBD

Any invalid fees collected by the contractor, i.e., bad checks, credit cards, etc., resulting in non-payment are the sole responsibility of the Vendor

MorphoTrust meets the requirements.

MorphoTrust will collect the appropriate fee for each applicant either from the applicants themselves or from the sponsoring agency, where applicable. We will be responsible for any monies resulting from bad checks or credit cards. Checks will be remotely deposited on the day of service but will be subject to a hold of up to five days to ensure valid payment prior to record submission.

b) Reconciliation

The Vendor and the State shall reconcile billing on a monthly basis. All billing reconciliation shall be based upon the successful transmission of an Applicant fingerprint transaction from the contractor to the State. The State will bill the contractor for Applicants fingerprinted at all sites on a monthly basis. The Vendor shall make payment to the State for all applicable State and Federal fees within 30 days of receipt of the bill unless a discrepancy is noted. If the Vendor detects a discrepancy, the State must be notified within five (5) days.

MorphoTrust meets the requirements.

We will adhere to the reconciliation process established by the State to ensure that monthly payments are remitted to the State within 30 days of the receipt of the bill. If a discrepancy is noted during the reconciliation process, we will notify the State within five (5) days.

We have provided additional details about our billing system in our response to requirement 4.4.5.1.

c) Account Establishment and Funding

The Vendor must provide user agencies with the option to establish a customer account for payment of user agency Applicants' fees. State Agency accounts must be in the form of billing accounts where the agency is billed at the end of the month for all activity on their account for that month. All other user agencies must be able to establish escrow accounts that allow their Applicants to be charged against a balance maintained in the account and/or be permitted to establish credit accounts. If a user agency does not maintain a balance in their account, or fails to maintain a current credit account, the Vendor may refuse to allow Applicants to be scheduled against the account or to continue to offer the agency credit. Vendor may provide credit account to non-governmental agencies.

MorphoTrust meets the requirements.

We will provide monthly invoicing for state or local governmental agencies and provide solutions for non-governmental entities that will enable them to pay on behalf of applicants via credit-card backed accounts. Each agency with an account will receive a monthly itemized statement that details Payment Date, Fees, Location, Last Name, UEID (Enrollment ID number), Service Date, & Authorization Code (unique one-time use code). In addition, all billing accounts customers will have access to MorphoTrust’s Billing Account Portal for the purpose of managing code distribution, verifying redemption, and reconciliation reporting.

MorphoTrust has proven processes that we currently follow to manage more than 5,000 customer billing accounts in multiple fingerprinting programs.

4.5.8 Maintenance

a) Equipment and Software

Describe the maintenance levels that will be provided for each of the elements of the network, including how the State would request maintenance and what the Vendor will do to mitigate disruption of service to the Applicants.

MorphoTrust meets the requirements.

MorphoTrust addresses maintenance of all systems at several levels: Enrollment Agent, Technical Help Desk, and Field Service Engineering. The State may initiate maintenance requests by calling our toll free Customer Service Center.

Our Technical Help Desk employs trained, experienced technicians that provide technical support for Enrollment Agents in the field as well as support for state agencies for issues such as web-based scheduling support, server issues, fingerprint transmissions, etc. In addition, we maintain a team of certified Field Service Engineers (FSEs), who are dispatched if a service visit is required.

We minimize disruption to customers, both state users and applicants, by planning maintenance to ensure downtime windows are as small as possible, by providing visibility into the planned maintenance schedule, and by robustly communicating when emergency maintenance or system failures occur.

If necessary, the State may escalate an issue according to our Issue Escalation Procedure described on page 85.

We have provided additional details about equipment and software maintenance in our response to requirement 4.4.8.1 through 4.4.8.3.

b) Response Time

Describe the expected response time for maintenance for each element of the services infrastructure, i.e. live scan failure, server downtime, web site disruption of service, etc.

MorphoTrust meets the requirements.

Table 16 summarizes the expected maintenance response activities and duration for our current solution and UEP. Approximately 80% of trouble tickets are resolved in under half an hour.

Table 16: Maintenance Response Times

Infrastructure Element	Action	Response Time	Impact
Live Scan Failure	Enrollment Agent conducts onsite troubleshooting	5-15 minutes	Wait time
	Field Service Engineer dials in to perform further troubleshooting	5 min-1 hour	Wait time or reschedule appointment
	Equipment is replaced	Next day start of business	Reschedule appointment - affected applicants contacted to reschedule
Server Downtime	Immediate trouble ticket issued and resources released to address issue as Top Priority	5-15 minutes	No disruption to enrollment customers – records queued on Livescan for submission when lines are re-established
Website disruption of service	Immediate trouble ticket issued and resources released to address issue as Top Priority	5-15 minutes	Applicants cannot pre-register online, but Enrollment Centers are operational on a walk-in basis and the Customer Service Center is available to provide directions to Enrollment Centers and answer questions
Communication lines disruption of service	Immediate trouble ticket issued and resources released to address issue as Top Priority	5-15 minutes	No disruption to customers – records queued on Livescan for submission when lines are re-established

We have provided additional detail in our response to requirement 4.4.8.2.

c) Call Escalation List

Provide a call escalation procedure with the name, title, area of responsibility and phone number for each level starting with the state program manager up to the top official in the company.

MorphoTrust meets the requirements.

4.4.8.3 The Vendor should describe in detail the call escalation procedure with the name, title, area of responsibility and phone number for each level starting with the state program manager up to the top official in the company.

All significant issues should be reported directly to the Program Manager for the West Virginia Applicant Fingerprinting Services program, Denny Wear. Mr. Wear's contact information is:

Denny Wear
Director – Program Management
Office phone: (217) 547-2116
Cell phone: (615) 946-7947
dwear@morphotrust.com

In the unlikely event that a problem must be escalated, it should be reported to Mr. Wear's supervisor, Kent Schmitt. Mr. Schmitt's contact information is:

Kent Schmitt
Program Executive
Office Phone: (202) 688-4826
Cell Phone: (615) 347-4627
kschmitt@morphoTrust.com

In the unlikely event that a problem must be escalated, it should be reported to Mr. Schmitt's supervisor, Charles Carroll. Mr. Carroll's contact information is:

Charles Carroll
Senior Vice-President
Office Phone: (615) 778-5752
Cell Phone: (937) 604-6595
ccarroll@morphoTrust.com

4.5.9 Project Management

a) The successful Vendor is required to assign an experienced and skilled project manager to the project. The Vendor's project manager will be responsible for the compilation of the project plan and will be required to maintain the detailed plan through .the full term of the project or until such time the Vendor has completed the contract obligation.

Vendor must provide a project manager to act as the primary contact with the State.

MorphoTrust meets the requirements.

Responsibility for MorphoTrust's project management and plan resides with the Program Manager, Denny Wear. Mr. Wear is empowered to make decisions and commitments on behalf of MorphoTrust and communicate those decisions and commitments to the designated representative of the state of West Virginia. He will be responsible for the project management and tracking the progress of each defined task, maintaining the project schedule, identifying any potential problem areas or risks, and communicating all of the activity status with the State's Contract Manager and Agency Program Managers.

MorphoTrust Program Manager
Denny Wear

Denny Wear has been MorphoTrust's Program Manager for the West Virginia fingerprinting network for more than two years.

The State of West Virginia will benefit from his knowledge of your fingerprinting network and his relationship with the West Virginia State Police, agencies, and applicants as he continues to serve as the primary point of contact for our performance in support of this contract.

Mr. Wear is responsible for compiling a detailed project plan and maintaining it through the full term of the project. We have provided a preliminary project schedule in Appendix B.

Mr. Wear has more than 15 years of skills and experience developed through involvement with numerous fingerprinting service programs. He has been instrumental in the successful deployment of large-scale statewide fingerprint networks including Massachusetts, the District of Columbia, New York, and Indiana, as well major expansion of the Florida statewide network and a fingerprint and identification badging solution for Broward County, Florida School Board, the nation's sixth largest school system.

We have provided more information about his qualifications and the qualifications of our proposed project team in our response to requirement 4.3.

b) The project plan will be required to contain, at a minimum, the following components; stakeholder register, communication management, budget management, issue management, change management, risk management, and a detailed schedule that includes a detailed description of the task, the type of resources need for the task, start date, end date and any task dependencies (predecessors or successors). The Vendor's project manager will also be required to develop a staffing plan. The Vendor's project manager will be required to submit an updated work plan at a frequency that is agreed upon and is documented in the communication plan.

Lowest Implementation Risk

As noted in our RFP response, we have significant infrastructure and proven processes in place that lower our implementation risk and reduce the timeline necessary to complete an implementation.

For example, we will utilize our existing Customer Service Centers, web scheduling software, FBI-certified Livescan hardware and servers, secure Data Centers, and reporting and tracking tools for this project.

Based on the requirements of the RFP and feedback obtained during implementation meetings, we will tailor these assets to meet the needs of WVSP and User Agencies—***but none of these assets will need to be developed from scratch***.

MorphoTrust meets the requirements.

Based on our past experience and the detailed project planning we have already completed specific to this RFP, we are confident of successfully implementing our proposed West Virginia network in accordance with the RFP requirement 90 days from contract award, provided there are no significant delays during the contract execution process. In fact, our implementation plan has sufficient cushion built into all tasks to offset unexpected delays. Within 45 days of contract award, we will deliver the formal project plan and staffing plan, which will include all the elements required by this RFP.

MorphoTrust has successfully implemented multiple statewide networks of similar size and scope within the timeframe required by this RFP. Examples of several such implementations are included in Table 2 on page 11. We have provided a preliminary project schedule in Appendix B that outlines the steps we will follow to achieve the program objectives.

Program Management Approach

Large-scale, mission-critical programs such as a statewide fingerprinting network require a disciplined project management approach to balance service delivery with risk mitigation. We provide the right management approach, a carefully selected and experienced leadership team, and existing infrastructure to achieve project objectives.

Program management is a MorphoTrust core competency and we have used our expertise to successfully implement 26 large-scale applicant fingerprinting networks. The objective of our program management plan is to provide a structure that enables the lowest risk implementation of the network.

We use the following Management Areas:

- Integration & Scope Management
    - Execute Configuration Management
    - Develop and maintain requirements traceability
    - Maintain an Integrated Master Plan and control metrics
- Communications Management
    - Conduct stakeholder outreach, issue management, and change management programs
    - Execute progress reviews and status reporting
- Time & Cost Management
    - Define, according to the MS Project Plan, all the necessary activities scheduling and its change management procedures
    - Develop time and cost baselines based on the MS Project Plan
    - Maintain project budget procedures
    - Monitor and measure progress to assure the project finishes on time and on budget
- Risk Management
    - Identify, Assess, Mitigate, and Monitor risks on an ongoing basis
    - Escalate issues when necessary
- Quality Management
    - Monitor project control metrics and Quality Assurance Surveillance Plan (QASP)
- Human Resources Management
    - Attract and retain the right people to facilitate project continuity and success
    - Utilize proven training courses customized for WVSP requirements
    - Manage personnel security

    - Maintain personnel database of all WVSP program participants with clearance status
    - Cross-train people to mitigate critical resource dependencies
- Procurement Management
    - Provide open, fair, and competitive processes to deliver best value to the WVSP program
    - Manage contract commitments to closure

We complement our methodology and assets with our experience in delivering superior Program Management services to our clients in time, on budget, and with a high level of responsiveness to Stakeholder needs.

Concept of Operations Document

As a component of our project management, we develop a Concept of Operations (ConOps) document, which provides detailed information about how contingencies will be dealt with. MorphoTrust proposes to support the business continuity requirements using a hot-standby, alternate Data Center. As part of our internal information assurance program, a contingency plan is created to address the specific mission needs and recovery requirements. The central component of this contingency plan is a Concept of Operations (ConOps) document. This document describes roles and responsibilities, system requirements, data requirements, and the overall process of detections, response, and recovery. The contingency plan is exercised in its entirety annually, and a tabletop exercise is conducted biannually.

The ConOps broadly addresses three areas of concern – management, operational, and technical:

- The ***management*** aspect of the ConOps defines several key individuals charged with the execution of the plan. At a minimum, executive management owner, contingency plan coordinator, damage assessment coordinator, information systems coordinator, operations and logistics coordinator, and security coordinator will be assigned.
- The ***operational*** aspect of the ConOps reflects the execution of the plan insofar as remote sites and the operational IT environment are involved. This component requires detailed documentation relative to the operational procedures, checklists, and contact information required for successful continuity of operations.
- The ***technical*** aspect covers the information and data flows, the mechanism used for real-time data replication between primary and hot-standby facilities, and the methods for recovery of mid-transaction

submissions. Each of these areas of concern is thoroughly addressed and reviewed by both management and the information systems security officer for completeness.

Risk Management Plan

MorphoTrust's risk mitigation plan has been developed and refined over many years in response to risks that we have identified during both normal operations and exceptional circumstances. For each risk, we have identified the likelihood and potential impact of the risk and implemented a response that appropriately addresses risk levels in an efficient manner. In the course of capturing over 21 million fingerprint records, our system has demonstrated up-time in excess of 99% and performed reliably with a high degree of customer satisfaction.

MorphoTrust's risk management program is a customized capability based on the National Institute of Standards and Technology (NIST) Special Publication 800 Series. The program we use is mission-centric, focusing on the customer delivery and mapping those capabilities to the supporting IT systems. Our program examines both qualitative and quantitative aspects of risk management at each step of the process. So, while the NIST publications were developed for federal use, they have provide a solid foundation upon which MorphoTrust has built a robust, thorough risk management capability.

The risk identification aspect of the overall risk program uses threat-sources as the means by which specific risks may be identified. At its highest level, the risk management program considers human, system, natural, and environmental risks. Each of these four categories is then systematically analyzed with respect to technical or non-technical risks and intentional or unintentional actions.

Human and system risks are concerned with actions taken by people or actions taken by systems as a result of human action. Examples of human risks are social engineering, theft, or device misconfiguration. System risks include viruses, worms, or even misbehaving devices. These risks are identified through the use of internal resources (risk meetings, internal security audits, previous risk assessments, etc.) and external resources (NIST SP 800 Series, FedCIRC, CERT, SANS, ISC2, etc.). Some of the risk identification tools are used both internally and externally (network scanners, penetration testing, configuration analysis tools, etc.).

Natural risks relate to so-called Acts of Nature. They include occurrences such as floods, earthquakes, fires, pandemic flu, and the like. The identification of these risks also requires internal and external analysis. Internally, MorphoTrust is able to review previous exposures to natural risks and is prompted by our internal risk management program to review each of the most common natural risks. External analysis includes the usage of risk resources provided by local, state, and federal agencies. Examples of external resources are the Emergency Management Agencies, National Oceanic and Atmospheric Administration, or the United States Geological Survey.

Environmental risk related to the facilities which support the business mission. Environmental risks are generally well-known and readily identified. Examples include loss of electricity, water main leak, failure of HVAC systems, and failure of physical access control systems. These risks are updated as experience, both corporate or industry, dictates. To be sure, the existing risk management program covers a detailed list of environmental risks.

The MorphoTrust risk management program characterizes likelihood of occurrence as the Annual Rate of Occurrence (ARO). This ARO value is later used in determining the appropriate risk response. The ARO for any given risk may be analyzed quantitatively and/or qualitatively.

Quantitative evaluations consider the ARO on the basis of internal and external data sets. Internally, MorphoTrust tracks previous risk exposures and what, if any, attempts were made to exploit those risks. These data points provide useful, quantitative information on likelihood of occurrence. Externally, MorphoTrust utilizes local, state, and federal resources that can provide Standard Annual Frequency Estimates (SAFE) and Local Annual Frequency Estimates (LAFE). These estimates come from organizations like NOAA and the USGS. While all four risk categories are considered in the quantitative analysis, natural and environmental risks are most frequently represented in the quantitative analysis.

Qualitative evaluations require a textual rubric describing the threat-source, its motivations/conditions, and its capabilities to exploit a particular risk. Many threats are necessarily qualitative owing to the newness of the risk posed. The MorphoTrust risk management program groups qualitative risks into High, Medium, and Low likelihood of occurrence. Each risk is then evaluated on the basis of these buckets. Internal analysis includes reviews of system controls and historical performance of the organization in maintaining mission capabilities. Externally, organizations like SANS, CERT, and FedCIRC provide technical data regarding likelihoods. While all four risk categories are considered in the qualitative analysis, human and system risks are most frequently represented in the qualitative analysis.

Potential impact data is quantified using a structured process that calculates dollar impact of a threat-source exploiting a vulnerability. This analysis is concrete, which requires the conversion of qualitative data to a relative, numerically-defined scale. Quantitative data sets are then normalized into this same scale. Using internally derived dollar values, a Single Loss Expectancy (SLE) is determined. This SLE considers mission impact (e.g., the ability for the program to continue in the face of media scrutiny), business impact (e.g., service level requirements or contractual penalties), and system impact (e.g., the cost to replace hardware components).

Once the SLE is determined, the ARO for the given risk is considered. The outcome of the SLE and ARO calculation is an Annual Loss Expectancy (ALE). The ALE is the final output of the activities around quantifying impact. It represents the cost associated with the realization or actualization of a given risk.

As part of the on-going security program, action plans are developed, maintained, updated, and reviewed. The plans and durations are based on residual risk. Residual risk is calculated using the ALE and is the determination of the amount of risk that remains when a risk is considered in the context of existing counter-measures, controls, and protections.

For each risk, a determination is made whether to accept, mitigate, or transfer the risk. MorphoTrust does not ignore risks or their associated residual risks. In cases where the cost impact of the risk is less than the cost of mitigation, the risk is noted to the risk program, reviewed by management, and monitored by the information systems security officer. In cases where the cost impact of the risk is greater than the cost of mitigation, MorphoTrust takes the necessary steps to implement the mitigations such that the new risk profile is acceptable. Finally, MorphoTrust may elect to transfer risk within the parameters outlined by contract. For example, MorphoTrust may elect to contract with a Call Center provider who would be responsible for continuity planning relative to that specific mission capability.

Issue Management

All significant issues should be reported directly to the Program Manager, Denny Wear. Mr. Wear’s contact information is:

Denny Wear
Director – Program Management
Office phone: (217) 547-2116
Cell phone: (615) 946-7947
dwear@morphotrust.com

In the unlikely event that a problem must be escalated, it should be reported to Mr. Wear’s supervisor, Kent Schmitt. Mr. Schmitt’s contact information is:

Kent Schmitt
Program Executive
Office Phone: (202) 688-4826
Cell Phone: (615) 347-4627
kschmitt@morphoTrust.com

In the unlikely event that a problem must be escalated, it should be reported to Mr. Schmitt's supervisor, Charles Carroll. Mr. Carroll's contact information is:

Charles Carroll
Senior Vice-President
Office Phone: (615) 778-5752
Cell Phone: (937) 604-6595
ccarroll@morphoTrust.com

Most day-to-day operational issues would typically be escalated in the following manner:

- ***Step One*** – Most problems should be reported to our toll free Customer Service Center which will be open 7:00 A.M - 4:00 P.M. CST Monday through Friday. All Customer Service Representatives assigned to this program will have a thorough knowledge of the program.
- ***Step Two*** - Problems that cannot be solved or addressed by a Customer Service Representative are forwarded to the West Virginia Customer Service Supervisor or our Technical Support Center for resolution.
- ***Step Three*** – Problems that cannot be solved or addressed by the Customer Service Supervisor or Technical Support will be forwarded to the Operations Manager.
- ***Step Four*** – If a problem cannot be solved by the Operations Manager, the issue will be escalated to the Project Manager, Denny Wear. Mr. Wear's contact information is included above.
- ***Step Five*** - In the unlikely event that a problem must be escalated above the Project Manager level, the Program Executive, Kent Schmitt, should be contacted. Mr. Schmitt's contact information is included above.
- ***Step Six*** - In the unlikely event that a problem must be escalated above the Program Executive level, the Senior Vice-President, Charles Carroll, should be contacted. Mr. Carroll's contact information is included above.

c) The Vendor's project manager is required to deliver the project plan and staffing plan within 45 days after the award. The Vendor's Project Manager will be responsible for the successful completion of all work tasks and deliverables as defined within the project plan within another 45 days for a total of 90 days after award.

MorphoTrust meets the requirements.

Our Project Manager will deliver the required project and staffing plans to the State within 45 days of award. The initial version of the project plan will be refined in consultation with the State and all work tasks and deliverables will be in place and fully operational within 90 days after award.

d) The Vendor's Project Manager will be required to plan for and conduct status meetings on a periodic and as needed basis to discuss current project activities and address questions, issues, and concerns. A written status report for high level executives will be required. The status report submission frequency is required to be included in the communication plan. This status report is required to include, at a minimum, a health indicator for budget, scope and schedule along with reporting period accomplishments, issues and upcoming action items.

MorphoTrust meets the requirements.

Our Project Manager will conduct regular and as needed status meetings with representatives of the State as a forum to discuss project activities and to address any questions, issues or concerns about the program. As an element of these meetings, he will prepare a written report that will address all applicable topics, including a health indicator for budget, scope and schedule, accomplishments, issues and action items as well as any additional features required by the State. The communication plan will include the frequency for submitting this report.

e) During the execution of the project, the Vendor's project manager will be required to maintain an issue log, risk log, change log, lessons learned, deliverable log, as well as the execution and management of the project plan.

MorphoTrust meets the requirements.

Our Project Manager will maintain a log tracking all risks identified, changes made and lessons learned. The log will also track the execution and management of the project plan to ensure that all tasks are performed successfully in a timely manner that meet all requirements of the project plan.

f) The Vendor's project manager will be required to conduct a session for post review of the project. The post review will contain at a minimum lessons learned, review of issues, review of risks, and review of project team performance.

MorphoTrust meets the requirements.

Our Project Manager will conduct a post review of the project that will contain at a minimum lessons learned, a review of issues that arose throughout the course of the project, the risks identified, and how the team performed the required tasks.

g) The Vendor's project manager will be required to ensure that accreditation and certification is performed during the closing of the project. Accreditation and certification can be done at the end of each phase of the project.

MorphoTrust meets the requirements.

Our Project Manager will be responsible for performing accreditation and certification during the closing of the project.

h) The Vendor's project Manager is expected to effectively and efficiently work under the direction of the awarding agency while adhering to all governing policies, procedures and standards of each.

MorphoTrust meets the requirements.

Our Project Manager has a long history of effective cooperation with stakeholders and team members and we are confident that he will work well with West Virginia Department of Administration, Purchasing Division and WVSP.

This page intentionally left blank.

Appendix A – MorphoTrust IT Security Policy and Personal Data Privacy Policy

MorphoTrust considers our IT Security Policies and Personal Data Privacy Policies to be exempt from public disclosure. Therefore, we have segregated these policies from the rest of our proposal and submitted them in a separate volume entitled "EXEMPT INFORMATION."

The documents contained in MorphoTrust's Exempt Information volume contain highly sensitive security information and are not to be considered as public documents or disclosed to the public.

MorphoTrust has provided the following policies in our Exempt Information volume:

- ***MorphoTrust Privacy Policy POL-00144-A*** – Describes our policies for safeguarding the private information of our customer's citizens (Personal Data Privacy Policy).
- ***MorphoTrust USA Cyber Security Plan PLN-00091-A-02*** – Describes our policies for ensuring the security and protection of the sensitive data and the information systems that transmit or store the data from cyber-attacks (IT Security Policy).

In addition, we have provided the following relevant policies:

- Information Security Customer Data Access and Security Policy PRC-00174-A-07
- IT Backup Recovery PRC-00084-B-03

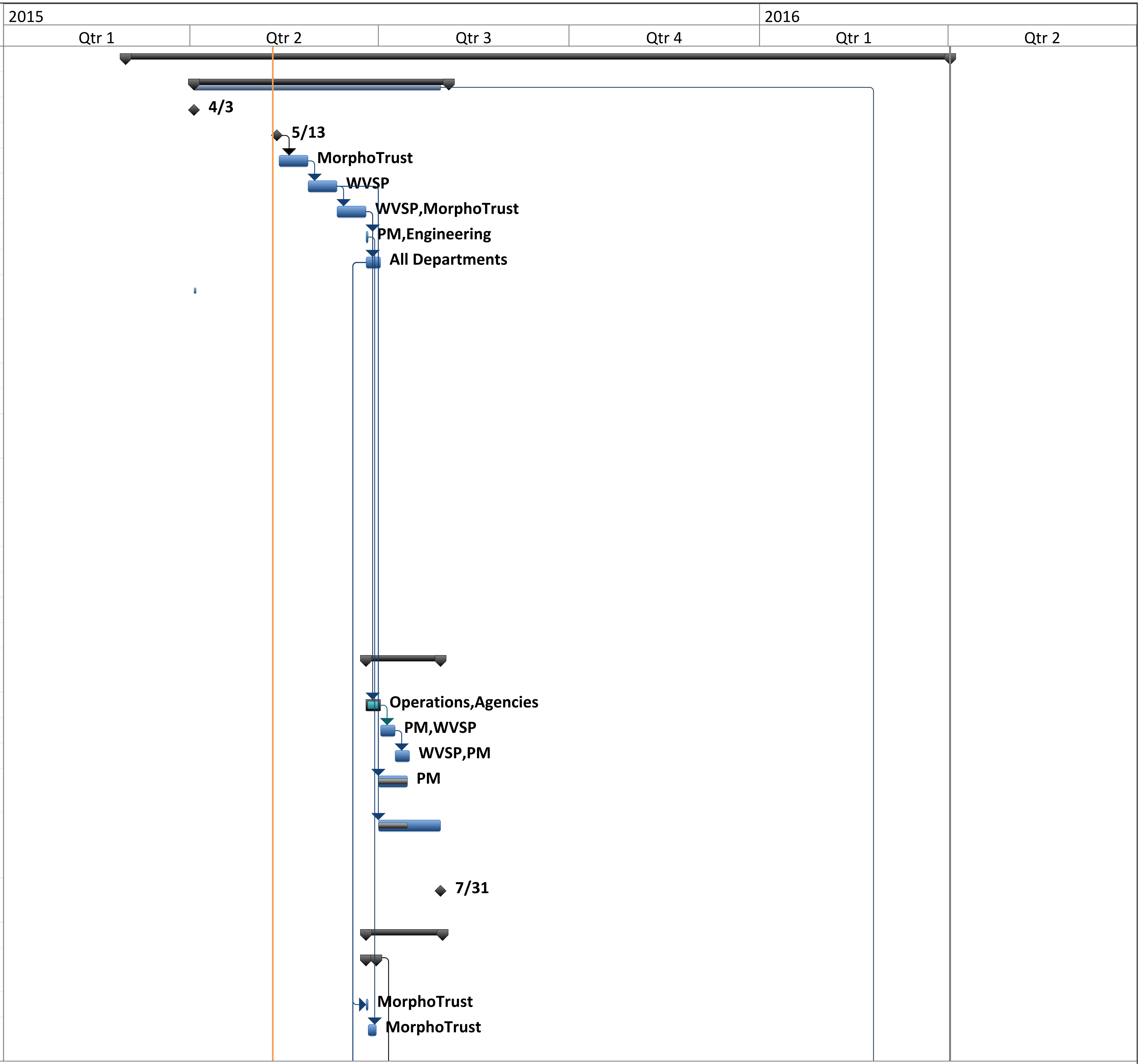
- IT Change Management Procedure PRC-00085-B-05
- IT Computer and System Use Procedures PRC-00110-A-10
- IT Computers on Network PRC-00086-B-01
- IT Disaster Recovery PRC-00095-B-02
- IT Electronic Communication Policy PRC-00113-A-02
- IT Firewall Policy PRC-00088-B-05
- IT Information Security PRC-00089-B-06
- IT Managing Operations PRC-00090-B-01
- IT Network Access Controls Procedures PRC-00091-B-02
- IT Physical IT Access Controls PRC-00091-B-01
- IT Remote Access PRC-00092-B-09
- IT Security Policy PRC-00112-A-03
- IT Sensitive Data Handling and Storage Procedures PRC-00148-A-05
- IT Virus Protection PRC-00093-B-01
- Removable Media Policy PRC-00150-A-01

Appendix B – Preliminary Project Schedule

MorphoTrust has provided our preliminary project schedule on the following pages.

This page intentionally left blank.

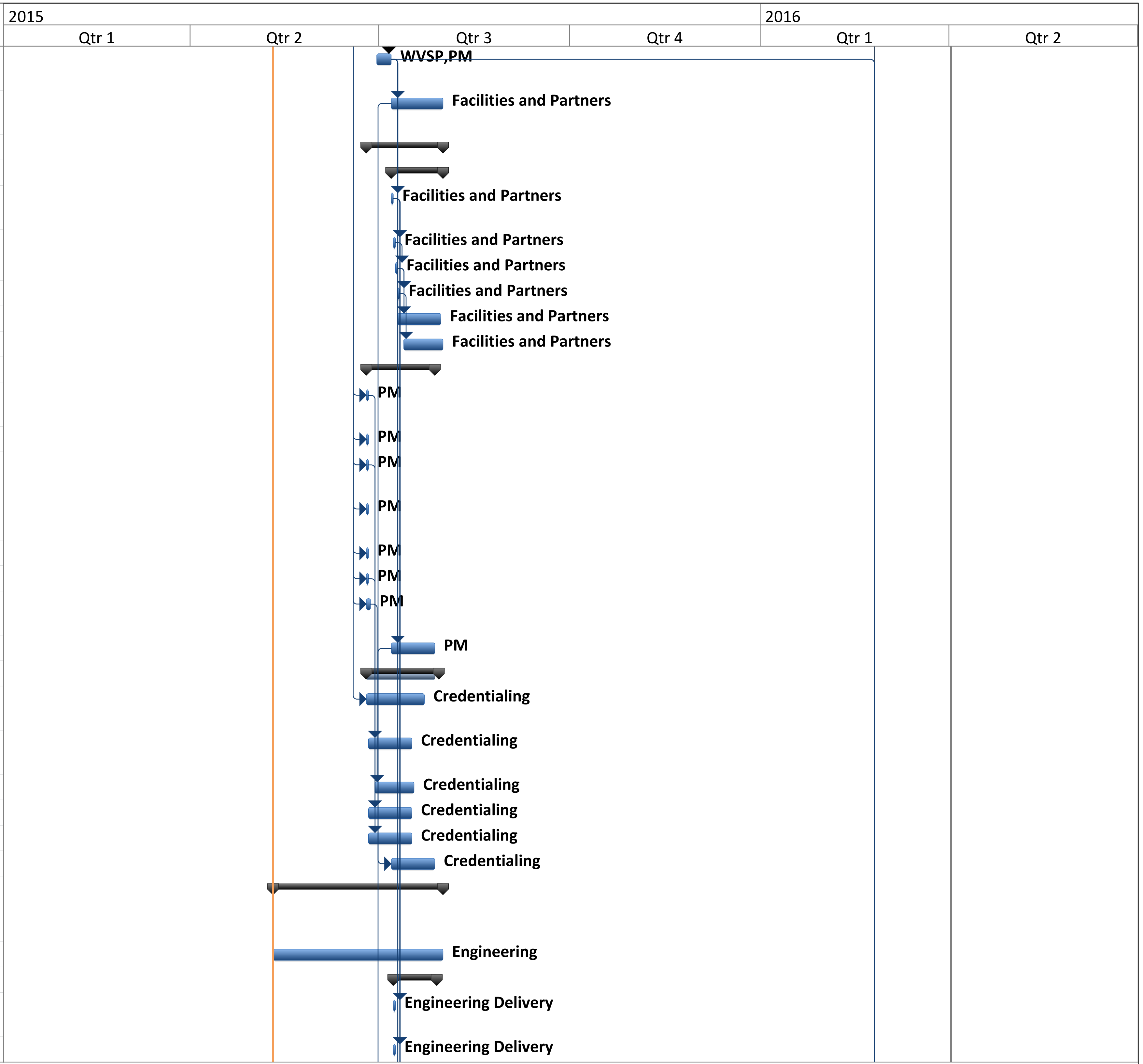
ID	Task Name	% Complete	Resource Names	Start
1	**West Virginia State Police, Applicant Fingerprinting Services**	**2%**		**Sun 3/1/15**
2	**PROJECT INITIALIZATION**	**22%**		**Fri 4/3/15**
3	RFP issue date	100%	WVSP	Fri 4/3/15
4	Submission of RFP Proposal	100%	MorphoTrust	Wed 5/13/15
5	Anticipated Oral Presentation	0%	MorphoTrust	Thu 5/14/15
6	Anticipated Contract Award to Chosen Vendor	0%	WVSP	Thu 5/28/15
7	Contract Signing Completed	0%	WVSP,MorphoTrust	Thu 6/11/15
8	**MorphoTrust Kickoff meeting with WV Stakeholders**	0%	PM,Engineering	Thu 6/25/15
9	MorphoTrust Internal Kickoff meeting	0%	All Departments	Thu 6/25/15
10	**MorphoTrust Internal WBS Planning/Status meetings - DATES TBD/ Meetings Scheduled As Needed**	**0%**		
11	Internal MorphoTrust Program Manager, Deployment Manager, and Project Manager	0%	Program Manager,Project	
12	Facilities and Partner Manager and team	0%	Facilities and Partners	
13	RFP Requirements Review	0%	WV Stakeholders	
14	MorphoTrust Internal IT/Hardware Procurement team	0%	Business Services	
15	MorphoTrust Internal IT/Registration System WorkStation Development Team	0%	Engineering Delivery	
16	MorphoTrust Internal IT/Registration System Reporting Development Team	0%	Engineering Delivery	
17	Call Center Team	0%	Call Center	
18	Training Team	0%	Training	
19	Finance Team	0%	Finance Dept.	
20	Field Service Engineering and Deployment Team	0%	Field Services	
21	**Communications to Agencies: Status, Schedule, Dependencies**	**44%**		**Thu 6/25/15**
22	Review Communication Plan with the Agencies	0%	Operations,Agencies	Thu 6/25/15
23	Prepare Notice and Information Packet for Agencies	0%	PM,WVSP	Thu 7/2/15
24	Send Notice and Information Packet to State Agencies	0%	WVSP,PM	Thu 7/9/15
25	Operational Toll Free number and Public Internet Website within 30 days of award	100%	PM	Wed 7/1/15
26	Operational Toll Free number, Call Center Services, and Public Internet Website within appointment scheduling capabilty within 60 days of award	50%		Wed 7/1/15
27	**All Current Enrollment Centers will remain operational by July 31, 2015.**	0%	PM	Fri 7/31/15
28	**Facility Location Selection**	**0%**		**Thu 6/25/15**
29	**Identify/Confirm Site Locations, Address, and Point of Contact for each site**	**0%**	**WVSP,PM**	**Thu 6/25/15**
30	Review of Current Active Enrollment Centers	0%	MorphoTrust	Thu 6/25/15
31	Additional sites: Present Expansion of Site List to Meet Requirements	0%	MorphoTrust	Fri 6/26/15



Project: West Virginia Applicant F
Date: Mon 5/11/15

Task	▬	Project Summary	▬	Inactive Milestone	◇	Manual Summary Rollup	▬	Deadline	⬇
Split	┈	External Tasks	▬	Inactive Summary	▭	Manual Summary	▬	Progress	▬
Milestone	◆	External Milestone	◆	Manual Task	▬	Start-only	[		
Summary	▬	Inactive Task	▭	Duration-only	▬	Finish-only	]		

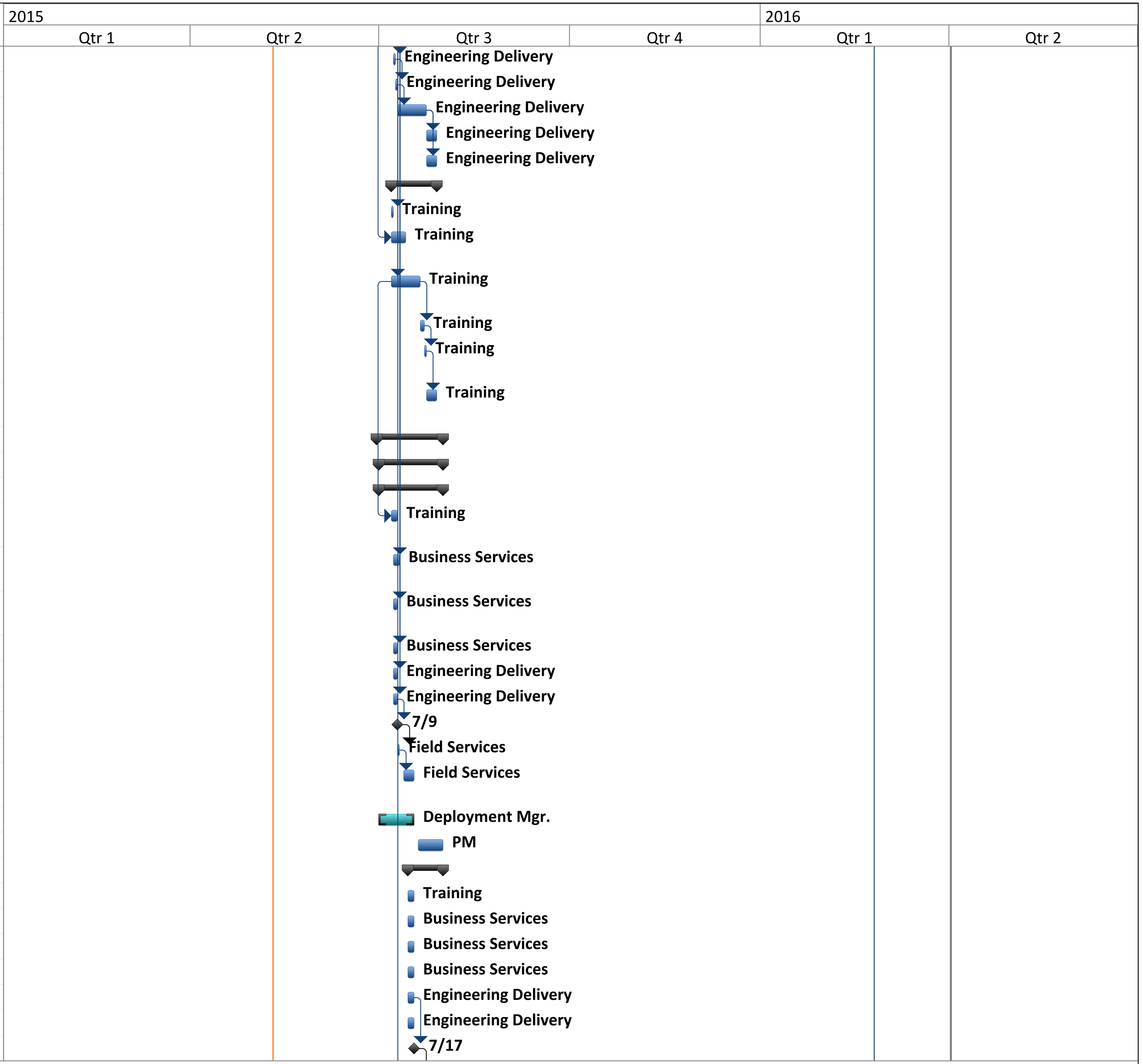
ID	Task Name	% Complete	Resource Names	Start
32	WVSP Approval of all Locations and Hours Of Operation (HOO)	0%	WVSP,PM	Tue 6/30/15
33	Secure Partner business - Agreement & Vetting for New Sites	0%	Facilities and Partners	Tue 7/7/15
34	**Resource Allocations**	**0%**		**Thu 6/25/15**
35	**Facilities**	**0%**		**Tue 7/7/15**
36	Determine Facility Status, Needs, and Requirements for additional sites	0%	Facilities and Partners	Tue 7/7/15
37	Publish Furniture and Fixture Bill of Material (BOM)	0%	Facilities and Partners	Wed 7/8/15
38	Order Furniture and Fixtures needed from BOM	0%	Facilities and Partners	Thu 7/9/15
39	Order Signage and Branding Material	0%	Facilities and Partners	Fri 7/10/15
40	Receive Furniture and Fixtures order	0%	Facilities and Partners	Fri 7/10/15
41	Receive Signage and Branding Material	0%	Facilities and Partners	Mon 7/13/15
42	**Personnel**	**0%**		**Thu 6/25/15**
43	Finalize List of MorphoTrust/WVSP Project Management Team	0%	PM	Thu 6/25/15
44	List Facilities and Partner Search Lead and Team	0%	PM	Thu 6/25/15
45	Assign MorphoTrust Internal Engineering Development Team	0%	PM	Thu 6/25/15
46	Assign Report Programmer Resource in Engineering Delivery	0%	PM	Thu 6/25/15
47	Assign the Team Lead for Finance	0%	PM	Thu 6/25/15
48	Assign the Team Lead for Call Center	0%	PM	Thu 6/25/15
49	Assign and Schedule Field Service Engineers (FSEs)/Trainers for Deployment	0%	PM	Thu 6/25/15
50	Identify/Secure/Hire new Enrollment Agents (EAs)	0%	PM	Tue 7/7/15
51	**Vetting of all New Team Members**	**0%**		**Thu 6/25/15**
52	Vet all New MorphoTrust employees with a WV fingerprint-based criminal background check.	0%	Credentialing	Thu 6/25/15
53	Vet New MorphoTrust Internal Engineering Development Team	0%	Credentialing	Fri 6/26/15
54	Vet New FSEs/Trainers	0%	Credentialing	Mon 6/29/15
55	Vet New MorphoTrust WV Team members	0%	Credentialing	Fri 6/26/15
56	Vet New Call Center Resource Persons	0%	Credentialing	Fri 6/26/15
57	Vet New EAs Hired and at Partner sites	0%	Credentialing	Tue 7/7/15
58	**PHASE 1 CURRENT ENVIRONMENT HARDWARE AND SOFTWARE IMPLEMENTATION AND DEPLOYMENT FOR 5 NEW SITES**	**0%**		**Mon 5/11/15**
59	Phase 1 Current Engineering Environment	0%	Engineering	Mon 5/11/15
60	**Livescan Hardware**	**0%**		**Wed 7/8/15**
61	Reserve necessary LiveScan equipment and Workstations in inventory.	0%	Engineering Delivery	Wed 7/8/15
62	Enrollment Center Bill Of Material (BOM)	0%	Engineering Delivery	Wed 7/8/15



Project: West Virginia Applicant F
Date: Mon 5/11/15

Task	▬	Project Summary	▬	Inactive Milestone	◇	Manual Summary Rollup	▬	Deadline	⬇
Split	┈	External Tasks	▬	Inactive Summary	▭	Manual Summary	▬	Progress	▬
Milestone	◆	External Milestone	◆	Manual Task	▬	Start-only	[		
Summary	▬	Inactive Task	▭	Duration-only	▬	Finish-only	]		

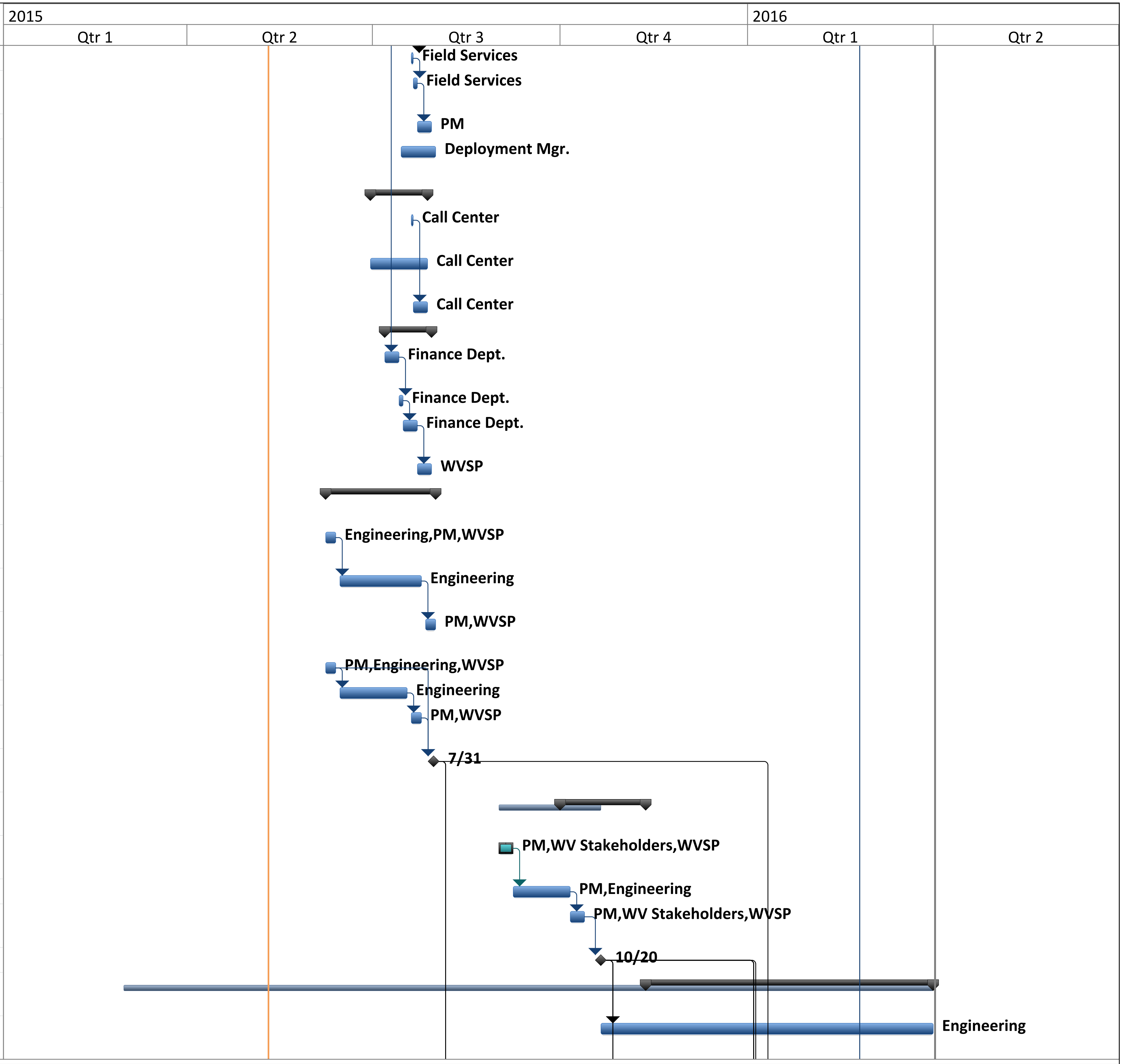
ID	Task Name	% Complete	Resource Names	Start
63	Mobile BOM (Hardware and Consumables)	0%	Engineering Delivery	Wed 7/8/15
64	Order additional Workstation Equipment	0%	Engineering Delivery	Thu 7/9/15
65	Workstation Received from Order	0%	Engineering Delivery	Fri 7/10/15
66	Prepare for shipping the Livescans	0%	Engineering Delivery	Fri 7/24/15
67	Prepare for shipping the Workstations	0%	Engineering Delivery	Fri 7/24/15
68	**Training**	**0%**		**Tue 7/7/15**
69	Identify the Training Coordinator	0%	Training	Tue 7/7/15
70	Site Development Schedule and Training of Staff - Draft Plan	0%	Training	Tue 7/7/15
71	Update Training Material: User manual, Quick Reference Guide, Training acknowledgement forms	0%	Training	Tue 7/7/15
72	Deliver Installation Guide	0%	Training	Tue 7/21/15
73	Schedule Train The Trainer: Schedule training session for the FSEs to provide the EA training	0%	Training	Thu 7/23/15
74	Provide Train The Trainer: Train the FSEs to provide the EA training	0%	Training	Fri 7/24/15
75	**Roll Out / Deployment**	**0%**		**Tue 6/30/15**
76	**Site List**	**0%**		**Wed 7/1/15**
77	**Current Site Preparation Plan and Schedule**	**0%**		**Wed 7/1/15**
78	Designated Sites: Ship Updated User Guides to Sites	0%	Training	Tue 7/7/15
79	Designated Sites: Ship Furniture and Fixtures if needed for a specific site	0%	Business Services	Wed 7/8/15
80	Designated Sites: Ship Signage and Branding Material	0%	Business Services	Wed 7/8/15
81	Designated Sites: Ship Consumables	0%	Business Services	Wed 7/8/15
82	Designated Sites: Ship Workstations	0%	Engineering Delivery	Wed 7/8/15
83	Designated Sites: Ship the LiveScans	0%	Engineering Delivery	Wed 7/8/15
84	Designated Sites: Equipment Received	0%	Field Services	Thu 7/9/15
85	Designated Sites: Installation of Workstation	0%	Field Services	Fri 7/10/15
86	Designated Sites: EA Training for Updated Equipment	0%	Field Services	Mon 7/13/15
87	Current Site Deployment	0%	Deployment Mgr.	Wed 7/1/15
88	Current Site HOO expansion if necessary	0%	PM	Mon 7/20/15
89	**New Site Preparation Plan and Schedule**	**0%**		**Wed 7/15/15**
90	Ship Training Material to Identified Sites	0%	Training	Wed 7/15/15
91	Ship Furniture and Fixtures	0%	Business Services	Wed 7/15/15
92	Ship Signage and Branding Material	0%	Business Services	Wed 7/15/15
93	Ship Consumables	0%	Business Services	Wed 7/15/15
94	Ship Workstations	0%	Engineering Delivery	Wed 7/15/15
95	Ship the LiveScans	0%	Engineering Delivery	Wed 7/15/15
96	Equipment Received	0%	Field Services	Fri 7/17/15



Project: West Virginia Applicant F
Date: Mon 5/11/15

Task	▬	Project Summary	▬	Inactive Milestone	◇	Manual Summary Rollup	▬	Deadline	⬇
Split	┈	External Tasks	▬	Inactive Summary	▭	Manual Summary	▬	Progress	▬
Milestone	◆	External Milestone	◆	Manual Task	▬	Start-only	[		
Summary	▬	Inactive Task	▭	Duration-only	▬	Finish-only	]		

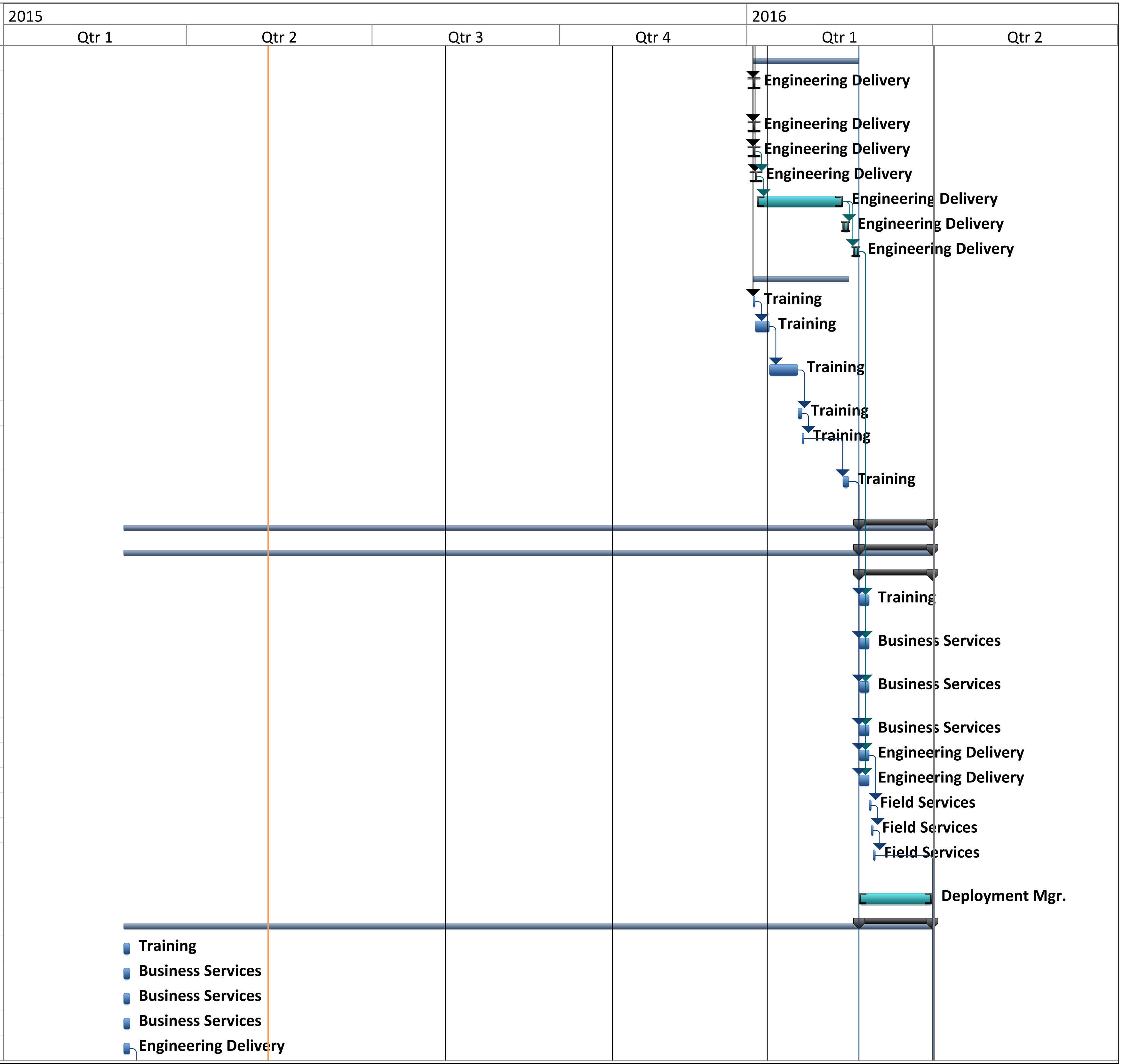
ID	Task Name	% Complete	Resource Names	Start
97	Installation of Workstation	0%	Field Services	Mon 7/20/15
98	EA Training/Transitioning for internal certificatior process	0%	Field Services	Tue 7/21/15
99	Monitor Performance and Service Quality	0%	PM	Thu 7/23/15
100	New Site Deployment -Detailed Schedule provided in body of Bid Response	0%	Deployment Mgr.	Wed 7/15/15
101	**Call Center**	**0%**		**Tue 6/30/15**
102	Provide info and training to Call Center to support Enrollment Centers and Mobiles	0%	Call Center	Mon 7/20/15
103	Expand call center staff if necessary to accommodate HOO	0%	Call Center	Tue 6/30/15
104	Integrate new sites into call system	0%	Call Center	Tue 7/21/15
105	**Finance**	**0%**		**Tue 7/7/15**
106	Collect & Identify Requirements for payment process/state/FBI fees	0%	Finance Dept.	Tue 7/7/15
107	Modify Process for Payment to State if needed.	0%	Finance Dept.	Tue 7/14/15
108	Modify Reporting/Reconciliation for State if needed	0%	Finance Dept.	Thu 7/16/15
109	Procedure Acceptance - WVSP	0%	WVSP	Thu 7/23/15
110	**PHASE 1 CURRENT ENVIRONMENT WEBSITE, USER APPLICATION, AND RESULTS DELIVERY DEVELOPMENT**	**0%**	**Engineering**	**Mon 6/8/15**
111	Website and User Application design and customer review	0%	Engineering,PM,WVSP	Mon 6/8/15
112	Development as needed of current environment and website	0%	Engineering	Mon 6/15/15
113	WV Customer Review and Acceptance of Website and User Application solution	0%	PM,WVSP	Mon 7/27/15
114	Results Delivery design and customer review	0%	PM,Engineering,WVSP	Mon 6/8/15
115	Development as needed of current results delivery	0%	Engineering	Mon 6/15/15
116	WV Customer Review and Acceptance of Results Delivery solution	0%	PM,WVSP	Mon 7/20/15
117	**PHASE 1 Current, Contract Compliant Environment GO-LIVE Completed**	0%		Fri 7/31/15
118	**Phase 2 UEP DESIGN, CUSTOMER REVIEW, AND ACCEPTANCE**	**0%**		**Thu 10/1/15**
119	MorphoTrust UEP Kickoff meeting with WV Stakeholders	0%	PM,WV Stakeholders,WVSP	Tue 9/1/15
120	WV UEP Design and Initial Development	0%	PM,Engineering	Tue 9/8/15
121	WV Customer Review of UEP	0%	PM,WV Stakeholders,WVSP	Tue 10/6/15
122	WV Stakeholder Acceptance of UEP	0%	WV Stakeholders,WVSP	Wed 10/14/15
123	**PHASE 2 UEP HARDWARE AND SOFTWARE IMPLEMENTATION AND DEPLOYMENT**	**0%**		**Thu 11/12/15**
124	Phase 2 UEP Engineering Environment (90-120 Days Estimated)	0%	Engineering	Wed 10/21/15



Project: West Virginia Applicant F
Date: Mon 5/11/15

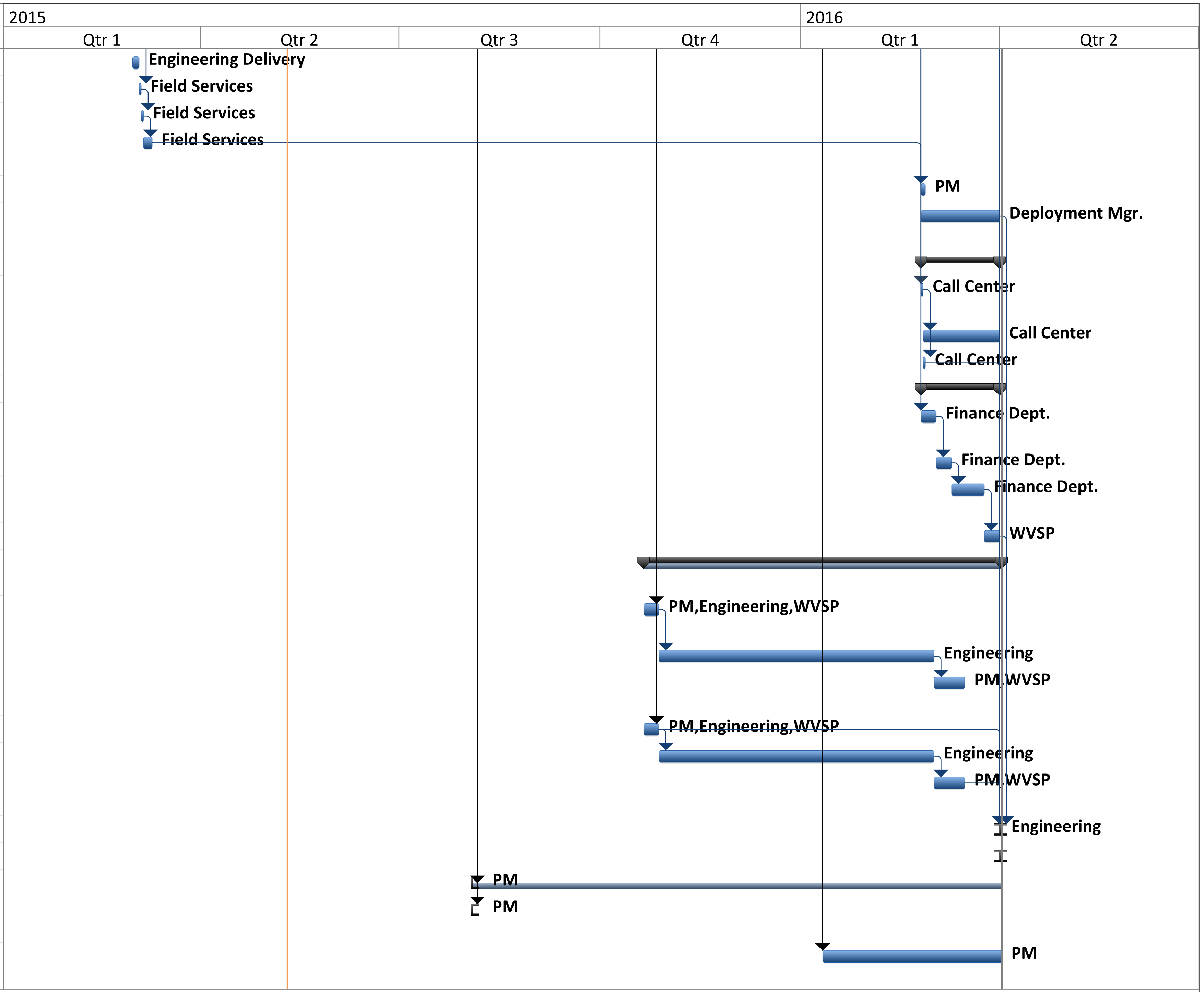
Task	▬	Project Summary	▬	Inactive Milestone	◇	Manual Summary Rollup	▬	Deadline	⇩
Split	┈	External Tasks	▬	Inactive Summary	▭	Manual Summary	▬	Progress	▬
Milestone	◆	External Milestone	◆	Manual Task	▬	Start-only	⊏		
Summary	▬	Inactive Task	▭	Duration-only	▬	Finish-only	⊐		

ID	Task Name	% Complete	Resource Names	Start
125	**Livescan Hardware**	**0%**		
126	Reserve necessary LiveScan equipment and Workstations in inventory.	0%	Engineering Delivery	Mon 1/4/16
127	Enrollment Center Bill Of Material (BOM)	0%	Engineering Delivery	Mon 1/4/16
128	Mobile BOM (Hardware and Consumables)	0%	Engineering Delivery	Mon 1/4/16
129	Order additional Workstation Equipment	0%	Engineering Delivery	Tue 1/5/16
130	Workstation Received from Order	0%	Engineering Delivery	Wed 1/6/16
131	Prepare for shipping the Livescans	0%	Engineering Delivery	Wed 2/17/16
132	Prepare for shipping the Workstations	0%	Engineering Delivery	Mon 2/22/16
133	**Training**	**0%**		
134	Identify the Training Coordinator	0%	Training	Mon 1/4/16
135	Site Development Schedule and Training of Staff - Draft Plan	0%	Training	Tue 1/5/16
136	Update Training Material: User manual, Quick Reference Guide, Training acknowledgement forms	0%	Training	Tue 1/12/16
137	Deliver Installation Guide	0%	Training	Tue 1/26/16
138	Schedule Train The Trainer: Schedule training session for the FSEs to provide the EA training	0%	Training	Thu 1/28/16
139	Provide Train The Trainer: Train the FSEs to provide the EA training	0%	Training	Wed 2/17/16
140	**Roll Out / Deployment**	**0%**		**Thu 2/25/16**
141	**Site List**	**0%**		**Thu 2/25/16**
142	**Current Site Preparation Plan and Schedule**	**0%**		**Thu 2/25/16**
143	Designated Sites: Ship Updated User Guides to Sites	0%	Training	Thu 2/25/16
144	Designated Sites: Ship Furniture and Fixtures if needed for a specific site	0%	Business Services	Thu 2/25/16
145	Designated Sites: Ship Signage and Branding Material	0%	Business Services	Thu 2/25/16
146	Designated Sites: Ship Consumables	0%	Business Services	Thu 2/25/16
147	Designated Sites: Ship Workstations	0%	Engineering Delivery	Thu 2/25/16
148	Designated Sites: Ship the LiveScans	0%	Engineering Delivery	Thu 2/25/16
149	Designated Sites: Equipment Received	0%	Field Services	Tue 3/1/16
150	Designated Sites: Installation of Workstation	0%	Field Services	Wed 3/2/16
151	Designated Sites: EA Training for Updated Equipment	0%	Field Services	Thu 3/3/16
152	Current Site Deployment	0%	Deployment Mgr.	Thu 2/25/16
153	**New Site Preparation Plan and Schedule**	**0%**		**Thu 2/25/16**
154	Ship Training Material to Identified Sites	0%	Training	Sun 3/1/15
155	Ship Furniture and Fixtures	0%	Business Services	Sun 3/1/15
156	Ship Signage and Branding Material	0%	Business Services	Sun 3/1/15
157	Ship Consumables	0%	Business Services	Sun 3/1/15
158	Ship Workstations	0%	Engineering Delivery	Sun 3/1/15



Project: West Virginia Applicant F Date: Mon 5/11/15	Task	▬	Project Summary	▬	Inactive Milestone	◇	Manual Summary Rollup	▬	Deadline	⬇
	Split	┅	External Tasks	▬	Inactive Summary	▭	Manual Summary	▬	Progress	▬
	Milestone	◆	External Milestone	◆	Manual Task	▬	Start-only	[		
	Summary	▬	Inactive Task	▭	Duration-only	▬	Finish-only	]		

ID	Task Name	% Complete	Resource Names	Start
159	Ship the LiveScans	0%	Engineering Delivery	Sun 3/1/15
160	Equipment Received	0%	Field Services	Wed 3/4/15
161	Installation of Workstation	0%	Field Services	Thu 3/5/15
162	EA Training/Transitioning for internal certificatior process	0%	Field Services	Fri 3/6/15
163	Monitor Performance and Service Quality	0%	PM	Thu 2/25/16
164	New Site Deployment -Detailed Schedule provided in body of Bid Response	0%	Deployment Mgr.	Thu 2/25/16
165	**Call Center**	**0%**		**Thu 2/25/16**
166	Provide info and access to UEP for Call Center to support	0%	Call Center	Thu 2/25/16
167	Provide training to Call Center for UEP interface	0%	Call Center	Fri 2/26/16
168	Integrate UEP into call system	0%	Call Center	Fri 2/26/16
169	**Finance**	**0%**		**Thu 2/25/16**
170	Collect & Identify Requirements for payment process/state/FBI fees	0%	Finance Dept.	Thu 2/25/16
171	Modify Process for Payment to State if needed.	0%	Finance Dept.	Thu 3/3/16
172	Modify Reporting/Reconciliation for State if needed	0%	Finance Dept.	Thu 3/10/16
173	Procedure Acceptance - WVSP	0%	WVSP	Fri 3/25/16
174	**PHASE 2 UEP WEBSITE, USER APPLICATION, AND RESULTS DELIVERY DEVELOPMENT**	**0%**	**Engineering**	**Wed 10/21/15**
175	UEP Website and User Application design and customer review	0%	PM,Engineering,WVSP	Wed 10/21/15
176	Development as needed of UEP environment and website	0%	Engineering	Wed 10/28/15
177	WV Customer Review and Acceptance of UEP Website and User Application solution	0%	PM,WVSP	Wed 3/2/16
178	UEP Results Delivery design and customer review	0%	PM,Engineering,WVSP	Wed 10/21/15
179	Development as needed of UEP results delivery	0%	Engineering	Wed 10/28/15
180	WV Customer Review and Acceptance of UEP Results Delivery solution	0%	PM,WVSP	Wed 3/2/16
181	Launch of UEP Public Website	0%	Engineering	Fri 4/1/16
182	PHASE 2 UEP GO-LIVE Completed	0%		Fri 4/1/16
183	**ONGOING OPERATIONS AND MARKETING**	**0%**	**PM**	**Mon 8/3/15**
184	Operational Management, Program reviews, Ongoing Quarterly	0%	PM	Mon 8/3/15
185	Legislative affairs and new user agency meeting, Ongoing Annually	0%	PM	Mon 1/11/16



Project: West Virginia Applicant F
Date: Mon 5/11/15

Task	▬	Project Summary	▬	Inactive Milestone	◇	Manual Summary Rollup	▬	Deadline	⇩
Split	┄	External Tasks	▬	Inactive Summary	▭	Manual Summary	▬	Progress	▬
Milestone	◆	External Milestone	◆	Manual Task	▬	Start-only	[		
Summary	▬	Inactive Task	▭	Duration-only	▬	Finish-only	]		

Appendix C – Lists of Fingerprinting Centers in Referenced Programs

As specified in RFP requirement 4.3.2, MorphoTrust has provided a list of Enrollment Centers, including the hours of availability, for the following referenced programs:

- Texas Department of Public Safety
- Tennessee Bureau of Investigations
- Massachusetts Executive Office of Public Safety

MorphoTrust Enrollment Centers in Texas

Texas City	Address	Hours of Operation
ABILENE	500 CHESTNUT, SUITE 856	HOURS VARY
Abilene	441 S Treadway Blvd	Mon - Fri 8:30 - 4:30
ALEDO	1008 BAILEY RANCH ROAD	M - F 8-4:30
Allen	210 Central Expressway S, Ste 98	Mon - Sat Hours Vary
ALLEN	612 EAST BETHANY DRIVE	M - F 8:30 - 4
Alpine	704 W Sul Ross Ave	Tue 8:30 - 3:30
Amarillo	3501 S Georgia St, Ste A	Mon - Fri 8:00 - 5:00
AMARILLO	1616 KENTUCKY, SUITE C-305	HOURS VARY
Argyle	306 U.S. 377 North, Suite G-1	M-THUR 9 - Fri 9:30 - 4:30 SAT. 10 - 4
Arlington	1601 E Lamar, Ste 118-A	Mon - Fri 8:30 - 4:30
AUSTIN	1033 La Posada Drive Suite 360	Mon - Fri 8:20-4:30
AUSTIN	1701 DIRECTOR BLVD, SUITE 350	HOURS VARY
Austin	108 Denson Dr	Mon - Fri 8:00 - 5:00
AUSTIN	1111 WEST 6TH STREET, BUILDING D, STE 130	HOURS VARY
Austin	1515 S Capital of Texas Hwy, Ste 114	Mon - Fri 8:20 - 4:30
AUSTIN	505 HUNTLAND EAST DR SUITE 330	HOURS VARY
Bay City	2113 Ave G, Ste A	Mon - Fri 8:00 - 5:00
Baytown	4804 East Freeway	Mon - Sat Hours Vary
Beaumont	3480 Fannin St, Ste F	Mon - Fri 8:00 - 4:30
Beeville	1402 East Houston Street	Pending
BELLAIRE	6800 WEST LOOP SOUTH, SUITE 405	HOURS VARY
Big Spring	1111 S Scurry St	Mon - Fri 9:00 - 5:00
Brady	2200 S Bridge St	Mon 11:30 - 3:30
BROWNSVILLE	7470 PADRE ISLAND HWY, SUITE 170	Mon-Fri 9:00-5:00
BROWNSVILLE	2477 East Price Road	M - F 10 - 3
Brownwood	3003 Hwy 377 S	Mon 9:20- 4:30; Tue - Thu 9:20 - 5:00
Bryan	3131 E 29th St, Bldg F, Ste 105	Mon - Fri 8:20 - 4:30
Burleson	300 Boone Road, Suite A1	M - Th 9:00-4:30; Fri 9:00-3:30
CANYON, TX	3301 N 23RD STREET	
Carrollton	1016 E Hebron Pkwy, Ste 175	Mon - Fri 9:00 - 3:00
Childress	3001 Ave F NW	Tue 10:00 - 5:00
College Station	1055 Texas Avenue S, Suite 100	9;00 - 5:00
Conroe	3205 West Davis Street, 201B	M - F 8:20-4:30

Texas City	Address	Hours of Operation
Converse	2661 N Graytown Rd	Mon - Fri 9:00 - 5:00
Coriscana	523 West 1st Avenue	Mon - Fri 8:00 - 4:30
Corpus Christi	1620 South Padre Island Drive, Suite 175	M - F 8:30-2:00
CORPUS CHRISTI	4646 CORONA DRIVE, SUITE 175	HOURS VARY
Corpus Christi	3403 S Padre Island Dr, Ste 205	Mon - Thu 8:00 - 4:00; Fri 8:00 - 12:00
Corpus Christi	209 N Water St	Mon - Fri 8:00 - 4:00
Dalhart	315 Rock Island	Tue 10:00 - 3:00
Dallas	1140 Empire Central Dr. Suite 570	Mon - Fri 8:20 - 4:30
DALLAS	12801 N CENTRAL EXPRESSWAY, SUITE 820	HOURS VARY
Dallas	8035 E R L Thornton, Ste 116	Mon - Fri 8:00 - 5:00
DALLAS	3807 ROSS AVENUE	M - F 8-4
Del Rio	295 FM 2523 Hamilton Ln	Mon - Fri 8:30 - 4:00
DENTON	230 NORTH MAYHILL	M - F 8-5
Edinburg	2616 W Freddy Gonzalez Dr	Mon, Wed & Fri 9:00 - 5:00; Sat 9:00 - 1:00
EL PASO	4110 RIO BRAVO, SUITE 222	HOURS VARY
El Paso	7500 Viscount, Ste C-79	Mon - Fri 8:00 - 6:00
Euless	418 N. Main St., Ste. 114	Mon - Thurs 9:00 - 5:00 Fri-Sat 9:00 - 1:00
FORNEY	600 S BOIS D' ARC	T, W, TH 9:45-12:15
Fort Worth	8240 West Freeway	Tues 10:00-4:00; Wed 10:00-5:00; Thurs 10:00-7:00
Fort Worth	4500 Mercantile Plaza Dr, Ste 106	Mon - Fri 10:00 - 7:00; Sat 10:00 - 2:00
Fort Worth	13820 Hwy 377 S	Hours Vary
FORT WORTH	100 UNIVERSITY DRIVE	M - F 8-4:30
Frisco	3311 Preston Rd, Ste 9	Mon - Sat Hours Vary
FRISCO	5515 OHIO	M - F 8 - 4:30
Galveston	4623 Fort Crockett	Mon - Fri 9:00 - 6:00
GARLAND	501 S JUPITER ROAD	M - F 9 - 4
George West	208 N Nueces	Thu 10:00 - 4:30
Gonzales	1811 E Sarah Dewitt Dr	Mon & Thu 11:00 - 4:30
Graham	1581 US 380	Tues 9:00-4:00
Greenville	2806 Mitchell St	Mon, Wed & Fri 1:00 - 4:30; T, Th 9:00-5:00
Harlingen	1325 South 77 Sunshine Strip, Ste. B	M, W, F 9:00-5:00; T, Th 9:00-7:00; Sat 9:00-4:00

Texas City	Address	Hours of Operation
HARLINGEN	222 VAN BUREN, SUITE 610	HOURS VARY
HEREFORD	601 N 25 MILE AVE	W 8:00-12:00
Hereford	601 N 25 Mile Ave	Tue 8:00 - 12:00; Thu 8:00 - 4:00
Hondo	1210 18th St, Ste B-1	Tue 10:00 - 5:00
Houston	6870 Harrisburg Blvd	M - F 11:00 - 7:00
Houston	9474 Hammerly Blvd	Mon - Thurs 11:00-7:00
Houston	10763 Gulf Freeway	M - F 11:00-6:40
Houston	11111 Katy Fwy. Suite 750	
Houston	11250 Charles Rd	Mon - Fri 8:30 - 4:30
Houston	440 Benmar Dr, Ste 2000	Mon - Fri 8:20 - 4:30
HOUSTON	14425 TORREY CHASE, SUITE 240	HOURS VARY
HOUSTON	8876 GULF FREEWAY, SUITE 220	HOURS VARY
HOUSTON	2424 WILCREST, SUITE 104	HOURS VARY
Houston	3262 S Loop W	Mon - Fri 9:00 - 6:00; Sat 9:00 - 3:00; Notary Services Tue - Sat
Houston	13135 Champions Dr, Ste 104	Mon - Fri 9:00-4:30; Sat 10-3
Houston	10039 Bissonnet St, Ste 112	Mon - Fri 8:00 - 3:00; Sat 8:00 - 2:00
Humble	20200 Eastway Village Drive	M - F 8:30-4:00
HURST	500 GRAPEVINE HWY, SUITE 401	HOURS VARY
Irving	8925 Sterling St, Ste 255	Mon - Fri 9:00 - 4:30
JUSTIN	2001 TEXAN DRIVE	M - F 9-4
JUSTIN	2001 TEXAN DRIVE	T & THUR 8:30-11:30
Katy	3815 N Fry Road, # 560	M - F 9:30-4:40
Kerrville	1886 Cypress Creek Rd	Thu & Fri 9:00 - 6:00
Killeen	4402 E Central Texas Expy	Mon - Fri 9:00-4:30; Sat 11:00-3:00
Kingsville	505 N U S Hwy 77	Wed 10:00 - 12:00 & 1:00 - 6:30
Kingwood	4311 Kingwood Dr	Mon - Fri 8:30 - 4:00; Sat 10:30 - 1:00
Lake Jackson	145 Oyster Creek Dr, Ste 7A	Mon - Sat 10:20 - 7:30
Laredo	802 E Saunders, Ste B	Mon - Fri 8:30 - 4:30
LEAGUE CITY	2425 E MAIN STREET	M - F 8-4:30
Lewisville	543 Bennett Lane, Suite 109	M, W, F 9:00-5:00; T, Th 10:00-7:00
Longview	414 E Loop 281, Ste 15	Mon - Fri 9:00 - 3:00

Texas City	Address	Hours of Operation
Longview	414 E Loop 281, Ste 15	Mon - Fri 10:00 - 3:00
LUBBOCK	1628 19TH STREET	PENDING
LUBBOCK	1500 BROADWAY, SUITE 1113	HOURS VARY
Lubbock	3417 73rd, Ste B2	Mon & Fri 8:00 - 4:30; Tue - Thu 8:00 - 7:30
LUFKIN	101 COTTON SQUARE	T - Th 9 - 11:30
Lufkin	515 S First St, Ste L	Mon - Fri 8:00 - 5:00
MANSFIELD	1522 N WALNUT CREEK DRIVE	M - F 9-4
McAllen	929 E Esperanza Ave, Ste 19	Mon - Fri 8:00 - 4:30
McKinney	1918 University Business Drive Suite 512	M-THUR 9-6 FRI 9-5 SAT 9-2
MCKINNEY	1 DUVALL STREET	M - F 8:00-4:00
MESQUITE	612 E. DAVIS	T & THUR 8-4
MIDLAND	3300 NORTH A STREET, BUILDING 4, SUITE 228	HOURS VARY
MIDLAND	615 W MISSOURI	M - F 8:30-11:30
New Braunfels	5990 FM 725	Tues - Sat 10:00-6:00
NEW BRAUNFELS	1404 IH-35 NORTH	M - F 8:30 - 4
Odessa	1560 W I-20	Mon, Wed Fri 8:00-4:40; Tue & Thur 8:00-5:20; Sat 8:20-11:20
Palestine	2908 West Oak Street	Mon-Fri 8:20-4:00
Pampa	1101 N Hobart St	Mon, Wed & Fri 8:30 - 4:30
Paris	420 N Collegiate Dr, Ste 100	Wed & Fri 8:30 - 5:00
Pearland	2010 East Broadway	M - F 8 - 5
Pittsburg	4845 N U S Hwy 271	Mon - Fri 9:00 - 3:00
PLANO	2608 AVENUE K	M - S 10-8:30
Presidio	406 E O'Reilly	Mon - Fri 9:00 - 1:00 & 2:00 - 5:00
RICHARDSON	100 N CENTRAL EXPRESSWAY, SUITE 350	PENDING
RICHARDSON	400 SOUTH GREENVILLE AVENUE	M - F 8-4
Richland Hills	6900 Boulevard 26, Ste A	Mon - Fri 8:00 - 4:30
Rosenberg	1912 Avenue H Suite D	M - F 9:00-5:30
Round Rock	555 Round Rock W Dr, Bldg E, Ste 224	Mon - Fri 8:20 - 4:30
ROYSE CITY	810 OLD GREENVILLE RD	TUES & THUR 8:30-2:00
San Angelo	917 S Abe St, Ste A-3	Mon - Fri 8:00 - 5:00
San Antonio	3859 E. Southcross Blvd. Suite H	M - F 9:8:30 - 5:00
San Antonio	9258 Culebra Road Suite 101 Room 5	M-F 9:20 - 5:20
SAN ANTONIO	6100 BANDERA ROAD, SUITE 407	HOURS VARY

Texas City	Address	Hours of Operation
SAN ANTONIO	10000 SAN PEDRO, SUITE 175	HOURS VARY
San Antonio	6800 Park Ten Blvd, Ste 108, N Bldg	Mon - Fri 8:00 - 5:30
SAN ANTONIO	5617 GRISSOM ROAD	HOURS VARY, PLEASE SCHEDULE FOR APPT AVAILABILITY
San Antonio	8750 Tesoro Dr, Rm 119	Mon - Fri 8:00 - 4:30
San Antonio	1314 Hines Ave	Mon - Fri 8:00 - 4:30
San Marcos	915 Highway 80	M, W, F 8:30-4:30; T, Th 10:00-6:00
Seminole	101 SW 6th St.	Tue 8:00 - 12:00
Sherman	1413 Texoma Parkway	M, W, F 8:20-12:00; 1:00-4:30
Sonora	311 N Hwy 277	Wed 11:00 - 5:00
Spring	4405 Spring Cypress Road, Suite 112	M - F 8:20-4:30
Sugar Land	2245 Texas Drive Suite 190	Hours Vary
Temple	18 E Ave A	M, W, Th 8:00-10:00; F 8:00-11:00
Terrell	804 E. Moore Ave. Suite A	Mon - Thurs 10:00 - 6:00
Texarkana	3939 Summerhill Road	M - Th 8:00-2:00; Fri 8:00-12:00
Texas City	3300 FM 1765	Mon - Fri 9:00 - 5:00
Tyler	1324 South Beckham, Suite 109	Mon - Fri 8:00-3:00
TYLER	909 ESE LOOP 323, SUITE 625	HOURS VARY
UValde	2801 E Main St	Wed 9:20 - 12:00 & 1:00 - 5:00
Victoria	3004 Sam Houston Street	M - F 9 - 5
WACO	1105 WOODED ACRES, SUITE 406	HOURS VARY
Waco	5016 W Waco Dr	Mon - Sat Hours Vary
Waxahachie	201 E Main St, Ste 201	Mon - Thu 9:00 - 5:00; Fri 9:00 - 12:00
Weatherford	1404 South Main	M - F 8:00-4:00
Wichita Falls	1501 Midwestern Pkwy, Ste 108	M, T, TH 8:15-4:30; Wed, Fri 8:00-12:00

MorphoTrust Enrollment Centers in Tennessee

Tennessee City	Address	Hours of Operation
Athens	412 S White St	Mon - Fri 9:00 - 6:00 Sat 10-2
Bristol	1101 Volunteer Parkway Suite 5	M-F 9-12 & 1-5 Sat 10-2
Chattanooga	6231 Perimeter Drive Suite 177	M-F 8-12&1-4
Chattanooga	694 Manufacturers Rd	Mon - Thu 9:00 - 12:00 & 1:00 - 4:00
Chattanooga	2288 Gunbarrel Rd, Ste 154	Mon - Fri 9:00 - 6:00; Sat 11:00 - 3:00
Clarksville	211 University Ave	Mon - Fri 8:30 - 4:30
Cleveland	114 Stuart Rd NE	Mon - Fri 10:00 - 6:00
Columbia	501 W Eighth St	Mon - Fri 7:30 - 5:00
Columbia	2516 Hospitality Dr	Mon - Thu 8:00 - 4:30; Fri 8:00 - 3:30; Sat 9:00 - 11:00
Cookeville	370 S Lowe Ave Suite A	Mon-Fri 9-12&1-5
Cordova	1138 N Germantown Pkwy, Ste 101	Mon - Fri 9:00 - 6:30; Sat 10:00 - 3:30
Covington	1580 Highway 51 S	M-Th 8:30-4:00, F 8:30-3:00
Covington	412 Long Ave (street sign shows Alston St)	Mon - Fri 9:00 - 12:00 & 1:00 - 5:00
Crossville	1576 N Main St	Mon - Fri 8:30 - 4:30
Dayton	9297 Rhea County Hwy	Mon - Fri 8:30 - 4:30
Dickson	432 Highway 46 South	Tue & Thu 8:30 - 11:00 & 1:00 - 3:00
Dyersburg	710 Hwy 51 By Pass West	Mon - Fri 8-11 & 1 - 6; Sat 9:00 - 1:00
Elizabethton	106 Broad St	Mon - Fri 9:00 - 6:20; Sat 9:00 - 1:00
Farragut	11519 Kingston Pike	Mon - Fri 9:00 - 6:00; Sat 9:00 - 2:00
Franklin	625 Bakers Bridge Ave, Ste 105	Mon - Fri 10:00 - 5:00
Gallatin	695 Nashville Pike	Tue - Fri 9:30 - 5:30; Sat 10:30 - 3:00
Greeneville	431 E. Bernard Avenue	Mon-Fri 10:00-4:30
Harriman	1824 Roane State Hwy	Mon - Fri 10:00 - 6:00; Sat 10:00 - 2:00
Hendersonville	600 W Main St	Mon, Tue, Thu & Fri 10:00 - 12:00 & 1:00 - 6:00; Sat 9:00 - 12:00
Hohenwald	43 Smith St	Fri 12:00 - 4:00
Jackson	266 Grady Montgomery Drive	M-F 8:30-11:00&12:30-5:00
Johnson City	3101 Browns Mill Rd	Mon - Fri 9:00 - 12:00 & 1:00 - 5:00; Sat 10:00 - 2:00

Tennessee City	Address	Hours of Operation
Kingsport	4128 Fort Henry Dr	Mon - Fri 9:00 - 5:30; Sat 10:00 - 2:00
Knoxville	7450 Chapman Hwy	Mon & Tue 10:00 - 5:00; Wed - Fri 1:00 - 6:00; Sat 10:00 - 2:00
Knoxville	6923 Maynardville Pike	Mon - Fri 9:00 - 6:00; Sat 11:00 - 12:00 & 1:00 - 2:00
Lawrenceburg	2362 Springer Rd	Mon - Fri 8:00 - 12:00 & 1:00 - 5:00
Lebanon	511 N Castle Heights Ave	M-F 9-12 & 1-4
Lebanon	1037 W Main St, Ste A	Mon - Fri 8:30 - 4:15
Lenoir City	312 W Broadway	Mon - Fri 10:00 - 6:00; Sat 10:00 - 3:00
Maryville	2208 E Broadway Ave	Mon - Fri 11:00 - 6:00; Sat 11:00 - 3:00
McKenzie	101 Wildcat Lane	M-F 8-3
Memphis	3385 Airways Blvd Suite 108	Mon - Fri 8:00 - 1:00
Memphis	1779 Kirby Parkway #1	Mon - Fri 9:00 - 5:30; Sat 10:30 - 3:30
Memphis	2770 Whitten Rd	Mon - Fri 10:00 - 6:00; Sat 10:00 - 2:00
Memphis	2577 Poplar Ave	Mon - Fri 9:00 - 5:00
Memphis	3463 Lamar Ave	Tue - Fri 10:00 - 4:30; Sat 10:00 - 3:00
Memphis	160 S Hollywood St C-140	M - F 8 -4 School Employees Only
Morristown	2812 W Andrew Johnson Hwy	Mon - Fri 9:00 - 12:00 & 1:00 - 3:30
Mt Juliet	11205 Lebanon Rd	Mon, Tue, Thu & Fri 10:00 - 5:00; Wed 10:00 - 7:00; Sat 10:00 - 1:00
Murfreesboro	1826 Ward Dr Suite 204	M-F 9-12 & 1-5
Nashville	2601 Bransford Ave	Mon - Fri 8:00 - 12:30 & 1:00 - 4:00
Nashville	1645 Murfreesboro Pike	Mon - Fri 8:30 - 12:30 & 1:00 - 5:00
Oakland	7740 Highway 64	Mon-Sat 10-2 &3-5:40
Rogersville	3825 Hwy 66, Ste B	Mon - Wed & Fri 9:00 - 11:00 & 1:00 - 3:00; Thu 9:00 - 11:00 & 2:00 - 3:00
Savannah	5 Main Street	Mon - Fri 8:00 - 12:00 & 1:00 - 3:00
Sevierville	1746 Newport Hwy	M-W 10-6 Thurs 11-7 & Fri 10-6
Shelbyville	113 W Depot St (113 Southside Square)	Tue & Thu 1:00 - 4:00; Wed 9:00 - 12:00
Springfield	408 N Willow St	M-F 10-12& 1-6 Sat 11-3
Tazewell	415 Straight Crk Rd, Ste 2	Mon - Fri 9:00 - 11:30 & 1:30 - 4:00
Winchester	209 S Jefferson St	Mon - Fri 10:00 - 2:00

MorphoTrust Enrollment Centers in Massachusetts

Massachusetts City	Address	Hours of Operation
Billerica	296 Concord Road Suite 200A	M, Tu, W 9:30-12:00, 1:00-6:00, Th 9:30-12, 1:00-7:00, F 9:30-12:00, 1:00-4:30, Sa 9:00-2:00
Boston	5 Drydock Avenue Suite 2040 (2nd floor)	M, Tu, We, F 9:00-12, 1:00-6:00; Th 9:00-12, 1:00-7:00; Sa 9:00-1:00
Brockton	1285 Belmont St. Suite 10	Mon, Tue, Wed, Fri 9:00-12, 1:00-5:30, Thu 10:00-1:00, 2:00-7, Sat. 9-1
Dedham	515 Providence Highway Suite 102	Tu,We,Fri 9:00-12:00, 1-5:30, Th 10:00-1:00, 2:00-7:00, Sa 10:00-3:00
Everett	930 Broadway	M, Tu, W, F 9:00-4:30; Th 9:00-7:00, Sa 9:00-1:00
Greenfield	486 Main Street Suite B7	**First day at this site 1/26/2015** M & W 9:00-12:00, 1:00-6:00
Haverhill	143 Essex St. Suite 205	Tu, We, Fr 9:00-12:00,1-5:30, Th 10:00-12:00,1:00-7:00, Sa 8:00-2:00
Hingham	160 Old Derby St., Suite 110	M, Tu 8:00-6:00, W 8:00-7:00, Th 8:00-8:00 F 7:00-6:00 Sa 7:00-2:00
Leominster	20 Main St Suite 2C	Mon - Fri 9:00-4:00; E/o Sat. 9:00-1:00
Methuen	119 Swan Street	Mon-Fri 9:00-1, 1:30-7:00, Sat 10:00-2:00
Milford	258 Main St., Suite 120	M, Tu, We, Fri 8:00-5:00 Th 8:00-7:00 Sa 10:00-3:00
Nantucket	32 First Way	Wednesdays 9:30-12:00, 1:00-3:00
Natick	251 West Central St. Bldg. D Suite 35 Back of Bldg	M 11:00-4:00, Tu 9:00-12:00, 1:00-7:00, W&F 9:00-12:00, 1:00-6:00 Sa 10:00-3:00
New Bedford	978 Nash Road	M,Tu, W, F 9:00-2:30, 3:30-5:00, Th 9:00-2:30, 3:30-7:00, Sa 11:00-3:00
North Adams	375 Church Street. Library Lower Level Rm. B03	Fridays 10:00-12:30, 1:00-4:00
North Attleboro	11 Robert Toner Blvd. Suite 5	M, Tu, Th, F 10:00-12:00, 1:00-5:00; W 10:00-12:00, 1:00-7:00 Sa 10:00-2:00
Pittsfield	160 North St. 1st floor, Suite 101	Mon - Fri, 9:00 - 4:00 Sat, 9:00-11:00

Massachusetts City	Address	Hours of Operation
Plymouth	385 Court Street Suite 305/306	Tu,We 9:00-12:00, 1:00-5:30, Th 10:00-1:00, 2:00-7:00, Sa 8:00-2:00
Pocasset	50 Portside Drive, Unit F, Suite 2	Tue,Thu,Fri, 8:00-12:00 1:004:30; Wed, 8:00-12:00, 1:00-7:00
Salem	265 Essex St.	M 9:00-5:00, Tu, We 11:00-7:00, Th 10:00-7:00, F 9:00-4:00, Sa 10:00-3:00
Southampton	12 College Highway	Starting 12/17/2014 M-F 9:00-12:30, 1:00-5:00 e/o Sa 9:00-2:00
Southbridge	100 Central Street	Mon - Fri 8:40-3:30, Sat 8:20-2:00
Springfield	155 Brookdale Drive	Mon 9:00-1:00, 2-6:00, Tue, Fri 9:00-1:00
Springfield	372 Cooley St	Tu & We 9-12, 1-6; Th 10-12, 1-7; Fr 9-12, 1-5; Sat 10-3
Taunton	71 Main Street Suite 2400	Thu 10:00-1:00, 2:00-7:00, Fri 9:00-12:00, 1:00-5:30, Sat 9:00-3:00
Tewksbury	1445 Main Street	Tu, We, Fr 9:00-12:00 1:005:30, Th 10:00-12:00 1:00-7:00, Sa 10:00-3:00
Vineyard Haven	4 Pine Street	Mon, Tue 3:00-6:00
Waltham	289 Moody St. Suite 112	new site starting 12/29/2014 M, Tu 9:00-12:00, 1:00-5:30 W 10:00-1:00, 2:00-7:00 Sa 9:00-3:00
West Yarmouth	572 Massachusetts Route 28 Unit 3E	Mon, Wed, Fri, Sat. 9:00-12:00, 1:00-5:00
Westport	519 American Legion Hwy. Unit 3	M, F 9:00-12:00 1:00-5:00, Tu, We, Th 9:00-12:00 1:00-5:30, 2nd Sa 10:30-2:30
Worcester	490 Lincoln Street Unit 5	Tu & W, 9:00-12 1:00-5:30, Th 10:00-1:00 2:00-7:00, Sa 10:00-3:00

Appendix D – Letters of Reference

MorphoTrust has provided letters of reference from the following fingerprinting programs, as specified in requirement 4.3.2:

- Texas Department of Public Safety
- Tennessee Bureau of Investigations
- Massachusetts Executive Office of Public Safety

This page intentionally left blank.

TEXAS DEPARTMENT OF PUBLIC SAFETY

5805 N LAMAR BLVD • BOX 4087 • AUSTIN, TEXAS 78773-0001
512/424-2000
www.dps.texas.gov

STEVEN C. McCRAW
DIRECTOR
DAVID G. BAKER
ROBERT J. BODISCH, SR.
DEPUTY DIRECTORS

COMMISSION
A. CYNTHIA LEON, CHAIR
MANNY FLORES
FAITH JOHNSON
STEVEN P. MACH
RANDY WATSON

April 16, 2015

Tara Lyle
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

RE: MorphoTrust USA Reference Letter

Dear Ms. Lyle:

MorphoTrust USA has requested that I write you this letter of recommendation in reference to their work here in Texas as our sole vendor providing statewide applicant fingerprinting and photo capture services.

The contract for these services began in August of 2005 and required the vendor to establish a network of electronic fingerprint and photo capture stations throughout Texas in a pattern of sites within a 50 mile radius for 98% of the population. The vendor was also required to provide phone and Internet appointment scheduling, fee collection through our State Comptroller's ePay system and customizations to integrate other State Agency customers into the program.

With a state as geographically large and diverse as Texas, a primary concern was that our vendor be able to quickly establish their network of offices to cover our population. MorphoTrust USA established the initial roster of locations within an acceptable time frame and then continued to add additional services throughout the state. Our target of 80 locations in Texas has been expanded to include additional public sites as well as devices that are for the use of a specific agency. The total number of locations has risen to over 120 and so our customers are receiving quick access to services.

In addition to the services MorphoTrust USA provides as required by our contract, they were instrumental in creating a program to support adherence to Senate Bill SB 9, which required the fingerprinting of over 400,000 Texas educators. MorphoTrust USA proposed a solution whereupon they would visit all 1,200 Independent School Districts within the timeframe required by the SB 9. This was truly a monumental task and was completed on schedule.

MorphoTrust USA has proved to be a dependable partner in our program and have worked with us to make continual improvements. The latest upgrade to our system was an electronic waiver form that allowed us to eliminate the need to collect and store over 500,000 paper documents containing personal data, each year.

Based on our experiences here in Texas, I would recommend MorphoTrust USA to the West Virginia State Police as a vendor for similar services in your state. Please contact me if you have any additional questions regarding MorphoTrust USA's performance in support of our contract.

Don Farris, Jr.
Texas Department of Public Safety
5805 N. Lamar Blvd.
Austin, TX 78765
512-424-2078
Donald.farris@dps.texas.gov

Sincerely,

Don Farris, Jr.
Manager, Access & Dissemination Bureau
Crime Records Service

TENNESSEE BUREAU OF INVESTIGATION
901 R.S. Gass Boulevard
Nashville, Tennessee 37216-2639
(615) 744-4000
Facsimile (615) 744-4500
TDD (615) 744-4001

BILL HASLAM
GOVERNOR

MARK GWYN
DIRECTOR

April 16, 2015

Tara Lyle
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Tara,

I am writing you on behalf of our vendor MorphoTrust. We have been doing business with them for the past four years and are currently exercising our 5th option to continue this partnership.

They have been an excellent vendor and went beyond their contractual requirements to appease potential customers. The transition from our previous vendor went well and they never missed a beat. I can recommend them without hesitation and know that West Virginia will enjoy the same professional service that the citizens of Tennessee have received over the last four years.

Respectfully,

Edward B Jones
Deputy Director

EBJ/kml

The Commonwealth of Massachusetts
Executive Office of Public Safety and Security
One Ashburton Place, Room 2133
Boston, Massachusetts 02108
Tel: (617) 727-7775
TTY Tel: (617) 727-6618
Fax: (617) 727-4764
www.mass.gov/eops

CHARLES D. BAKER
Governor

KARYN E. POLITO
Lt. Governor

DANIEL BENNETT
Secretary

April 21, 2015

Tara Lyle
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Dear Ms. Lyle:

The Executive Office of Public Safety and Security (EOPSS) has been asked to provide a reference letter for MorphoTrust USA, LLC (MorphoTrust) which provides non-criminal justice applicant fingerprint services for the Statewide Applicant Fingerprint Identification Service (SAFIS) program in the Commonwealth of Massachusetts.

MorphoTrust was the successful bidder and was awarded a one year contract with EOPSS in 2013 with the option to renew through a competitive bid process. MorphoTrust provides the following services in support of the SAFIS program:

- Appointment scheduling by phone and secure online registration website;
- Enrollment centers throughout the Commonwealth equipped with enrollment workstations and staffed with enrollment agents;
- Card scan processing for out of state applicants;
- Electronic connection to our state AFIS managed by the Massachusetts State Police; and
- Fee collection and remittance.

In addition, EOPSS is currently working with MorphoTrust on the development and implementation of a web based results system.

EOPSS awarded our SAFIS contract to MorphoTrust with a short implementation timeline. In addition, the Commonwealth of Massachusetts did not have an existing statewide non-criminal justice fingerprint background check program. MorphoTrust worked in partnership with EOPSS to stand-up the statewide network within agreed upon implementation timelines. EOPSS has been pleased with the services provided by

MorphoTrust and renewed their contract in September 2014 for an additional three years. MorphoTrust continues to work with EOPSS on adding new user groups to the SAFIS program.

I recommend MorphoTrust to the Department of Administration, Purchasing Division to provide non-criminal applicant fingerprint services within the State of West Virginia.

If you have any questions, please feel free to contact me at your convenience by phone at 617-274-5512 or by email at curtis.wood@state.ma.us

Sincerely,

Curtis M. Wood

Curtis M. Wood
Undersecretary for Forensic Science & Technology
Secretariat Chief Information Officer

Appendix E – FBI Certification

Per RFP requirement 4.5.2, MorphoTrust has provided letters from the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) certifying that our TouchPrint 4100 (TP-4100), TouchPrint 5100 (TP-5100), and TouchPrint 5300 (TP-5300) Livescan devices have been tested and found to be in compliance with the FBI CJIS Integrated Automated Fingerprint Identification System Image Quality Specifications (IQS) Appendix F Specifications.

Please note that the FBI certification letters are addressed to Identix, Inc. and L- 1 Identity Solutions, Inc. Both companies are original entities that are now MorphoTrust USA, LLC.

This page intentionally left blank.

U.S. Department of Justice

Federal Bureau of Investigation

Clarksburg, WV 26306

June 27, 2006

Mr. Dan Maase
Identix, Inc.
Suite 205
5600 Rowland Road
Minnetonka, MN 55343

Dear Mr. Maase:

The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division has completed a review of the following test data:

Submitting Vendor	Equipment
Identix, Inc.	***TouchPrint 4100* (TP-4100) Livescan Fingerprint and Identification Flats device at 500 ppi, with and without membrane.**

This review was conducted by representatives of the FBI and the MITRE Corporation's image processing laboratory located in Bedford, Massachusetts. Based on the results of this review, the FBI certifies that the equipment described above is in compliance with the following FBI CJIS Division's Integrated Automated Fingerprint Identification System Image Quality Specifications (IQS):

Appendix F Specifications

Please note, the certification process does not endorse one product over any other product and only demonstrates that the product meets FBI standards. Continued acceptance of the images created by an installed system, for retention in the FBI Master Fingerprint files, is contingent on the ability of the product to meet the IQS over time. As equipment can degrade, the FBI recommends that your company assist customers in the establishment of quality assurance programs and appropriate maintenance schedules for your products.

Please direct any questions regarding this certification to Mr. Thomas E. Hopper, at (202) 324-3506.

Sincerely yours,

Monte C Strait

Monte C. Strait
Deputy Assistant Director
Policy, Administrative and Liaison Branch
Criminal Justice Information Services Division

U.S. Department of Justice

Federal Bureau of Investigation

Clarksburg, WV 26306

January 26, 2010

Mr. Dan Maase
L-1 Identity Solutions, Inc.
Biometrics Division
5705 West Old Shakopee Road
Suite 100
Bloomington, MN 55437-3107

Dear Mr. Maase:

The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division has completed a review of the following test data:

Submitting Vendor	Equipment
L-1 Identity Solutions, Inc.	**TouchPrint 5100 (TP-5100), incorporating the L-1 TP-5750 tenprint livescan device at 500 and 1000 ppi, without membrane**

This review was conducted by representatives of the FBI and the MITRE Corporation's image processing laboratory located in Bedford, Massachusetts. Based on the results of this review, the FBI certifies that the equipment described above is in compliance with the following FBI CJIS Division's Integrated Automated Fingerprint Identification System Image Quality Specifications (IQS):

Appendix F Specifications

Please note, the certification process does not endorse one product over any other product and only demonstrates that the product meets FBI standards. Continued acceptance of the images created by an installed system, for retention in the FBI Master Fingerprint files, is contingent on the ability of the product to meet the IQS over time. As equipment can degrade, the FBI recommends that your company assist customers in the establishment of quality assurance programs and appropriate maintenance schedules for your products.

Please direct any questions regarding this certification to Mr. B. Scott Swann at (304) 625-2477.

Sincerely yours,

Jerome M. Pender
Deputy Assistant Director
Operations Branch
Criminal Justice Information Services Division

U.S. Department of Justice

Federal Bureau of Investigation

Clarksburg, WV 26306

March 23, 2010

Mr. Dan Maase
L-1 Identity Solutions, Inc.
Biometrics Division
5705 West Old Shakopee Road
Suite 100
Bloomington, MN 55437-3107

Dear Mr. Maase:

The Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division has completed a review of the following test data:

Submitting Vendor	Equipment
L-1 Identity Solutions, Inc.	**TouchPrint 5300 (TP-5300) tenprint/palm and Identification Flats livescan device at 500 and 1000 ppi, without membrane**

This review was conducted by representatives of the FBI and the MITRE Corporation's image processing laboratory located in Bedford, Massachusetts. Based on the results of this review, the FBI certifies that the equipment described above is in compliance with the following FBI CJIS Division's Integrated Automated Fingerprint Identification System Image Quality Specifications (IQS):

Appendix F Specifications

Please note, the certification process does not endorse one product over any other product and only demonstrates that the product meets FBI standards. Continued acceptance of the images created by an installed system, for retention in the FBI Master Fingerprint files, is contingent on the ability of the product to meet the IQS over time. As equipment can degrade, the FBI recommends that your company assist customers in the establishment of quality assurance programs and appropriate maintenance schedules for your products.

Please direct any questions regarding this certification to Mr. B. Scott Swann at (304) 625-2477.

Sincerely yours,

fo Jerome M. Pender
Deputy Assistant Director
Operations Branch
Criminal Justice Information Services Division

This page intentionally left blank.

Appendix F – Optional Features

MorphoTrust proposes several innovative concepts and custom enhancements that will provide additional services for applicants and establish the State of West Virginia's leadership as a highly effective, efficient and automated collector and provider of non-criminal justice fingerprints.

We have described each of these premium options on the following pages. Pricing for options is provided in our Cost Proposal.

1. Universal Enrollment Platform (UEP) Enhancements Package:

   A. Administrative Support and Reporting Portal

   B. Applicant Status Notification

   C. Back-up Print Capture for Poor Quality Prints

   D. Address Verification

   FULL PACKAGE OF UEP ENHANCEMENTS

2. Out-of-State Applicants

3. Expedited Fingerprinting Service

4. Custom Engineering Requests

5. Agency-Owned Livescan Systems

6. Photo Capture/Production and Delivery of Identification Badges

1. Universal Enrollment Platform (UEP) Enhancements Package

The full package of optional enhancements to the UEP Platform may be purchased for all applicants and agencies for an additional fee as listed in our Cost Proposal.

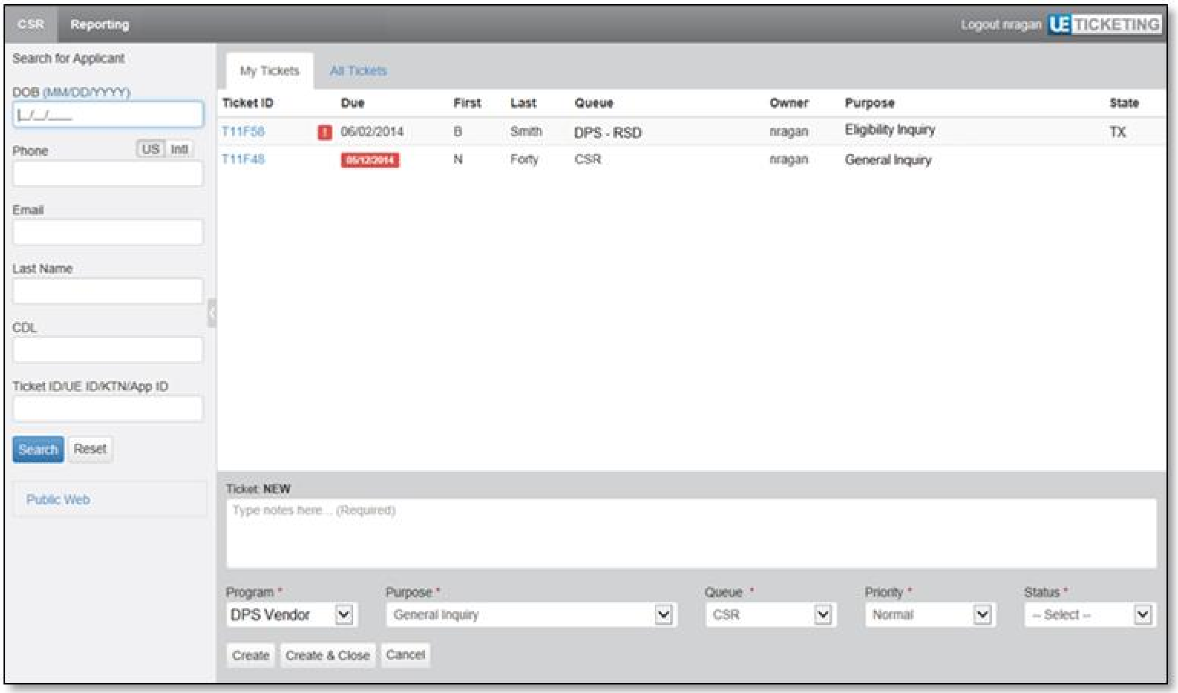
Alternatively, individual enhancements as described in A – F below may be purchased on a case-by-case basis for the additional fees listed in our Cost Proposal.

A. Administrative Support and Reporting Portal

Our Call Center has a 360° applicant-centric view that delivers important data that leads to better system monitoring and increased customer satisfaction. Our administrative portal is built specially for the enrollment industry. It combines details such as applicant status, applicant notifications, appointments, biographics, and ticketing into one system accessible by MorphoTrust clients.

With access to this portal, the State Police and User Agencies can stay connected with the entire process. This portal includes:

- Detailed transaction history and status for a real-time view of the process
- Ticketing for managing applicant support inquiries (Figure 47) across multiple teams
- Images of biometrics captured (photos, fingerprints, identity documents) for research and forensics purposes
- Management and statistical reports for operational and quality oversight



Ticket ID	Due	First	Last	Queue	Owner	Purpose	State
T11F58	! 06/02/2014	B	Smith	DPS - RSD	nragan	Eligibility Inquiry	TX
T11F48	05/12/2014	N	Forty	CSR	nragan	General Inquiry	

Ticket: NEW

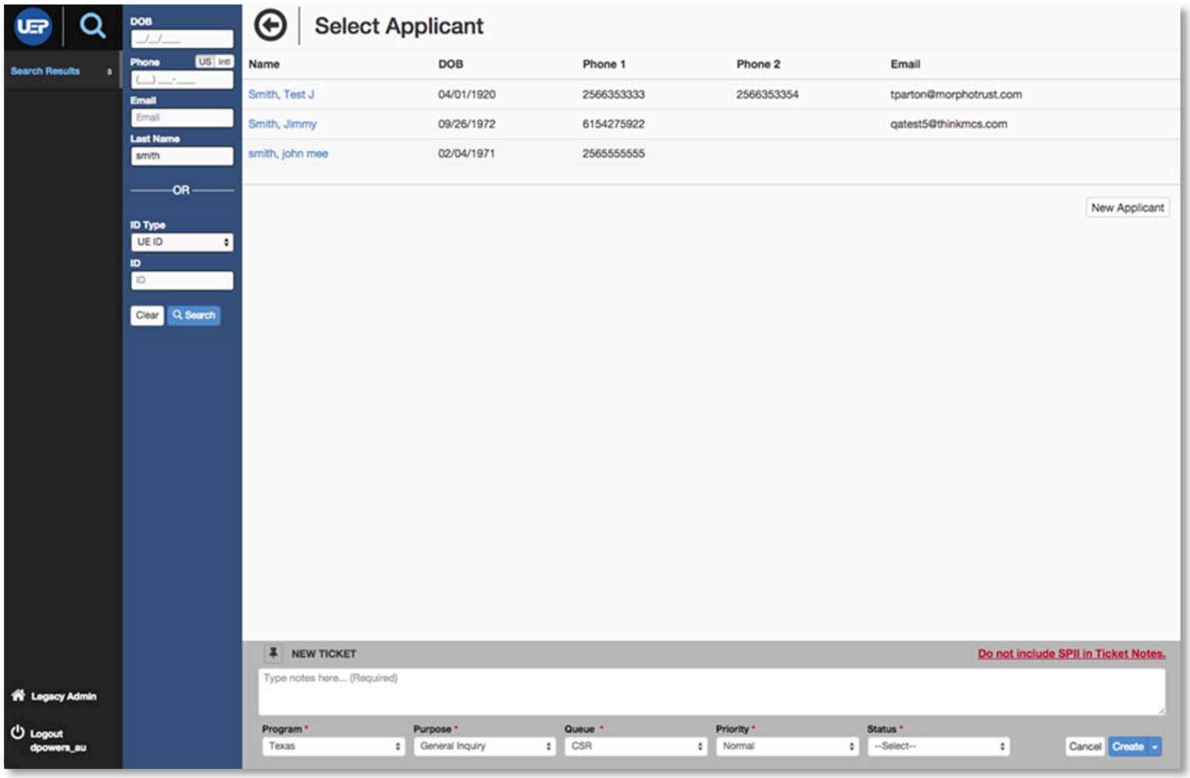
Type notes here... (Required)

Program *: DPS Vendor
Purpose *: General Inquiry
Queue *: CSR
Priority *: Normal
Status *: -- Select --

Figure 47: UEP Administrative Portal

With the UEP Administrative portal, the State of West Virginia and West Virginia agencies will have access to the same support and tracking system used by MorphoTrust Customer Service Representatives to quickly find applicants and see the status of their enrollments.

Authorized users can quickly search and find applicants related to their agency (Figure 48). Once an applicant is located, the admin user can view details about the applicant's interactions with the MorphoTrust enrollment process.



Select Applicant

Name	DOB	Phone 1	Phone 2	Email
Smith, Test J	04/01/1920	2566353333	2566353354	tparton@morphotrust.com
Smith, Jimmy	09/26/1972	6154275922		qatest5@thinkmcs.com
smith, john mee	02/04/1971	2565555555		

Last Name: smith

ID Type: UE ID

Program *: Texas

Purpose *: General Inquiry

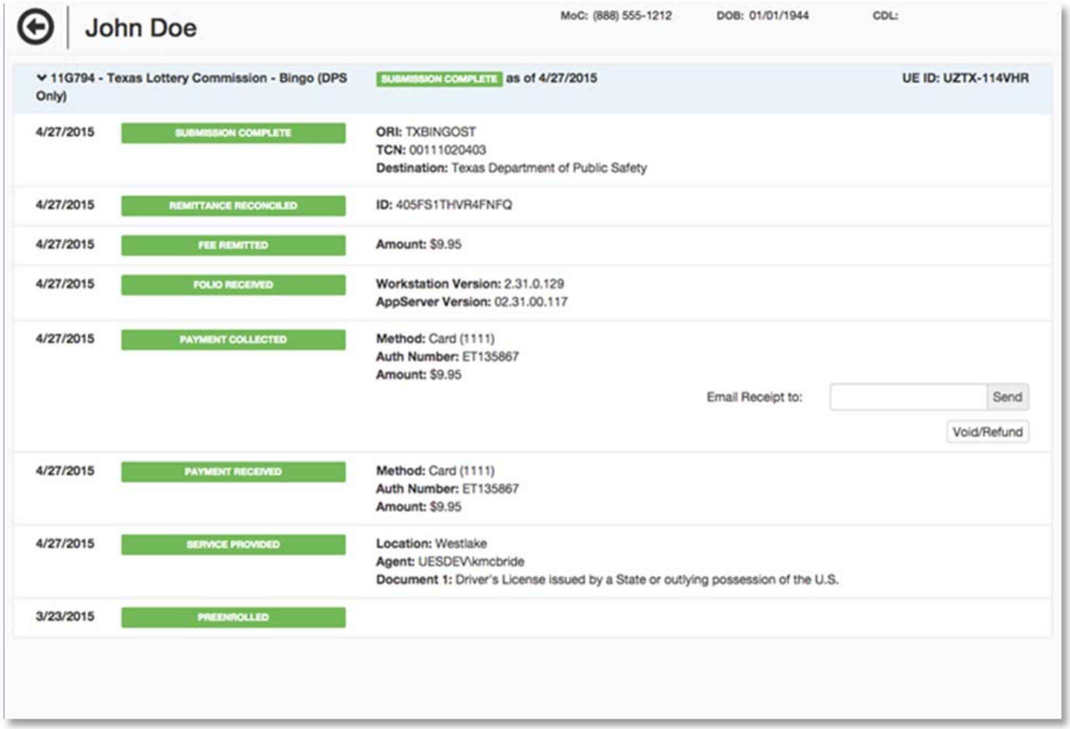
Queue *: CSR

Priority *: Normal

Status *: --Select--

Figure 48: UEP Administrative Portal – Applicant Search

This complete step-by-step history of every enrollment (Figure 49) provides details about when appointments were made, when services were provided, how payment was made, when the record was submitted to the state, and when all responses have been received.



John Doe — MoC: (888) 555-1212 DOB: 01/01/1944 CDL:

11G794 - Texas Lottery Commission - Bingo (DPS Only) — SUBMISSION COMPLETE as of 4/27/2015 — UE ID: UZTX-114VHR

4/27/2015	SUBMISSION COMPLETE	**ORI:** TXBINGOST **TCN:** 00111020403 **Destination:** Texas Department of Public Safety
4/27/2015	REMITTANCE RECONCILED	**ID:** 405FS1THVR4FNFQ
4/27/2015	FEE REMITTED	**Amount:** $9.95
4/27/2015	FOLIO RECEIVED	**Workstation Version:** 2.31.0.129 **AppServer Version:** 02.31.00.117
4/27/2015	PAYMENT COLLECTED	**Method:** Card (1111) **Auth Number:** ET135867 **Amount:** $9.95 Email Receipt to: Send Void/Refund
4/27/2015	PAYMENT RECEIVED	**Method:** Card (1111) **Auth Number:** ET135867 **Amount:** $9.95
4/27/2015	SERVICE PROVIDED	**Location:** Westlake **Agent:** UESDEV\kmcbride **Document 1:** Driver's License issued by a State or outlying possession of the U.S.
3/23/2015	PREENROLLED	

Figure 49: UEP Administrative Portal – Enrollment History

User Agencies and the State will have access to the history of any relevant transaction. Every stakeholder will know what services have been provided and what the system status is.

Should any problem be identified, an administrative user can quickly create a support ticket from any page. As shown in Figure 47, tickets may be assigned various purposes, queues, priorities, and statuses for easy sorting, management, and ultimate resolution.

With this tool, User Agencies and the State of West Virginia can observe transactional details, collaborate on any issue, maintain a single historic record of all issues, avoid redirecting the applicant, and provide superior customer support.

B. Applicant Status Notification

At any time, an applicant may review the status of their submission by either contacting our Call Center or utilizing secure features on our public website. Currently, this status is limited to alerting the user to whether or not their record has been submitted to the State of West Virginia and if that record has been rejected due to bad prints.

MorphoTrust proposes optional additional status details for the applicant, including:

- Whether their FBI background check is complete

- Whether their state background check is complete
- Whether the results are in the agency's hands for adjudication

MorphoTrust will provide this detailed status information for the applicant through our secure public website, and will also proactively notify the applicant via their preferred contact method when their request reaches a final state.

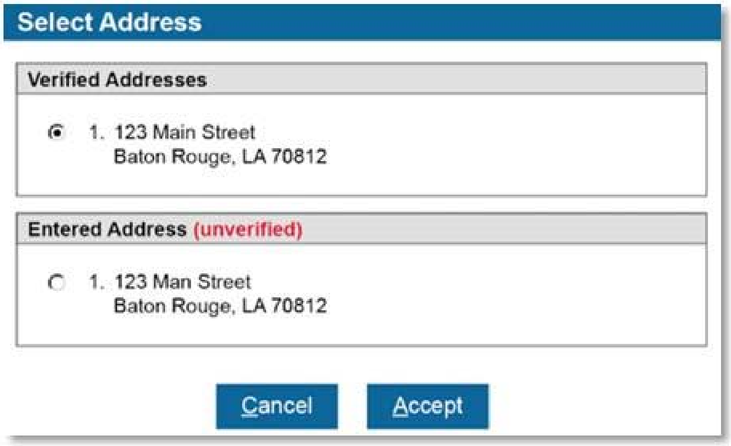
C. Back-up Print Capture for Poor Quality Prints

When digitally collecting fingerprints, MorphoTrust's workstation software will automatically compute quality scores for each finger. If the score for a fingerprint is below an acceptable threshold, the software will direct the Enrollment Agent to re-collect the fingerprint. If the Enrollment Agent is unable to collect a fingerprint that meets acceptable quality standards, the software will direct the Enrollment Agent to collect two sets of fingerprints.

MorphoTrust will always submit the best fingerprint record. However, if that print is rejected by the FBI or the Department's AFIS, MorphoTrust will automatically submit the second best print without requiring the applicant to revisit an Enrollment Center.

D. Address Verification

MorphoTrust proposes optional address verification services to ensure that mailing addresses collected are valid. This feature (Figure 50) ensures that the street address, city, state, and zip code provided by an applicant is a valid combination recognized by the United States Postal Service. When an invalid or incomplete address is given, this service will attempt to "fill in the blanks" and provide the user with suggested corrections. This service will ensure that when a mailing address is required, the State of West Virginia will always receive clean and verified data.



Select Address

Verified Addresses

● 1. 123 Main Street
Baton Rouge, LA 70812

Entered Address (unverified)

○ 1. 123 Man Street
Baton Rouge, LA 70812

Figure 50: Address Verification

This verification process ensures that the address data captured is accurate, valid, and free of typos.

FULL PACKAGE OF UEP ENHANCEMENTS

While the aforementioned UEP Enhancements can be purchased individually, MorphoTrust also offers this suite of enhancements for a single additional fee when enabled for the entire applicant population. This price is inclusive of any and all new UEP enhancements to be developed at a later date.

This package includes:

A. Support and Reporting Portal

B. Applicant Status Notification

C. Back-up Print Capture for Poor Quality Prints

D. Address Verification

2. Out-of-State Applicants

MorphoTrust can provide services for out-of-state applicants wishing to submit electronic fingerprints. Out-of-state electronic fingerprinting will initially be located in selected major cities throughout the country. Over time, as more states purchase the UEP platform, our nationwide network of over 1,200 Enrollment Centers will be enabled to allow West Virginia electronic Livescan submissions from every state, essentially eliminating the need for out-of-state Cardscan submissions. Local operating procedures and technology will be utilized at these Enrollment Centers.

3. Expedited Fingerprinting Service

In order to quickly process applicants with special circumstances, such as VIPs, adoption placements, or hiring applicants (non-certified education, private security guards, etc.) MorphoTrust will offer a limited number of premium same-day appointment slots for an additional fee. This process will be managed to ensure that applicants with appointment reservations are served during their appointed times.

4. Custom Engineering Requests

Additional Time and Material services are available upon request at our standard labor rates for custom engineering outside the scope of this RFP.

5. Agency-Owned Livescan Systems

MorphoTrust understands that some agencies prefer the opportunity to have immediate same-day printing in their own facility. Such agencies may purchase Livescan equipment and capture fingerprints utilizing that equipment, allowing the agency to process applicants on a schedule that meets their individual needs.

Agencies wishing to purchase equipment and print their own applicants for purposes authorized by statute/regulation will be presented to the West Virginia State Police for pre-approval and must execute a user agreement (Memorandum of Understanding (MOU)) with MorphoTrust. The MOU is a standard user agreement that ensures fair and equitable treatment of those agencies choosing to purchase their own Livescan equipment. It includes a pass-through of the State's Standard Terms and Conditions as well as contract-specific requirements applicable to obtaining and submitting Livescan fingerprints for background searches.

6. Photo Capture/Production and Delivery of Identification Badges

Many agencies need to produce a badge or identification card once an applicant has been fully vetted. By adding photo capture services at the time of enrollment, MorphoTrust can deliver such a badge. We provide this service for school districts in Florida and for Concealed Weapons Permits in South Carolina.

This page intentionally left blank.

Appendix G – Bid Bond (Copy)

MorphoTrust has submitted our Bid Bond document with raised seal directly to Tara Lyle, Buyer Supervisor, West Virginia Purchasing Division, as advised by Ms. Lyle by telephone on May 5, 2015.

The following pages contain a copy of the Bid Bond.

This page intentionally left blank.

Agency Dept. of Admin/Purchasing Div.
REQ.P.O#

BID BOND

KNOW ALL MEN BY THESE PRESENTS, That we, the undersigned, MorphoTrust USA, LLC of 296 Concord Road, Suite 300, Billerica, MA 01821, as Principal, and RLI Insurance Company of 9025 North Lindbergh Dr. Peoria, IL 61615, a corporation organized and existing under the laws of the State of Illinois with its principal office in the City of Peoria, IL, as Surety, are held and firmly bound unto the State of West Virginia, as Obligee, in the penal sum of Five Percent of Amount Bid ($ --5% of Amount Bid--) for the payment of which, well and truly to be made, we jointly and severally bind ourselves, our heirs, administrators, executors, successors and assigns.

The Condition of the above obligation is such that whereas the Principal has submitted to the Purchasing Section of the Department of Administration a certain bid or proposal, attached hereto and made a part hereof, to enter into a contract in writing for
Solicitation Number: CRFP-0612-DPS1500000010
West Virginia State Police, Applicant Fingerprinting Services

NOW THEREFORE,

(a) If said bid shall be rejected, or

(b) If said bid shall be accepted and the Principal shall enter into a contract in accordance with the bid or proposal attached hereto and shall furnish any other bonds and insurance required by the bid or proposal, and shall in all other respects perform the agreement created by the acceptance of said bid, then this obligation shall be null and void, otherwise this obligation shall remain in full force and effect. It is expressly understood and agreed that the liability of the Surety for any and all claims hereunder shall, in no event, exceed the penal amount of this obligation as herein stated.

The Surety, for the value received, hereby stipulates and agrees that the obligations of said Surety and its bond shall be in no way impaired or affected by any extension of the time within which the Obligee may accept such bid, and said Surety does hereby waive notice of any such extension.

WITNESS, the following signatures and seals of Principal and Surety, executed and sealed by a proper officer of Principal and Surety, or by Principal individually if Principal is an individual, this 7th day of May, 20 15.

Principal Seal

MorphoTrust USA, LLC
(Name of Principal)

By
(Must be President, Vice President, or
Duly Authorized Agent)

CFO
(Title)

Surety Seal

RLI Insurance Company
(Name of Surety)

Katherine J Foreit
Katherine J. Foreit, Attorney-in-Fact for Surety
Attorney-in-Fact
West Virginia License #2124095

IMPORTANT – Surety executing bonds must be licensed in West Virginia to transact surety insurance, must affix its seal, and must attach a power of attorney with its seal affixed.

RLI

RLI Surety
9025 N. Lindbergh Dr. | Peoria, IL 61615
Phone: (800)645-2402 | Fax: (309)689-2036
www.rlicorp.com

POWER OF ATTORNEY
RLI Insurance Company

Know All Men by These Presents:

That this Power of Attorney is not valid or in effect unless attached to the bond which it authorizes executed, but may be detached by the approving officer if desired.

That **RLI Insurance Company**, an Illinois corporation, does hereby make, constitute and appoint: C.R. Hernandez, Katherine J. Foreit, Beatriz Polito, Adrienne C. Stevenson, John K. Johnson, Amy B. Wickett, Triniy Garcia, Michael Dougherty, Rebecca J. Hobbs, jointly or severally

in the City of Chicago, State of Illinois its true and lawful Agent and Attorney in Fact, with full power and authority hereby conferred, to sign, execute, acknowledge and deliver for and on its behalf as Surety, the following described bond.

Any and all bonds provided the bond penalty does not exceed Twenty Five Million Dollars ($25,000,000.00).

The acknowledgment and execution of such bond by the said Attorney in Fact shall be as binding upon this Company as if such bond had been executed and acknowledged by the regularly elected officers of this Company.

The **RLI Insurance Company** further certifies that the following is a true and exact copy of the Resolution adopted by the Board of Directors of **RLI Insurance Company**, and now in force to-wit:

> "All bonds, policies, undertakings, Powers of Attorney or other obligations of the corporation shall be executed in the corporate name of the Company by the President, Secretary, any Assistant Secretary, Treasurer, or any Vice President, or by such other officers as the Board of Directors may authorize. The President, any Vice President, Secretary, any Assistant Secretary, or the Treasurer may appoint Attorneys in Fact or Agents who shall have authority to issue bonds, policies or undertakings in the name of the Company. The corporate seal is not necessary for the validity of any bonds, policies, undertakings, Powers of Attorney or other obligations of the corporation. The signature of any such officer and the corporate seal may be printed by facsimile."

IN WITNESS WHEREOF, the **RLI Insurance Company** has caused these presents to be executed by its Vice President with its corporate seal affixed this 13th day of February, 2015.

RLI INSURANCE COMPANY CORPORATE SEAL ILLINOIS

RLI Insurance Company

By: ______________________
Roy C. Die Vice President

State of Illinois
County of Peoria } SS

On this 13th day of February, 2015, before me, a Notary Public, personally appeared Roy C. Die, who being by me duly sworn, acknowledged that he signed the above Power of Attorney as the aforesaid officer of the **RLI Insurance Company** and acknowledged said instrument to be the voluntary act and deed of said corporation.

By: Jacqueline M. Bockler
Jacqueline M. Bockler Notary Public

"OFFICIAL SEAL"
NOTARY PUBLIC STATE OF ILLINOIS
JACQUELINE M. BOCKLER
COMMISSION EXPIRES 01/14/16

CERTIFICATE

I, the undersigned officer of **RLI Insurance Company**, a stock corporation of the State of Illinois, do hereby certify that the attached Power of Attorney is in full force and effect and is irrevocable; and furthermore, that the Resolution of the Company as set forth in the Power of Attorney, is now in force. In testimony whereof, I have hereunto set my hand and the seal of the **RLI Insurance Company** this 7 day of May, 2015.

RLI Insurance Company

By: ______________________
Roy C. Die Vice President

1233339020212

STATE OF ILLINOIS
COUNTY OF COOK

I, **Adrienne C. Stevenson**, a Notary Public in and for said County do hereby certify that **Katherine J. Foreit** Attorney-in-Fact, of these:

RLI Insurance Company, an Illinois Corporation

who is personally known to me to be the same person whose name is subscribed to the foregoing instrument appeared before me this day in person, and, acknowledged that they signed, sealed, and delivered said instrument for and on behalf of:

RLI Insurance Company, an Illinois Corporation

for the uses and purposes therein set forth.

Given under my hand and notarial seal at my office in the City of **Chicago** in said County, this 7 day of May A.D. 2015

Adrienne C Stevenson
Notary Public

"OFFICIAL SEAL"
ADRIENNE C STEVENSON
NOTARY PUBLIC, STATE OF ILLINOIS
MY COMMISSION EXPIRES DECEMBER 15, 2015

MorphoTrust USA

The Identity Company

State of West Virginia
Department of Administration
Purchasing Division

EXEMPT INFORMATION

In Response to:
CRFP_DPS1500000010
West Virginia State Police
Applicant Fingerprinting Services

Submission Date:
May 13, 2015

Submitted via wvOASIS to:
Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Submitted by:
MorphoTrust USA, LLC
296 Concord Road, Suite 300
Billerica, Massachusetts 01821
www.morphotrust.com

Contact:
John Olson
Principal Proposal Manager
Telephone: 952-945-3307
Fax: 952-932-7181
Email: jolson@morphotrust.com

SAFRAN
MorphoTrust USA

Confidential Notice

Certain information in this proposal is protected from disclosure to the public because it is a proprietary trade secret or confidential commercial or financial information of MorphoTrust USA, LLC. or its affiliates (individually and collectively, "MorphoTrust USA" or "MorphoTrust").

MorphoTrust has endeavored to identify each page of its proposal that contains any such proprietary or confidential information with the legends "**COMPANY CONFIDENTIAL – Not for Public Disclosure**" or "PROPRIETARY" (or words of similar import) somewhere on the relevant page or pages of its proposal. MorphoTrust's proposal includes all exhibits and appendices thereto, as well as all extrinsic documents and materials that may be identified and incorporated therein by specific reference. MorphoTrust's proprietary information typically includes, but is not limited to, information related to proprietary security features and related designs, techniques and materials, formulas, manufacturing methods, business plans, pricing and other financial information, technology and product roadmaps, and customer lists and references. Subject to applicable law, such proprietary or confidential information may not be disclosed (pursuant to freedom of information legislation or otherwise), reproduced in whole or in part, or used for any purpose other than the recipient's evaluation of this proposal, without the prior written consent of an executive officer or the General Counsel of MorphoTrust USA, LLC.

We understand that the Grand Total Contract Price is subject to Public Information release. However, we deem all computation and supporting price information as CONFIDENTIAL and not subject to Public Information release.

EXEMPT INFORMATION

MorphoTrust considers all information in this volume to be exempt from public disclosure. The documents contained in this volume contain highly sensitive security information as are not to be considered as public documents or disclosed to the public. Therefore, MorphoTrust has segregated this information from the rest of our proposal.

We base our claim for exemption on the following article from the West Virginia Code Chapter 29B, Freedom of Information Act:

> ARTICLE 1. PUBLIC RECORDS
>
> §29B-1-4. Exemptions
>
> > (a) The following categories of information are specifically exempt from disclosure under the provisions of this article:
> >
> > > **(14) Security or disaster recovery plans, risk assessments, tests or the results of those tests;**

MorphoTrust IT Security Policy and Personal Data Privacy Policy

MorphoTrust has provided the following policies:

- MorphoTrust Privacy Policy POL-00144-A – Describes our policies for safeguarding the private information of our customer's citizens (Personal Data Privacy Policy).
- MorphoTrust USA Cyber Security Plan PLN-00091-A-02 – Describes our policies for ensuring the security and protection of the sensitive data and the information systems that transmit or store the data from cyber-attacks (IT Security Policy).

In addition, we have provided the following relevant policies:

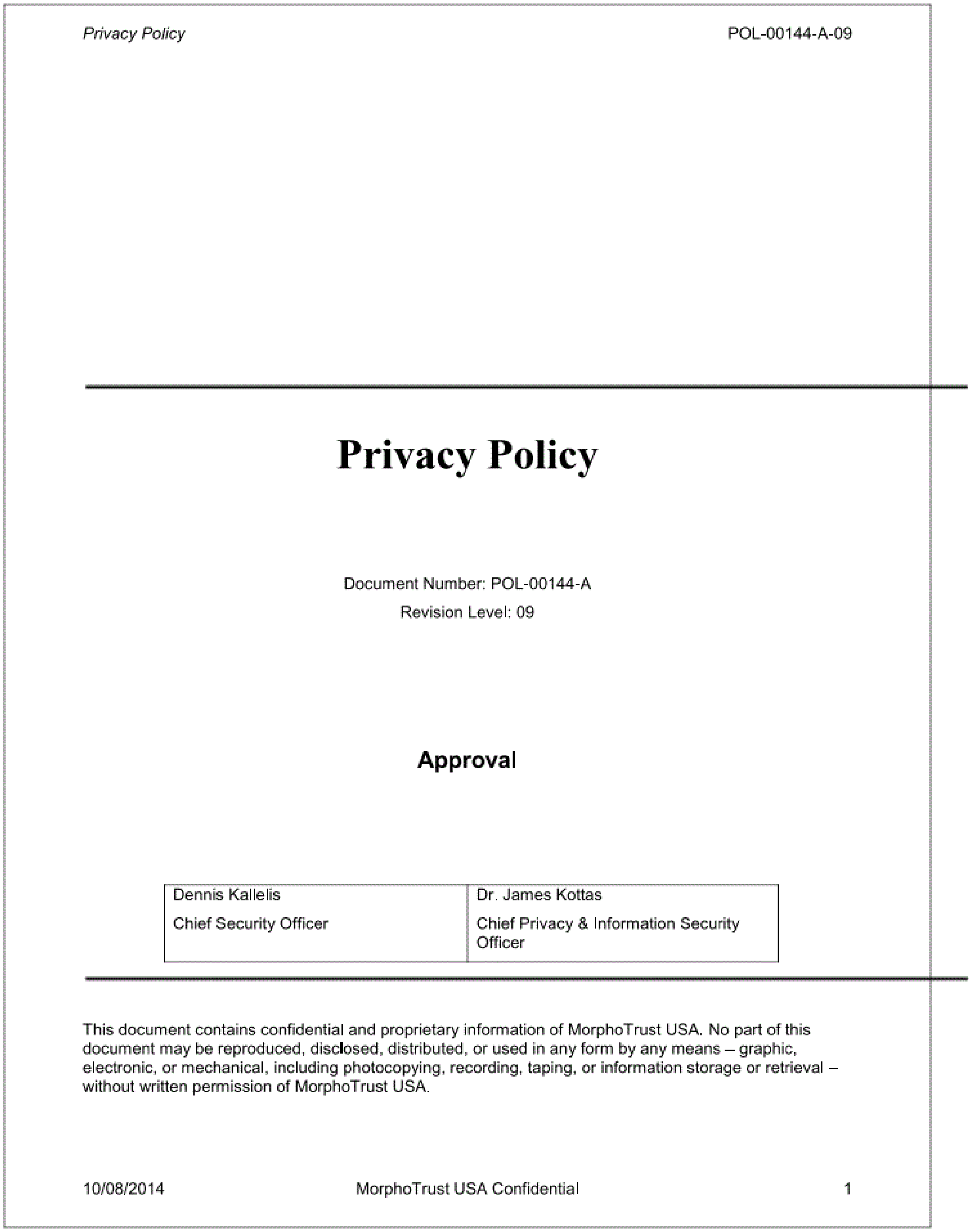
- Information Security Customer Data Access and Security Policy PRC-00174-A-07
- IT Backup Recovery PRC-00084-B-03
- IT Change Management Procedure PRC-00085-B-05
- IT Computer and System Use Procedures PRC-00110-A-10
- IT Computers on Network PRC-00086-B-01
- IT Disaster Recovery PRC-00095-B-02
- IT Electronic Communication Policy PRC-00113-A-02
- IT Firewall Policy PRC-00088-B-05
- IT Information Security PRC-00089-B-06
- IT Managing Operations PRC-00090-B-01
- IT Network Access Controls Procedures PRC-00091-B-02
- IT Physical IT Access Controls PRC-00091-B-01
- IT Remote Access PRC-00092-B-09
- IT Security Policy PRC-00112-A-03
- IT Sensitive Data Handling and Storage Procedures PRC-00148-A-05
- IT Virus Protection PRC-00093-B-01
- Removable Media Policy PRC-00150-A-01

SAFRAN
MorphoTrust USA

Click here to print

Printed By: Joan Wotkowicz
Document Printed On: Friday, April 17, 2015 1:48:19 PM
Reference: 64899314-e7ce-4bfd-be83-61d792444d09

MorphoTrust - Privacy Policy
CD398489V1



Privacy Policy

Document Number: POL-00144-A
Revision Level: 09

Approval

Dennis Kallelis Chief Security Officer	Dr. James Kottas Chief Privacy & Information Security Officer

This document contains confidential and proprietary information of MorphoTrust USA. No part of this document may be reproduced, disclosed, distributed, or used in any form by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage or retrieval – without written permission of MorphoTrust USA.

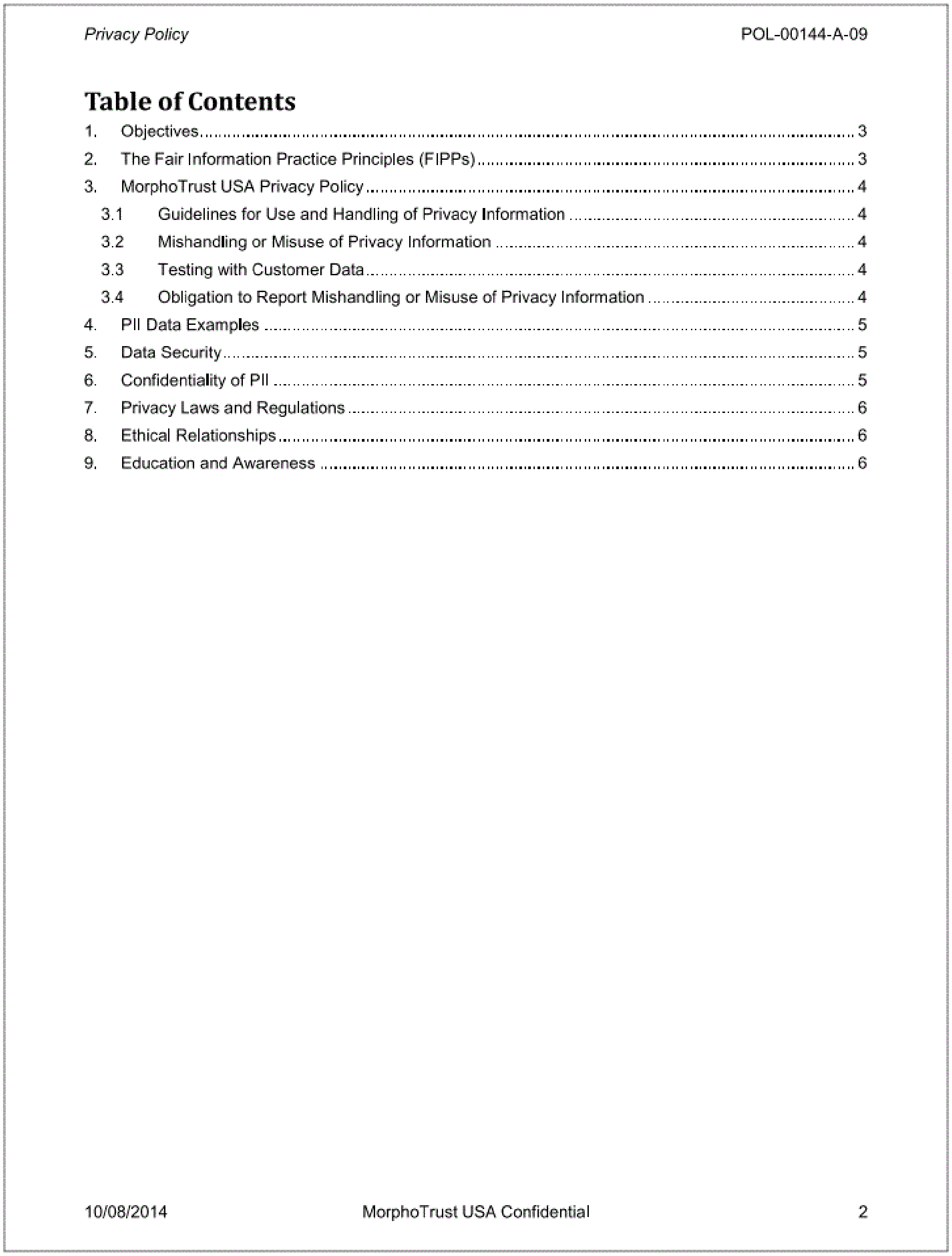
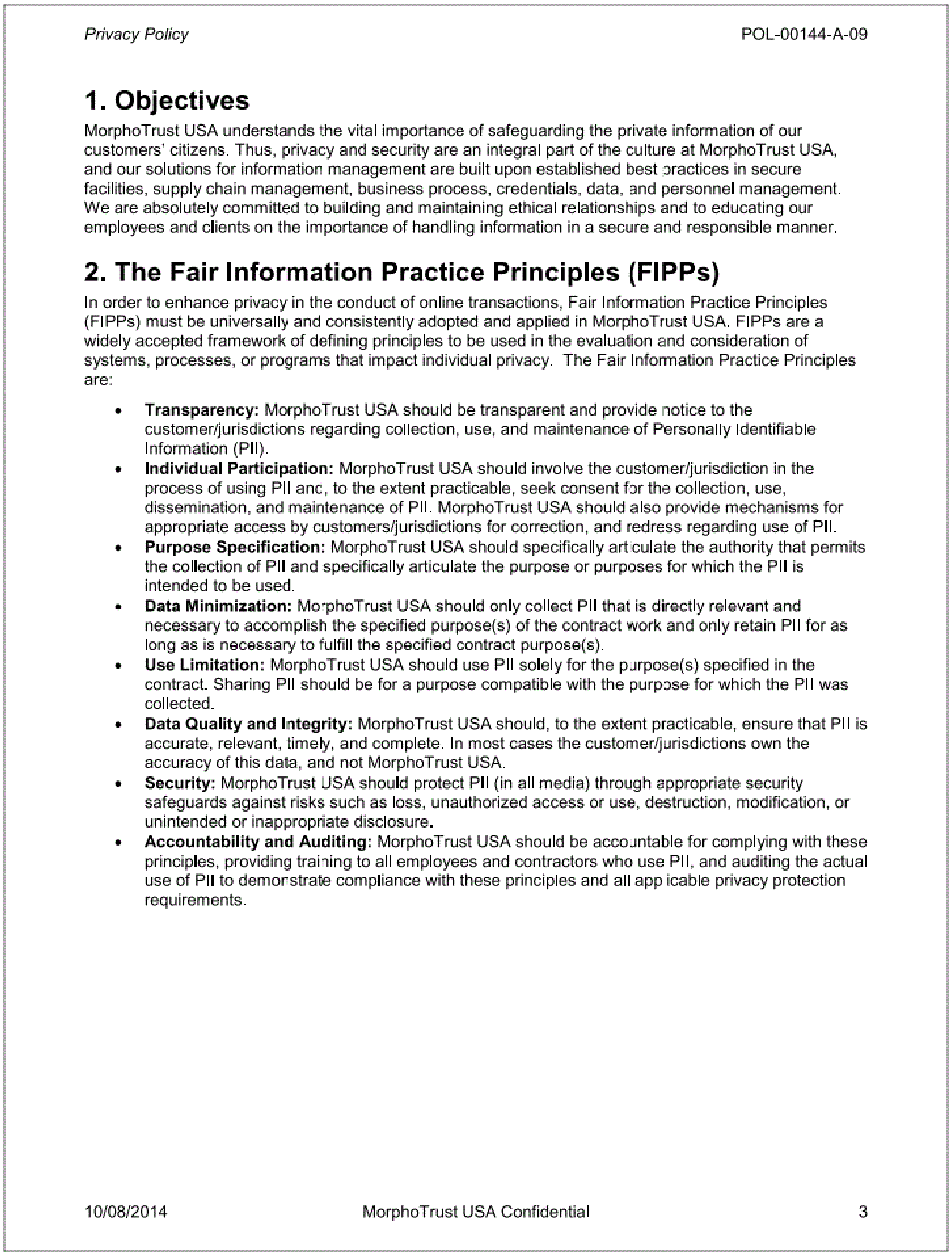


Table of Contents



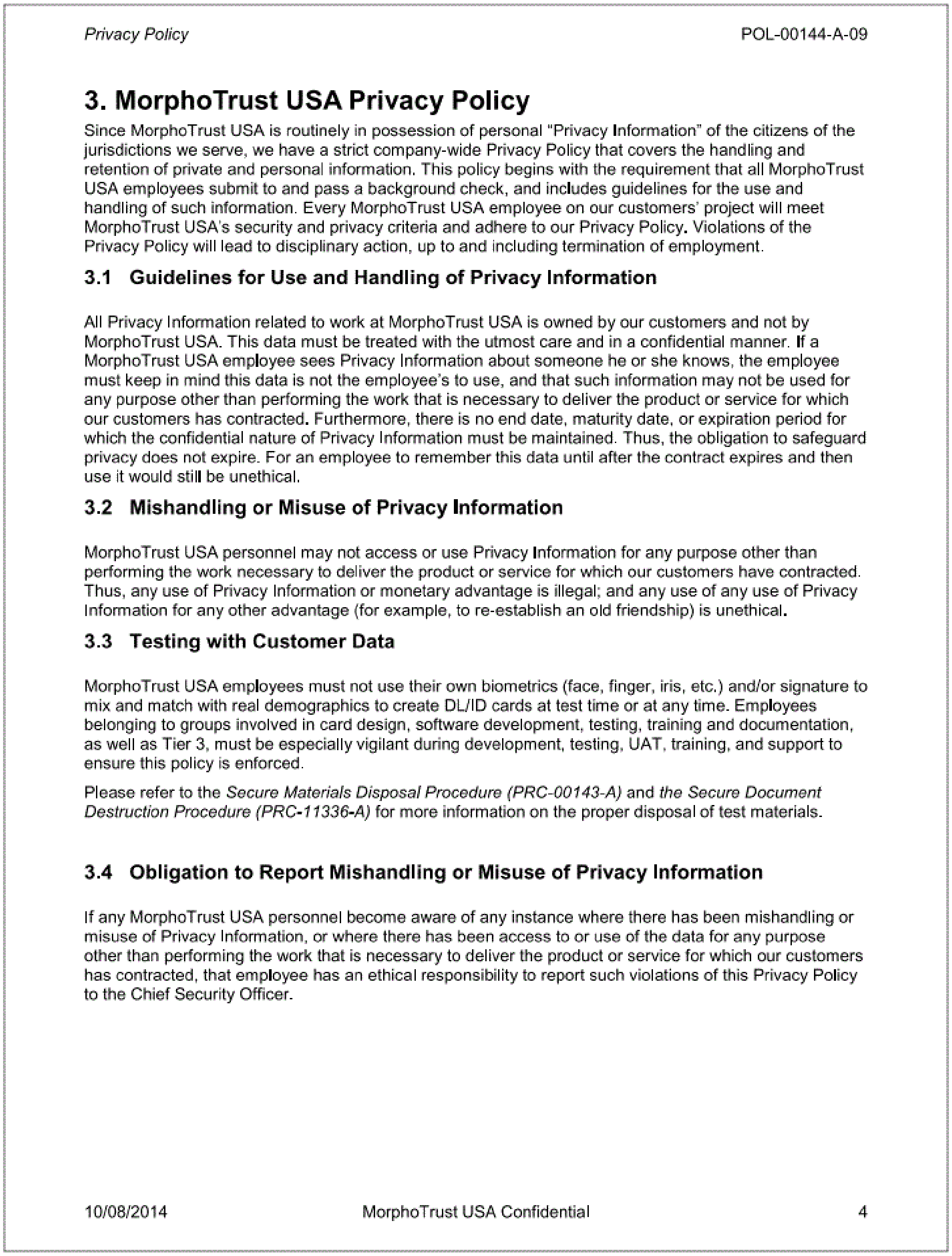
1. Objectives

MorphoTrust USA understands the vital importance of safeguarding the private information of our customers' citizens. Thus, privacy and security are an integral part of the culture at MorphoTrust USA, and our solutions for information management are built upon established best practices in secure facilities, supply chain management, business process, credentials, data, and personnel management. We are absolutely committed to building and maintaining ethical relationships and to educating our employees and clients on the importance of handling information in a secure and responsible manner.

2. The Fair Information Practice Principles (FIPPs)

In order to enhance privacy in the conduct of online transactions, Fair Information Practice Principles (FIPPs) must be universally and consistently adopted and applied in MorphoTrust USA. FIPPs are a widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that impact individual privacy. The Fair Information Practice Principles are:

- **Transparency:** MorphoTrust USA should be transparent and provide notice to the customer/jurisdictions regarding collection, use, and maintenance of Personally Identifiable Information (PII).
- **Individual Participation:** MorphoTrust USA should involve the customer/jurisdiction in the process of using PII and, to the extent practicable, seek consent for the collection, use, dissemination, and maintenance of PII. MorphoTrust USA should also provide mechanisms for appropriate access by customers/jurisdictions for correction, and redress regarding use of PII.
- **Purpose Specification:** MorphoTrust USA should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization:** MorphoTrust USA should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) of the contract work and only retain PII for as long as is necessary to fulfill the specified contract purpose(s).
- **Use Limitation:** MorphoTrust USA should use PII solely for the purpose(s) specified in the contract. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity:** MorphoTrust USA should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. In most cases the customer/jurisdictions own the accuracy of this data, and not MorphoTrust USA.
- **Security:** MorphoTrust USA should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure**.**
- **Accountability and Auditing:** MorphoTrust USA should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.



3. MorphoTrust USA Privacy Policy

Since MorphoTrust USA is routinely in possession of personal "Privacy Information" of the citizens of the jurisdictions we serve, we have a strict company-wide Privacy Policy that covers the handling and retention of private and personal information. This policy begins with the requirement that all MorphoTrust USA employees submit to and pass a background check, and includes guidelines for the use and handling of such information. Every MorphoTrust USA employee on our customers' project will meet MorphoTrust USA's security and privacy criteria and adhere to our Privacy Policy. Violations of the Privacy Policy will lead to disciplinary action, up to and including termination of employment.

3.1 Guidelines for Use and Handling of Privacy Information

All Privacy Information related to work at MorphoTrust USA is owned by our customers and not by MorphoTrust USA. This data must be treated with the utmost care and in a confidential manner. If a MorphoTrust USA employee sees Privacy Information about someone he or she knows, the employee must keep in mind this data is not the employee's to use, and that such information may not be used for any purpose other than performing the work that is necessary to deliver the product or service for which our customers has contracted. Furthermore, there is no end date, maturity date, or expiration period for which the confidential nature of Privacy Information must be maintained. Thus, the obligation to safeguard privacy does not expire. For an employee to remember this data until after the contract expires and then use it would still be unethical.

3.2 Mishandling or Misuse of Privacy Information

MorphoTrust USA personnel may not access or use Privacy Information for any purpose other than performing the work necessary to deliver the product or service for which our customers have contracted. Thus, any use of Privacy Information or monetary advantage is illegal; and any use of any use of Privacy Information for any other advantage (for example, to re-establish an old friendship) is unethical.

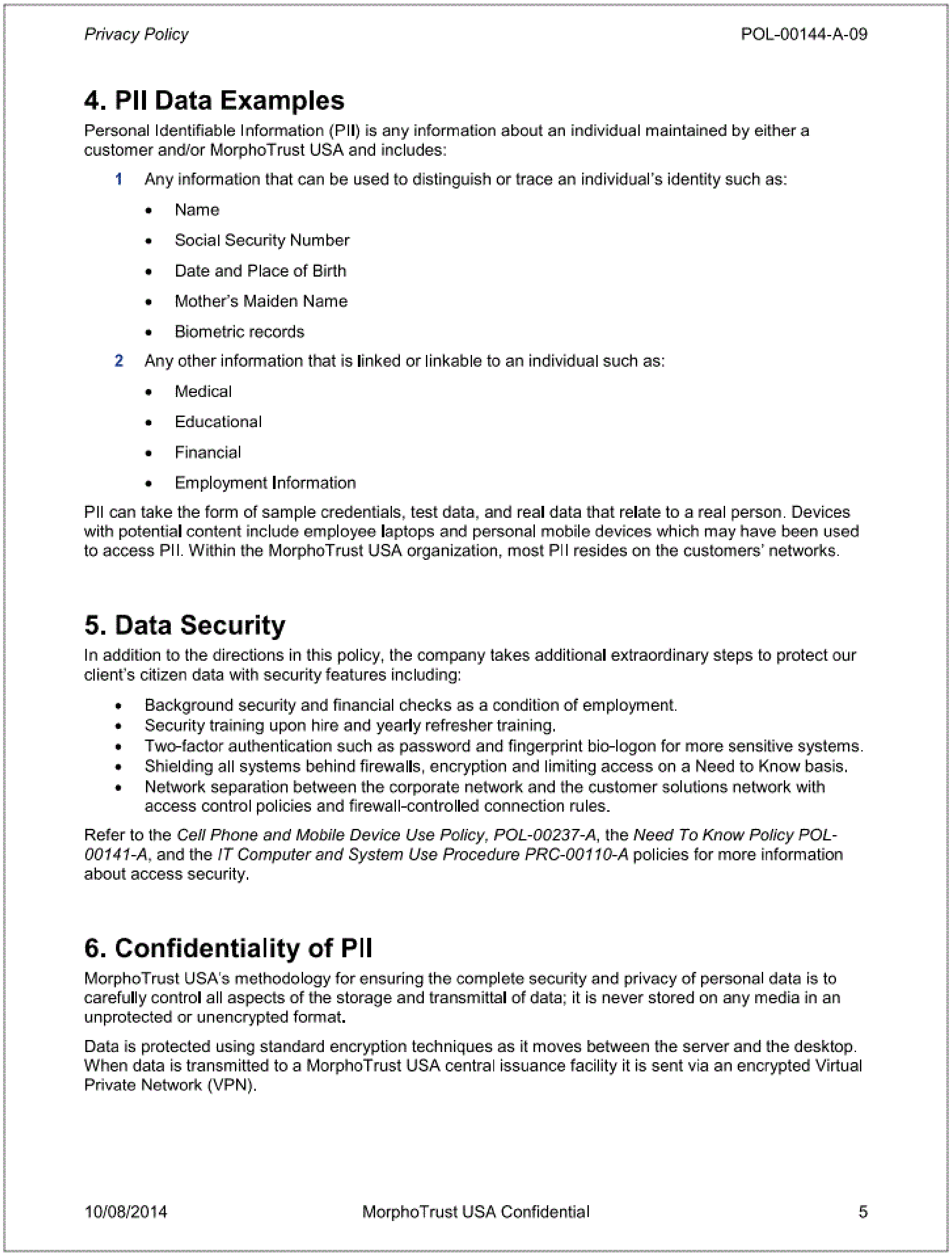
3.3 Testing with Customer Data

MorphoTrust USA employees must not use their own biometrics (face, finger, iris, etc.) and/or signature to mix and match with real demographics to create DL/ID cards at test time or at any time. Employees belonging to groups involved in card design, software development, testing, training and documentation, as well as Tier 3, must be especially vigilant during development, testing, UAT, training, and support to ensure this policy is enforced.

Please refer to the *Secure Materials Disposal Procedure (PRC-00143-A)* and *the Secure Document Destruction Procedure (PRC-11336-A)* for more information on the proper disposal of test materials.

3.4 Obligation to Report Mishandling or Misuse of Privacy Information

If any MorphoTrust USA personnel become aware of any instance where there has been mishandling or misuse of Privacy Information, or where there has been access to or use of the data for any purpose other than performing the work that is necessary to deliver the product or service for which our customers has contracted, that employee has an ethical responsibility to report such violations of this Privacy Policy to the Chief Security Officer.



4. PII Data Examples

Personal Identifiable Information (PII) is any information about an individual maintained by either a customer and/or MorphoTrust USA and includes:

1 Any information that can be used to distinguish or trace an individual's identity such as:

- Name
- Social Security Number
- Date and Place of Birth
- Mother's Maiden Name
- Biometric records

2 Any other information that is linked or linkable to an individual such as:

- Medical
- Educational
- Financial
- Employment Information

PII can take the form of sample credentials, test data, and real data that relate to a real person. Devices with potential content include employee laptops and personal mobile devices which may have been used to access PII. Within the MorphoTrust USA organization, most PII resides on the customers' networks.

5. Data Security

In addition to the directions in this policy, the company takes additional extraordinary steps to protect our client's citizen data with security features including:

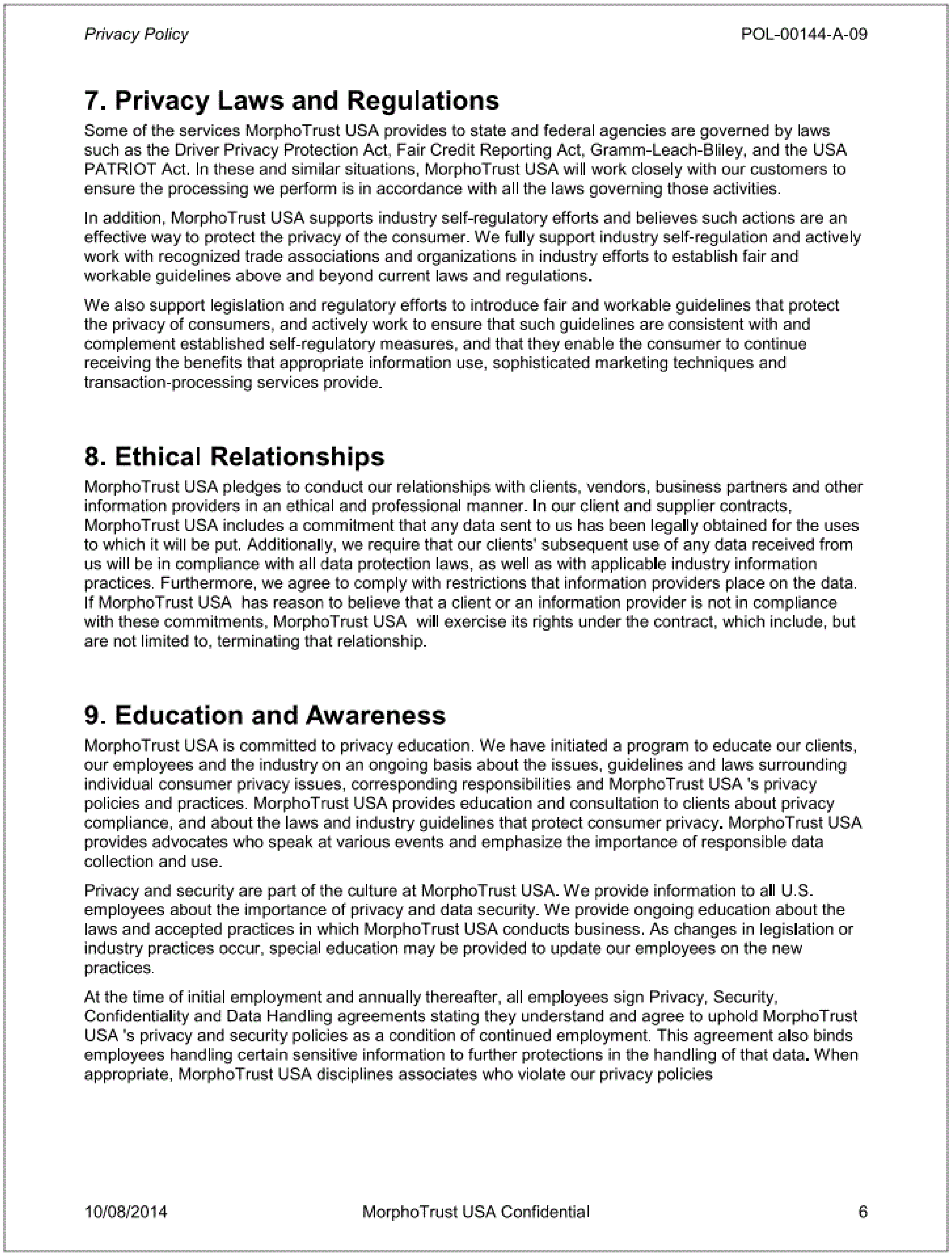
- Background security and financial checks as a condition of employment.
- Security training upon hire and yearly refresher training.
- Two-factor authentication such as password and fingerprint bio-logon for more sensitive systems.
- Shielding all systems behind firewalls, encryption and limiting access on a Need to Know basis.
- Network separation between the corporate network and the customer solutions network with access control policies and firewall-controlled connection rules.

Refer to the *Cell Phone and Mobile Device Use Policy, POL-00237-A*, the *Need To Know Policy POL-00141-A*, and the *IT Computer and System Use Procedure PRC-00110-A* policies for more information about access security.

6. Confidentiality of PII

MorphoTrust USA's methodology for ensuring the complete security and privacy of personal data is to carefully control all aspects of the storage and transmittal of data; it is never stored on any media in an unprotected or unencrypted format.

Data is protected using standard encryption techniques as it moves between the server and the desktop. When data is transmitted to a MorphoTrust USA central issuance facility it is sent via an encrypted Virtual Private Network (VPN).



7. Privacy Laws and Regulations

Some of the services MorphoTrust USA provides to state and federal agencies are governed by laws such as the Driver Privacy Protection Act, Fair Credit Reporting Act, Gramm-Leach-Bliley, and the USA PATRIOT Act. In these and similar situations, MorphoTrust USA will work closely with our customers to ensure the processing we perform is in accordance with all the laws governing those activities.

In addition, MorphoTrust USA supports industry self-regulatory efforts and believes such actions are an effective way to protect the privacy of the consumer. We fully support industry self-regulation and actively work with recognized trade associations and organizations in industry efforts to establish fair and workable guidelines above and beyond current laws and regulations.

We also support legislation and regulatory efforts to introduce fair and workable guidelines that protect the privacy of consumers, and actively work to ensure that such guidelines are consistent with and complement established self-regulatory measures, and that they enable the consumer to continue receiving the benefits that appropriate information use, sophisticated marketing techniques and transaction-processing services provide.

8. Ethical Relationships

MorphoTrust USA pledges to conduct our relationships with clients, vendors, business partners and other information providers in an ethical and professional manner. In our client and supplier contracts, MorphoTrust USA includes a commitment that any data sent to us has been legally obtained for the uses to which it will be put. Additionally, we require that our clients' subsequent use of any data received from us will be in compliance with all data protection laws, as well as with applicable industry information practices. Furthermore, we agree to comply with restrictions that information providers place on the data. If MorphoTrust USA has reason to believe that a client or an information provider is not in compliance with these commitments, MorphoTrust USA will exercise its rights under the contract, which include, but are not limited to, terminating that relationship.

9. Education and Awareness

MorphoTrust USA is committed to privacy education. We have initiated a program to educate our clients, our employees and the industry on an ongoing basis about the issues, guidelines and laws surrounding individual consumer privacy issues, corresponding responsibilities and MorphoTrust USA 's privacy policies and practices. MorphoTrust USA provides education and consultation to clients about privacy compliance, and about the laws and industry guidelines that protect consumer privacy. MorphoTrust USA provides advocates who speak at various events and emphasize the importance of responsible data collection and use.

Privacy and security are part of the culture at MorphoTrust USA. We provide information to all U.S. employees about the importance of privacy and data security. We provide ongoing education about the laws and accepted practices in which MorphoTrust USA conducts business. As changes in legislation or industry practices occur, special education may be provided to update our employees on the new practices.

At the time of initial employment and annually thereafter, all employees sign Privacy, Security, Confidentiality and Data Handling agreements stating they understand and agree to uphold MorphoTrust USA 's privacy and security policies as a condition of continued employment. This agreement also binds employees handling certain sensitive information to further protections in the handling of that data. When appropriate, MorphoTrust USA disciplines associates who violate our privacy policies

MorphoTrust USA
Cyber Security Plan

Document Number: PLN-00091-A
Revision Level: 02

Approval

Dennis Kallelis Chief Security Officer	Robert Eckel Chief Executive Officer
James Kottas Information Security Officer	John May Chief Information Officer

TABLE OF CONTENTS

1 INTRODUCTION

MorphoTrust USA, Inc. (“MorphoTrust”) operates under a Proxy Agreement and a National Security Agreement (NSA) with the U.S. Department of Defense (DoD) Defense Security Service (DSS) and U.S. Government Agencies (USGA), respectively. As part of these agreements, MorphoTrust is required to generate, maintain, and operate under an Electronic Communications Plan (ECP) and a Cyber Security Plan (CSP). This document is the CSP.

MorphoTrust operates a highly connected network environment that is used by both company information systems and customer production systems. Furthermore, the network can transmit and store two types of sensitive data:

1. Company confidential data, which includes company trade secrets, financial information, legal information, and Human Resource (HR) records.
2. Customer information, which often includes personally identifiable information (PII), which is very valuable to identity thieves.

It is critical for the success of MorphoTrust as a company and as a proxy organization to protect both types of sensitive data and make them secure throughout all MorphoTrust transactions. The goal of this CSP is to provide the policy framework for MorphoTrust which will ensure the security and protection of the sensitive data and the information systems that transmit or store the data from cyber-attacks.

MorphoTrust has identified a set of possible threats from its main security vulnerability policy:

- **SPC-00264-A** *Security Vulnerability Identification and Analysis*

Common cyber threats include:

- Unauthorized access of confidential information or PII data by MorphoTrust personnel, leading to theft of data. In this case, the attacker is likely to be at least somewhat knowledgeable about the systems they are trying to infiltrate.
- Unauthorized access of confidential information or PII data by non-MorphoTrust personnel. In this case, the attacker is attempting to infiltrate MorphoTrust systems by circumventing the security controls, processes, and procedures that MorphoTrust has in place to prevent such infiltration. However, in the case of a breach, the policies presented in this CSP can provide additional security to help mitigate this risk.
- Unauthorized access which is designed to inhibit normal network or systems operations.

Access to MorphoTrust-deployed systems in a customer’s environment is usually controlled by the customer. In case of a breach on the customer’s network, the CSP policies herein can help mitigate any possible damage and loss of PII data.

2 PURPOSE

The CSP defines the policies for protecting sensitive and confidential electronic data, information, and communication within the entire MorphoTrust environment, by externally-hosted MorphoTrust applications and services, and in deployed systems within customer environments.

Security considerations cannot be an afterthought when designing and implementing systems. The goal of the CSP is to make sure that security considerations are factored into the design and implementation of all systems that could be affected by a cyber-attack.

For existing systems that are in production, either for MorphoTrust's internal use or for providing actual customer services, it is possible that those systems may not be fully compliant with all of the policies in this CSP. It is understood that changes to those systems may incur unexpected costs, both for the customer as well as MorphoTrust, and with potential downtime which could seriously affect customer operations and services. When a subsystem that is suspected or at risk of noncompliance with the CSP is planned to be updated or changed, the MorphoTrust management in charge of the system should perform a risk/cost/benefit tradeoff in conjunction with the customer to determine if it is feasible and prudent to incorporate security updates at that time. For any security improvements which are deferred or declined, both the customer and MorphoTrust must fully understand and acknowledge the risks and potential costs of such a decision. If any security updates are required for compliance with the Proxy Agreement and the NSA, then the Facility Security Officer (FSO) and Information Security Officer (ISO) must be consulted first so that MorphoTrust does not fail to remain compliant with the Proxy Agreement and the NSA. The MorphoTrust FSO also functions as the Compliance Officer for the NSA.

For information on how electronic communications coming into or leaving the MorphoTrust environment (either by network or physically) for the purposes of compliance with the Proxy Agreement and the NSA, see the ECP:

- **PLN-00090-A** *MorphoTrust USA Electronic Communications Plan*

All MorphoTrust personnel are expected to comply with this CSP.

3 SCOPE

The CSP applies to all MorphoTrust personnel (employees, contractors, temporary employees, etc.) as well as MorphoTrust subsidiaries.

The CSP applies to all MorphoTrust information processing systems, whether they are hosted and maintained within MorphoTrust facilities or in secure third-party facilities.

Deployed systems are often installed within a customer's environment and thus may need to conform to the standards imposed or mandated by the customer. This often is true for production systems hosted by MorphoTrust, either internally or externally, for specific customers. In the absence of any customer mandates, guidelines or requests, the CSP should be followed for those deployments. If the customer cannot accept the level of security prescribed by the CSP, typically because of required compatibility with legacy customer systems, the MorphoTrust Program Manager or Product Manager for the project must get written permission from the customer to approve a lesser level of security. However, the lesser security level can only be used to accommodate the affected customer subsystems and not throughout all of the MorphoTrust systems in the deployment for that customer.

The CSP specifies a minimum level of security throughout all of its policies. Additional security measures can be added on an as-needed basis at the request of the appropriate subsystem owner(s), the customer, the MorphoTrust Legal Department, the Chief Security Officer (CSO), the FSO, or any other governmental requirement or mandate.

In addition, the CSP considers the CSO as the top-level corporate officer for cyber security issues. However, when dealing with proxy-related cyber security issues, the CSO should consult with the FSO for guidance and feedback.

If any parts of the CSP which deal with information coming into or going out of MorphoTrust are found to conflict with the ECP, the ECP shall prevail.

4 CYBER SECURITY PLAN

4.1 Preface

The overall description of the CSP starts with defining a set of terms categorizing the types of information that need to be protected. The distinction in the types of information will be important for defining and describing the security policies.

MorphoTrust uses a risk-based management approach for making decisions on security policy and actions, as discussed in:

- **PRC-00149-A** *Risk Management Plan*

In addition, MorphoTrust has an overall security governance policy in:

- **PRC-00173-A** *Security Governance Policy*

A high-level overview of the MorphoTrust's security philosophy, goals, and policies is in:

- **PUB-00185-A** *Security Quick Reference*

4.2 Definitions

4.2.1 Types of Information

The following definitions are used to describe the different types of information that need to be protected within the MorphoTrust environment.

Company Confidential Information – Any information that is both internal and confidential to MorphoTrust. Examples of this type of information include, but are not limited to, finance information, accounting information, Human Resource (HR) information, policy documents marked as confidential, company-owned intellectual property such as software source code, hardware designs, technical drawings and specifications. In general, customers do not see or have access to Company Confidential Information. Customer requests to see Company Confidential Information must be approved by both the Chief Executive Officer (CEO) and the Head of the Department which owns or maintains the requested information (for example, the Chief Finance Officer (CFO) in the case of requests for financial or accounting information).

Customer Confidential Information – Any information that is received from the customer in confidence or to be shared with the customer in confidence. The information may originate with the customer or it may originate within MorphoTrust (such as any program specifications for which the customer needs to sign off). Depending on the information involved, it may be considered as being both Customer Confidential Information and Company Confidential Information. In this case, the stronger of the security policies protecting Customer Confidential Information and Company Confidential Information shall hold, unless the CSO and ISO give explicit permission otherwise.

Confidential Information – Can be either Company Confidential Information or Customer Confidential Information or the combination of both types of information.

Personally Identifiable Information (PII) – The definition for PII is taken from the NSA between MorphoTrust and the United States of America, from section 1.1, bullet 'O', subsection (ii):

> U.S. and foreign citizen personally identifiable information/data (i.e., any information which can be used to distinguish or trace an individual's identity,

including but not limited to their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.)

Other definitions from the Federal government [1] are considered equally applicable.

Sensitive Information – Can be either Confidential Information or PII data.

4.2.2 Network Classifications

The following terminology is used when specifying security policies based on the network management:

Managed Network – A network that is controlled by MorphoTrust. In this case, MorphoTrust personnel have control over the necessary firewalls, routers and switches, and any other relevant networking equipment.

Unmanaged Network – A network that is not controlled by MorphoTrust. These networks usually are customer networks. Typically, the firewalls, routers and switches within a customer's environment are controlled by the customer and not MorphoTrust.

4.2.3 System Classifications

Internal System – A MorphoTrust computing system (examples: workstations, servers, peripherals, software, applications, etc.) that is located within a managed network and is used for normal business activities (HR, finance, payroll, engineering, etc.). Customers do not interact with these systems.

Deployed System – A MorphoTrust computing system (examples: workstations, servers, peripherals, software, applications, etc.) that is installed and operating in an unmanaged environment. Typically, deployed systems are contained within a customer's network. The systems usually are operated by the customer, and they may be supported and maintained by either the customer and/or MorphoTrust personnel. The hardware may be owned by the customer or MorphoTrust.

Internally-Hosted System – A MorphoTrust computing system that is operating within a managed network within a MorphoTrust facility and is accessible from an unmanaged network. In some cases, firewall rules are used to ensure that certain internally-hosted systems are only accessible from certain unmanaged networks.

Externally-Hosted System – A MorphoTrust computing system that is operating within a third-party's secure hosting environment and is running one or more MorphoTrust applications. The hosting facility's network is unmanaged but the MorphoTrust portion of the network is managed.

MorphoTrust-Controlled System – Refers to a system that is either an internal MorphoTrust system, an internally-hosted system, or an externally-hosted system.

Secure Network – A managed network that resides within a secure facility or a secure room within a secure facility [2] and uses access control technologies to control access to resources. The access control technologies can include identity-based, role-based, and/or rule-based access control lists (ACLs) as well as other authentication and authorization mechanisms.

Customer-Secured Network – A network that is managed by a customer and that resides within the customer's secure facility and uses access control technologies to control access to resources. The access control technologies can include identity-based, role-based, and/or rule-based ACLs as well as other authentication and authorization mechanisms.

4.3 Cyber System Overview

For the CSP, the MorphoTrust network system consists of six logical groupings:

1. An Admin Network which functions as a corporate network for administration and corporate functions (finance, accounting, HR, legal, etc.).
2. An Engineering Network for engineering development, testing, quality control, and internally-based customer support.
3. A Customer Network into which deployed MorphoTrust systems are installed. Often times, the Customer Network can include other subnets for development, testing, user acceptance testing (UAT), pilot implementations, and production.
4. A Factory Network which provides access to MorphoTrust production facilities.
5. A Customer Support Network (CSN, sometimes known as the Customer Solutions Network) which connects a Customer Network to a Factory Network and allows the Engineering Network access to it for maintenance and updates.
6. A Services Network which offers public-facing, Internet-accessible applications.

Firewalls with IP and port routing rules along with virtual local area network (VLAN) routing rules are used to control connectivity and access between these different logical networks. VLANs are used extensively within MorphoTrust to allow for finer control within these logical groupings.

The following table shows the type of data that can be stored or transmitted for the type of logical network:

Logical Network Type	Company Confidential Information	Customer Confidential Information	PII Data
Admin Network	Yes	Yes	Yes
Engineering Network	Yes	Yes	Yes[1]
Customer Network	No[2]	Yes	Yes
Factory Network	No	No	Yes
Customer Support Network (CSN)	No	Yes	Yes
Services Network	No	No	Yes

[1] The Engineering Network has only a limited amount of access-controlled PII data on it for development, testing, and investigating specialized problems, as authorized by management.

[2] There may be circumstances when certain Company Confidential Information will be shared with a customer or potential customer, with the appropriate approvals from MorphoTrust senior management. This information may be delivered to the customer by conventional electronic mechanisms such as email, and as such, may end up residing somewhere on the Customer Network.

> *However, customer environments are typically segmented so that the part of the Customer Network that would receive the Company Confidential Information is not same part of the network into which MorphoTrust-deployed systems are installed and operated. During normal delivery and operation of MorphoTrust systems within a customer's environment, no Company Confidential Information should be transmitted or stored by those systems.*

4.4 Organizational and Functional Responsibilities

The following roles have the specified responsibilities for ensuring and maintaining compliance with this CSP. Note that the role names may not correspond directly to the actual titles of MorphoTrust personnel. However, the responsibilities outlined below will be assigned to the appropriate individuals, regardless of their actual title.

Furthermore, because of the diverse types of products, programs, solutions, and services offered and supported by MorphoTrust, there can be multiple roles listed for a particular responsibility. However, for any particular information processing system or network, there should be one person, the **Primary Owner**, who is both responsible and accountable for it. If appropriate or necessary, a second person may be identified as a **Secondary Owner**, if the **Primary Owner** is temporarily unavailable.

At a high level, the roles and responsibilities of MorphoTrust are given in:

- **PRC-00174-A** *Information Security: Customer Data Access and Security Policy*

For internal MorphoTrust systems in the Admin Network and Engineering Network, the **Chief Information Officer (CIO)** is responsible for making sure they are compliant with the CSP. For the Factory Network and the CSN, the **Tier 3 Support Administrator** or the **CIO** is responsible for its systems. The **Services Manager** or the **CIO** is responsible for the Services Network. In the Customer Network, the responsibility for the systems may be some combination of the customer and the MorphoTrust **Program Manager**, **Product Manager**, or **Service Manager**.

For deploying systems into a customer's environment, the **Program Manager**, **Product Manager**, or **Service Manager** (collectively, the "**Responsible Manager**") that is assigned to the customer's contract or program is responsible for ensuring that a system to be deployed will be compliant with this CSP. A **Systems Engineer** or a **Product Designer** is responsible for ensuring the system design and architecture will be secure and compliant with this CSP. A **Development Engineer**, a **Quality Assurance Engineer,** and a **Delivery IT Engineer** should ensure that the software and systems they create, test, and configure will be secure and compliant with this CSP, especially when deployed or installed into a customer's environment. A **Configuration Engineer** should maintain the repository of software, configuration information, documentation, and any other build artifacts that are approved for release to a customer.

During installation and testing in the customer's environment, an **Integration Engineer** should monitor the state of the system's security and CSP compliance and identify any issues as soon as they are found to the **Responsible Manager,** and if applicable, the **Systems Engineer**. If these issues cannot be remedied due to customer limitations, the **Responsible Manager** should get a written release from the customer which explicitly allows for the lesser security in their environment. (See Section 4.18 for more information.) A copy of the release should be forwarded to the **CSO** and **ISO**. If any network infrastructure needs to change during installation and testing, the **Systems Engineer** should review and approve the change to ensure that it does not compromise security or CSP compliance, and then they should issue the change request to the IT Department.

For deployed systems, the **Operations Manager** for the customer will periodically monitor the deployed systems for compliance at least once a year, and report the findings to the ISO. The status of the compliance must be reevaluated when the system is changed or updated in any significant way, either by MorphoTrust or by the customer. A **Tier 3 Support Engineer** can assist the **Operations Manager** with this task. If any new compliance issues are identified, they should be addressed as soon as possible. However, if they cannot be remedied because of customer limitations, the **Operations Manager** should get a written release from the customer which explicitly allows for the lesser security in their environment. (See Section 4.18 for more information.) A copy of the release should be forwarded to the **CSO** and **ISO**.

For both internally-hosted systems and externally-hosted systems, the **CIO**, the **Tier 3 Support Administrator**, or the **Service Manager** is responsible for making sure the network and operating system (OS) configurations are secure and compliant with the CSP, including regular patching, updating, and monitoring. For the applications being hosted, the responsible MorphoTrust party or **Primary Owner**, typically a **Product Manager**, **Program Manager** or **Service Manager**, is responsible for ensuring that the applications and any associated databases are secure and compliant.

For internal corporate applications and databases on the Admin Network such as HR, Finance and Accounting systems, the **CIO** is responsible for securing them. Furthermore, the **CIO** is the data owner for company confidential information and all data processed and stored on internal systems in the Admin Network. The **Configuration Manager** is the data owner for all development outputs on the Engineering Network, such as software, source code, build instructions, technical documentation, quality control information, etc.

When any role becomes unfulfilled due to the loss of MorphoTrust personnel, the **Manager** of that role assumes the responsibility for security and compliance until the role can be properly staffed or reassigned. The titles of the responsible MorphoTrust personnel may not match the role name, but their expected duties and/or job description will include the responsibilities of the role.

Finally, all MorphoTrust personnel are responsible for protecting the sensitive and confidential information and resources to which they have access, and to report suspected security incidents to their **Manager**, the **CSO** and the **ISO**.

4.5 Information Policy

All information, regardless of the form or format, which is created, acquired or used in support of MorphoTrust business activities, must be used only for MorphoTrust business. MorphoTrust information is an asset and must be protected from its creation, through its useful life and to its authorized disposal. It must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use.

Information security management enables information to be shared while ensuring protection of that information and its associated computer assets including the network over which the information travels. MorphoTrust-designated staff is responsible for ensuring that appropriate physical, logical and procedural controls are in place on these assets to preserve the security properties of confidentiality, integrity, availability and privacy of sensitive information.

Individual accountability is the cornerstone of any security program. Without it, there can be no security. Usernames or IDs must not be shared and must be unique enough to identify each person individually. Furthermore, each person must treat their account passwords as confidential information and not disclose them to anyone. In addition, each person must reasonably protect against unauthorized activities.

The use of built-in user accounts (such as Administrator) that are shared among users, especially privileged users, should be discouraged as much as possible. For practical reasons, though, specialized situations, such as the need to maintain large numbers of similar or identical workstations by multiple people, may require the use of common user accounts, but these accounts should not be built-in accounts if possible, and their usage should be logged.

Confidential information and PII data should only be made available on a Need-To-Know basis according to:

- **PRC-00141-A** *Need To Know Policy*

Furthermore, MorphoTrust personnel shall only be given the minimum necessary privileges, often called Least Privilege, to perform their normal business duties. Any increase in privileges must be approved by their manager and by the role in charge of the information systems for the relevant network zone.

MorphoTrust also has a privacy policy which provides the overall framework for dealing with sensitive information:

- **PRC-00144-A** *Privacy Policy*

MorphoTrust will maintain appropriate processes and procedures for reasonable and timely recovery of all information processing systems, applications, and data in a secure way, without causing information to become corrupt, destroyed, or unavailable for an unreasonable amount of time.

Confidential information and PII data that is old, obsolete, invalid, or inaccurate should be deleted or disposed of promptly and properly.

MorphoTrust has an overarching policy for the protection of customer data:

- **PRC-00174-A** *Information Security: Customer Data Access and Security Policy*

MorphoTrust has its general IT security policies given in:

- **PRC-00112-A** *IT Security Policy*

When new projects or programs are started, the security considerations that should be incorporated are described in:

- **PRC-00111-A** *Project Security Policy*

4.6 Organizational Security Policy

The **ISO** is the main authority for any questions or interpretation issues on the CSP. The **CSO** is main authority for resolving any conflicts between the CSP and practical implementation or customer issues. If any issues involve compliance risks with the Proxy Agreement or the NSA, the **FSO** must be consulted.

If any security event or incident occurs due a breach in compliance with the CSP, the **CSO** must be notified promptly.

4.7 Personnel Security Policy

The intent of the Personnel Security Policy is to reduce the risk of human error and misuse of sensitive information and facilities to an acceptable level.

Security roles and responsibilities must be documented and they should include general responsibilities for all MorphoTrust personnel. Whenever possible, they should include specific responsibilities for protecting specific confidential information and performing tasks related to the relevant security processes and/or procedures.

MorphoTrust has a policy for screening potential employees and contractors to evaluate their security risk and potential:

- **PRC-00134-A** *Employee Security Screening Policy*

MorphoTrust has a security awareness training policy that must be followed:

- **PRC-00152-A** *Security Training Awareness Policy*

MorphoTrust also has a policy so individuals can understand the liability issues involved with protecting sensitive information:

- **PRC-00140-A** *Liability Policy*

4.8 Physical and Environmental Security Policy

Critical sensitive information processing and storage facilities must be contained in secure areas protected by a defined security perimeter, with appropriate security barriers and physical access controls. Physical protection measures must be implemented to protect each facility from unauthorized access, damage and interference.

4.8.1 MorphoTrust Facilities

All MorphoTrust facilities have physical security, such as controlling access to the building and to secure rooms within the building or facility. The **CSO** will perform periodic threat and risk analysis to determine where additional physical security measures are necessary, and implement these measures to mitigate the risks.

MorphoTrust has several policies for protecting the physical and environmental aspects of its facilities:

- **PRC-00098-A** *Building Access & Badging Policy*
- **PRC-00136-A** *Security Events Planning Policy*

Secure server rooms within MorphoTrust facilities have their own security policy:

- **PRC-00091-B** *Physical IT Access Controls Policy*

Special consideration is given to MorphoTrust card production facilities to make them compliant with NASPO security requirements:

- **PRC-00147-A** *Building Access and Badging Policy for Production Facilities*
- **PRC-00133-A** *MorphoTrust USA Central Production Center Physical Security* and its associated policies (PRC-00121-*x*, PRC-00122-*x*, SPC-00255-*x*, where *x* is a letter).
- **SPC-00280-A** *MorphoTrust USA NASPO Production Centers Security*

Information processing terminals on the corporate domain such as workstations must automatically screen-lock themselves after a fixed period of inactivity, as outlined in:

- **PRC-00089-B** *IT Information Security Policy*

Users must re-authenticate in order to gain access to the system again.

To protect against sensitive information from escaping on aging media or media that is to be reallocated, the information and, if applicable, the media should be destroyed according to the policies in:

- **PRC-00146-A** *Destruction of Electronic Media Policy*

4.8.2 Customer Environments

When new projects or programs are started that will be deployed into customer environments, the physical security considerations that should be addressed are described in:

- **PRC-00111-A** *Project Security Policy*

These considerations also factor in the physical security measures that are required in the customer's environment into which MorphoTrust systems will be deployed. The lack of sufficient physical security protections, such as in the customer's front offices, will require that any sensitive data (typically PII data) is protected with additional means, such as encryption.

4.8.3 Third-Party Environments

For any MorphoTrust systems that are hosted in third-party environments, these environments must be secure data centers with appropriate policies, processes and procedures to ensure the protection of the MorphoTrust systems from any non-MorphoTrust individuals. The third-party management of their facility should include risk management policies, incident reporting procedures, and escalation processes to mitigate the effects of a suspected breach. If a suspected breach occurs, both the **CSO** and **FSO** must be notified as soon as possible. The **CSO** then will notify immediately the **CEO** and the **GSC Chair**, who will be responsible for informing the DSS and the USGA as appropriate.

4.9 Communication Policy

MorphoTrust has its main corporate communications policy in:

- **PRC-00123-A** *Communications Policy*

Furthermore, IT has a policy on electronic communications and email usage in:

- **PRC-00113-A** *IT Electronic Communication Policy*

Email is saved and archived for logging, legal, and monitoring purposes, according to:

- **PRC-00114-A** *E-Mail Archiving and Retention Policy*

4.10 Network Management Policy

4.10.1 Network Management

All MorphoTrust networks will implement appropriate security controls to ensure the integrity of the data flowing across these networks. If there is a business need, additional measures to ensure the confidentiality of the data shall also be implemented.

The **ISO** will ensure that measures are in place to mitigate any new security risks created by MorphoTrust systems programmatically accessing a third-party network for special or dedicated services.

Where MorphoTrust has outsourced a server or application to a third-party service, such as web applications or Software as a Service (SAAS), the **CSO** or **ISO** or their designated staff must perform or have performed periodic security reviews of the outsourced environment to ensure the security and availability of MorphoTrust's information and application.

All connections to the MorphoTrust network must be authorized by the **Responsible Manager**. Connections to the Admin and Engineering Networks also require **CIO** approval. Connections to the CSN require the approval of the **CIO** and the **Tier 3 Support Administrator**. Additions or changes to network configurations must be reviewed and approved through the MorphoTrust Change Control Board according to the policy:

- **PRC-00085-B** *IT Change Management Policy & Procedure*

Reasonable computer use on the MorphoTrust network is governed by:

- **PRC-00110-A** *IT Computer and System Use Policy*
- **PRC-00086-B** *Computers on the Network*

Similarly, MorphoTrust has a policy on cell phones and mobile devices such as tablets to protect access to the network:

- **PRC-00237-A** *Cell Phone and Mobile Devices Use Policy*

MorphoTrust has a policy for remote access to its network:

- **PRC-00092-B** *IT Remote Access Policy*

4.10.2 Vulnerability Scanning

MorphoTrust systems that are accessible from outside the network must be periodically scanned on a regular basis for vulnerabilities and weaknesses. Additional scans should be performed when the systems have been updated in some manner, either with application changes or OS configuration changes. For both internal and external systems, scans will be performed at least annually to ensure that no major vulnerabilities have been introduced into the environment. The frequency of additional scans will be determined by the **CSO** and the **ISO**, and it will depend on the criticality and sensitivity of the information on the system. This scanning should include the CSN and any systems hosted in third-party facilities.

Network vulnerability scanning will be conducted after new network software or major configuration changes have been made on systems that are essential to supporting a process that is critical to MorphoTrust business, and annually on all other systems. The output of the scans will be reviewed in a timely manner by the **CSO** and **ISO**, and any vulnerability detected will be evaluated for risk and mitigated. The tools used to scan for vulnerabilities will be updated periodically to ensure that recently discovered vulnerabilities are included in any scans.

Only the CSO or their designated authority can authorize and approve vulnerability scanning. Anyone authorized to perform vulnerability scanning must have a process defined, tested and followed at all times to minimize the possibility of disruption. Reports of exposures to vulnerabilities will be forwarded to the **CSO** and **ISO** and other designated staff.

4.10.3 Penetration and Intrusion Testing

All MorphoTrust computing systems that are accessible from outside of MorphoTrust will be subjected to penetration analysis and intrusion testing. Such analysis and testing will be used to determine if:

- An individual can make an unauthorized change to an application;
- A user may access the application and cause it to perform unauthorized tasks;
- An unauthorized individual may access, destroy or change any data; or
- An unauthorized individual may access the application and cause it to take actions unintended by the application designer(s).

The output of the penetration testing and intrusion testing will be reviewed in a timely manner by the **CSO** and **ISO**, and any vulnerability detected will be evaluated for risk and mitigated as appropriate.

The penetration and intrusion testing should include the CSN and the MorphoTrust systems hosted at third-party facilities.

The tools used to perform the penetration testing will be updated to ensure that recently discovered vulnerabilities are included in any testing.

Only individuals authorized by the **CSO** are authorized to perform penetration testing. The **CSO** must be notified when penetration testing will be performed. Any other attempts to perform such penetration testing will be deemed an unauthorized access attempt.

MorphoTrust currently contracts with a third-party security company to perform ethical hacking on its networks to try to identify potential security issues.

4.10.4 Networking Devices

All networking devices must be approved by the MorphoTrust IT Department before they are connected to the MorphoTrust network. Unapproved devices must not be connected to the MorphoTrust network at any time.

4.10.5 Wireless Networks

Advances in wireless technology and pervasive mobile devices create opportunities for new and innovative business solutions. However, security risks, if not addressed correctly, could expose information processing systems to a loss of service or a compromise of sensitive information.

Wireless networking is a shared medium. Everything that is transmitted over the radio waves can be intercepted if the interceptor is within the coverage area of the radio transmitters. This represents a potential security issue with wireless Local Area Networks (LANs). The security exposure is more evident if the wireless LANs are deployed or used in public areas, both in MorphoTrust facilities (such as shared building areas) and in customers' environments.

Authentication and strong encryption must be implemented to ensure that a wireless network or access point cannot be exploited to disrupt sensitive information services or to gain unauthorized access to sensitive information. When applicable and practical, suitable controls should be used as well, such as Media Access Control (MAC) address restrictions or Remote Authentication Dial In User Service (RADIUS) authentication with access profiles. When selecting wireless technologies, 802.11x wireless network security features on the equipment must be available and implemented from the beginning of the deployment. All wireless networks must be secured by the MorphoTrust IT Department.

Access to systems that hold sensitive information or the transmission of sensitive information via a wireless network is not permitted unless appropriate and adequate measures have been implemented and approved by the **CSO** and **CIO**. Such measures must include authentication, authorization, strong encryption, access controls and logging.

4.10.6 Publicly-Accessible Websites

Because anything posted on a public web server is globally available and each web presence is a potential connection path to the MorphoTrust network, care must be exercised in the deployment of publicly accessible servers. There is also potential for an insecure server to be used or exploited to assist in an unauthorized or illegal activity, such as an attack on internal MorphoTrust systems or other web sites.

Sensitive information must not be made available through a server that is available to a public network without appropriate safeguards approved by the **CSO** and **CIO**. The **ISO** and designated IT staff will ensure that user authentication, data confidentiality and integrity, access control, data protection, logging and monitoring mechanisms are sufficient to protect the sensitive information.

4.11 Operational Management Policy

MorphoTrust has a general operations management policy in:

- **PRC-00090-B** *IT Managing Operations Policy*

4.11.1 Segregation of Security Duties

To reduce the risk of accidental or deliberate system misuse, separation of duties or areas of responsibility must be implemented where practical.

Whenever separation of duties is difficult to achieve, other compensating controls such as monitoring of activities, audit trails and management supervision must be implemented. At a minimum, the audit of security must remain independent and segregated from the security function.

4.11.2 Separation of Development, Test and Production Environments

It is preferable to have engineering development environments, quality assurance (QA) test environments, user acceptance testing (UAT) environments, and production environments to be separated from one another, either logically or physically or both. Processes should be documented and implemented to govern the transfer of software from the engineering development environment on through QA and UAT testing and into the production environment. The following controls should be considered:

- Development software and tools should be maintained on systems isolated from the production environment. Development software should be contained on physically separate machines or separate them by access-controlled domains, VLANs, or directories;
- Access to compilers, editors and other system utilities should be removed from production systems when not required;
- Logon procedures and environmental identification should be sufficiently unique for all environments;
- Whenever possible with production systems, controls should be in place to issue short-term access to development staff to correct problems with production systems, allowing access only as necessary.

Depending on the complexity of the system, performing development, QA testing or UAT testing could cause serious problems to an existing production environment if separation of these environments does not exist. The degree of separation between the production and UAT environments should be considered by the **Responsible Manager** to ensure adequate protection of the production environment.

To the extent that it is practical, separation should also be implemented between engineering development and QA test functions so that engineering changes are not introduced into the QA testing area in a way which bypasses the above controls or configuration management. In addition, each **Responsible Manager** should consider the use of a stable UAT environment where the customer can test the system without changes being made to the system.

When creating a new system and before it has been put into production, it is acceptable and often necessary for the UAT environment to become the production environment once the UAT has finished successfully. It is also acceptable that specialized tests for compliance with service level agreements (SLAs) be run against production environments.

4.11.3 Protection against Malicious Code

Software and associated controls must be implemented across MorphoTrust systems to prevent and detect the introduction of malicious code. The introduction of malicious code, such as a virus, network worm program or Trojan horse, can cause serious damage to networks, workstations and business data, particularly sensitive information. Users must be made aware of the dangers of unauthorized or malicious code. MorphoTrust must implement controls to detect and prevent a virus from being introduced to the MorphoTrust environment. The types of controls and frequency of updating signature files, is dependent on the value and sensitivity of the information that could be potentially at risk. For most MorphoTrust workstations, virus signature files must be updated daily. On host systems or servers, the signature files will be updated daily or when the virus software vendor’s signature files are updated and published.

MorphoTrust has an antivirus policy to help reduce the chance of malware causing damage or information loss:

- **PRC-00093-B** *IT Virus Protection Policy*

MorphoTrust also uses web-filtering technologies to reduce the chance of malware entering the network through web browsing.

4.11.4 Software Maintenance

Computing systems in all logical network types should keep their commercial software installations current and update to date with patches, fixes, etc. This includes OS-level updates and fixes (such as from Microsoft Update). For computing systems in the Customer Network, if the customer assumes the responsibility for the updates and fixes to non-MorphoTrust applications, the **Responsible Manager** should ensure that the updates will be done with a reasonable frequency for the environment and understand the level of risk involved with making these changes.

Computing systems in all other logical network types should evaluate the fixes and updates to see if they pose any risk to production systems. If so, the fixes and updates should be tested separately before being deployed. If a particular fix or update poses an identifiable risk to production, and if the systems are on a secure network, the fix and update can be deferred until either the fix or the update has been tested fully, or reissued by the manufacturer so it is less risky, or until there can be a sufficient break in production that it can be installed and tested safely and, if necessary, backed out or reverted.

4.11.5 Information Backup

Computing systems need their data, configuration, and any other important information backed up to prevent data loss and make possible business continuity and disaster recovery.

For computing systems on the Admin and Engineering Networks, their relevant data, including sensitive information, should be backed up according to the MorphoTrust policy:

- **PRC-00084-B** *IT Backup & Recovery Policy*

Similarly, the backups should be capable and useful in the case of a disaster and the sensitive information needs to be recovered in a reasonable timeframe. MorphoTrust has a disaster recovery policy in:

- **PRC-00095-B** *IT Disaster Recovery Policy*

4.12 Access Control Policy

To preserve the properties of integrity, confidentiality and availability, MorphoTrust's information assets must be protected by logical and physical access control mechanisms commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements and ease of recovery of these assets.

Responsible Managers and other relevant information owners are responsible for determining who should have access to protected resources within their purview, and what those access privileges will be (read, write, update, etc.). These access privileges will be granted in accordance with the user's job responsibilities.

For any type of device on the MorphoTrust network, if it has any accounts or access methods with any default passwords, those passwords must be changed to be secure passwords that are compliant with all applicable policies and guidelines.

4.12.1 User Registration and Management

A user management process shall be established and documented by the MorphoTrust **Human Resources** (HR) and **IT Departments** to outline and identify all functions of user management, to include the generation, distribution, modification and deletion of user accounts for access to resources. The purpose of this process is to ensure that only authorized individuals have access to MorphoTrust applications, network resources, and information and that these users only have access to the resources required for authorized purposes. The principle of Least Privilege always should be followed, as described in:

- **PRC-00141-A** *Need to Know Policy*

The user management process should include the following sub-processes as appropriate:

- Enrolling new users;
- Removing user IDs;
- Granting "privileged accounts" to a user;
- Removing "privileged accounts" from a user;
- Periodic reviewing "privileged accounts" of users;
- Periodic reviewing of users enrolled to any system; and
- Assigning a new authentication token (e.g., password reset processing).

These sub-processes are typically part of the HR Add/Drop procedure for bringing on-board ("onboarding") a new MorphoTrust employee or contractor, or when a MorphoTrust individual leaves the company ("offboarding").

The appropriate **Responsible Manager** or other authorized person will make requests for the registration and granting of access rights for MorphoTrust personnel.

4.12.2 Privileged Accounts Management

The issuance and use of privileged accounts will be restricted and controlled. Inappropriate use of system account privileges is often found to be a major contributing factor to the failure of systems that have been breached. Processes must be developed to ensure that uses of privileged accounts are monitored, and any suspected misuse of these accounts is promptly investigated.

4.12.3 User Password Management

Passwords are a common means of authenticating a user's identity to access an information system or service. Password standards must be developed and implemented to ensure all authorized individuals accessing MorphoTrust resources follow proven password management practices. These password rules must be mandated by automated system controls whenever possible.

The MorphoTrust policy on user passwords is in:

- **PRC-00089-B** *IT Information Security Policy*

The use of two-factor authentication methods is encouraged whenever possible and practical.

4.12.4 Service Account Management

Background processes and services that run on MorphoTrust computing systems all require some identity by the OS. Background processes and services that are created by MorphoTrust and run as part of MorphoTrust products, programs, and solutions must also have an identity. Consideration must be given as to the identity of MorphoTrust background processes and services and the security implications involved. In general, the MorphoTrust service account identities should be distinguishable and unique to allow to monitoring, logging, and resource tracking. The use of existing OS-level service and network accounts is discouraged unless it is required to make the system be functional and operational. However, customer policies and standards may require or forbid the use of service accounts, so suitable accommodations should be made with security in mind.

The service accounts should be considered as a form of privileged account because they provide a means of controlling how an application works along with aspects of the security associated with those applications.

4.12.5 Security Group Management

A security group is a collection of user IDs or other security groups. It can be used to assign a common set of privileges and access rights to a group of users. Requests to add a user to a particular security group must be approved by the **Responsible Manager** or their designated authorities.

Security groups should be considered for use in MorphoTrust applications whenever multiple users should be granted the same privileges. Similarly, nested security groups should be considered whenever more-privileged users should inherit the privilege levels of less-privileged users. When designing a structure of security groups, considerations for domain trust relationships such as with one-way and two-way trusted domains must be included. In the absence of guidance or requirements from either MorphoTrust or customer environments, the structure of security groups should be as simple as possible to keep it maintainable and to prevent security errors from being introduced, for example, by complex nesting, which could give users more privileges than they should have.

4.12.6 Network Access Control

Access to any internal MorphoTrust network must require all authorized users to authenticate themselves through the use of an individually assigned user ID and one or more authentication mechanisms, e.g., password, token, smart card, etc. Network controls must be developed and implemented that ensure that an authorized user can access only those network resources and services necessary to perform their assigned job responsibilities.

To maintain information security, MorphoTrust requires that individual accountability be maintained at all times, including during remote access.

Connections to any internal MorphoTrust network must be done in a secure manner to preserve the integrity of the network, the data transmitted over that network, and the availability of the network. Security mechanisms must be in place to control access to MorphoTrust systems and networks remotely from fixed or mobile locations.

When accessing a MorphoTrust network remotely, identification and authentication of the entity requesting access must be performed in such a manner as to not disclose the password or other authentication information that could be intercepted and used by a third party.

In the special case where servers, storage devices or other information technology equipment has the capability to automatically connect to a third-party vendor for processing services or to report problems or suspected problems, the **CSO**, **ISO**, **CIO** and the **Responsible Manager** must review any such connection and process to ensure that the connectivity does not compromise MorphoTrust or other third-party connections.

Working from a remote location must be authorized by MorphoTrust **Management** and appropriate arrangements made for this activity through written policy and procedure, to ensure the work environment at the remote location provides adequate security for MorphoTrust data and computing resources. Appropriate protection mechanisms commensurate with risk and exposure must be in place to protect against theft of MorphoTrust equipment, unauthorized disclosure of sensitive information, misuse of MorphoTrust equipment or unauthorized access to the MorphoTrust internal network or other facilities by anyone, including family and friends. To ensure the proper security controls are in place and all MorphoTrust security standards are followed, the following must be considered:

- The physical security of the remote location including using a laptop at any location other than an employee’s work station;
- The accessing mechanism, given the sensitivity of MorphoTrust’s internal systems and method of transmitting information; and
- Appropriate business continuity procedures including backing up critical information.

Encryption requirements are described in the policy:

- **PRC-00233-A** *Data Encryption Policy*

4.12.7 Remote Access Control

The MorphoTrust policy on remote network access by approved users is in:

- **PRC-00092-B** *IT Remote Access Policy*

4.12.8 Segregation of Networks

For the different logical networks, the MorphoTrust **IT Department** should only allow connections to be made between them when there is legitimate business reason as identified by MorphoTrust

Management. IT can use any and all of its technologies for implementing access control between the logical networks, including using firewall rules, IP/port/VLAN routing rules, identity-based access controls, and requiring special jump boxes as a high-level access bridge between two networks, such as accessing individual customer VLANs in the CSN.

No connections originating in the CSN should be allowed to terminate in the Admin or Engineering Networks.

The general policies for governing the segregation between networks are in:

- **PRC-00089-B** *IT Information Security Policy*
- **PRC-00088-B** *IT Firewall Policies and Procedures*

Any specific network segregation policy for compliance with the Proxy Agreement and the NSA is covered in:

- **PLN-00090-A** *MorphoTrust USA Electronic Communications Plan*

4.12.9 Operating System Access Control

Access to local administrative OS-level user accounts is a special type of privilege that must be guarded carefully. Unauthorized access could lead to a significant breach of security, including a loss of operational functionality as well as a leakage of sensitive information. These accounts could be the system's Administrator account (or root or its equivalent) or special user accounts that have local administrative privileges and are intended for use with maintaining or updating MorphoTrust applications.

Computing servers are usually involved in processing sensitive information in a variety of ways. For example, they can be functioning as web servers, file servers, application servers, workflow servers, database servers, communication servers, and so on. For most if not all of these functions, the servers are handling or storing sensitive information, and thus they should be protected more from any potential break-in attack or spread of attacks.

On server machines in production environments or customer environments, the passwords for local administrative accounts should be different for every machine. Non-built-in Administrator accounts should only have the privileges necessary to administer the machine and the MorphoTrust applications. If possible, the built-in Administrator account should be renamed. Any guest accounts should be disabled. The default passwords for all default accounts should be changed.

For several types of deployments, computing devices (workstations, servers, networking gear, etc.) may be logically organized into groups of devices that are configured in the same way and provide the same functionality within a group. In production environments or customer environments, the local Administrator account on these groups of devices may be the same on all devices or within a group, provided the devices are on a secure network or a customer-secured network. This usually is necessary when the number of computing devices is large, such as a large number of client workstations.

Passwords on all computing devices should not be reused between different programs or customers.

4.12.10 Application Access Security Policy

All access to publicly-available MorphoTrust services (such as web applications and FTP sites) that require authentication should use a secure logon process so that usernames and passwords are protected at all times. All access should be logged.

If a secure transport mechanism such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL) is used during the login process, it must continue to be used throughout the duration of the login session.

4.12.11 Cloud Environments

Utility-like computing environments like third-party cloud infrastructure services (Infrastructure as a Service, or IAAS), cloud platform services (Platform as a Service, or PAAS), or cloud application services (Software as a Service, or SAAS) can only be considered for MorphoTrust use provided:

- The security of the environment, applications, and any stored sensitive information can be guaranteed to a very low level of risk, even from the third-party cloud vendor itself; and
- The intended marketplace and/or customers are amenable to a cloud solution, possibly with additional restrictions and conditions.
- The use of the environment does not cause MorphoTrust to become non-compliant with either its NSA and proxy agreements or state cyber laws and regulations.

MorphoTrust can host its own cloud environment, provided the above conditions are met as well.

4.12.12 Application Monitoring Systems

Wherever feasible, systems to monitor the status and health of the MorphoTrust applications, particularly in customer environments, the CSN, the Factory Network, and the Service Network, along with the health of the servers running the applications should be monitored at regular but frequent intervals, especially before and during production periods. Any loss in service or the availability of an application or a server could indicate a possible attack, so the cause of the loss of functionality should be investigated immediately. Automated notification mechanisms should be in place to notify the appropriate personnel when any such outage occurs. If a possible security condition is detected, it must be reported to the **CSO** and **ISO** immediately.

4.13 Information Security Policy

All active sensitive information must always be stored on a secure network or a customer-secured network. The policies governing the storage and handling of sensitive data are given in:

- **PRC-00148-A** *Sensitive Data Handling and Storage Policy*
- **PRC-00174-A** *Information Security: Customer Data Access and Security Policy*

PII data should be protected with encryption according to the policy in:

- **PRC-00233-A** *Data Encryption Policy*

PII data must not be stored on removable media as stated in:

- **PRC-00150-A** *Removable Media Policy*

However, it is possible that customers may send or deliver PII data to MorphoTrust for analysis, evaluation, and diagnostic purposes. If the PII data is transmitted electronically to MorphoTrust in an unprotected format, it should be moved to the MorphoTrust secure network. If the PII data is transmitted to MorphoTrust via a customer email in the course of researching a customer issue, the PII data should be removed from the email before forwarding the email to other MorphoTrust personnel. In this case, the PII data should be saved temporarily on a secured MorphoTrust server and protected with ACLs. References to the network location with the PII can be passed around via email. When the issue has been resolved, the PII data should be deleted within a week. If any email replies to the customer require the PII data for referencing purposes, only a minimal or incomplete amount of PII that is uniquely identifiable by the customer should be included in the email reply.

Unencrypted PII data that is reported to the MorphoTrust Help Desk by customers in the course of opening a service request ticket should not be stored in the ticket on a long-term basis. Small amounts of PII data should be stored in a secure data field while the ticket is open and then be deleted when the ticket is closed. Large amounts of PII data should be stored on a secured MorphoTrust server and protected with ACLs. References to the PII data can be included in the ticket or in emails regarding the ticket. When the ticket is closed, the PII data associated with the ticket should be deleted within a week.

PII data can be emailed to a customer or within the MorphoTrust network provided:

a. The PII data remains encrypted at all times. The encryption level should be AES-128 or better.[1]

b. The encryption password or key for the encrypted PII data is not transmitted with the encrypted PII data. The password or key must be transmitted separately, preferably using a different mechanism (i.e., “out-of-band”).

c. The recipients must have a need-to-know of the PII data in order to perform their duties in support of a customer contract.

If the PII data is delivered on physically removable media, the PII data contents of the media should be transferred to the MorphoTrust secure network and the media should be locked in a secure cabinet with limited or controlled access. Alternatively, the media can be properly erased or destroyed if requested by the customer or the supervising **Responsible Manager**. If the removable media is to be destroyed, it should be done according to:

- **PRC-00146-A** *Destruction of Electronic Media Policy*

Any sensitive information that is backed up or archived should follow the appropriate polices in:

- **PRC-00084-B** *IT Backup & Recovery Policy*
- **PRC-00124-A** *MorphoTrust USA DL/ID Installation Data & Security Policy*
- **PRC-00233-A** *Data Encryption Policy*

If sensitive information is to be backed up or archived at an off-site location that is maintained by an approved third-party backup provider, the following conditions should be enforced:

- The sensitive information must be encrypted using a reasonably strong encryption algorithm. While the strongest encryption algorithms are preferable, their increased computational demands may not be practical for very large amounts of data.
- The encryption key must remain under the control of MorphoTrust and should not be available to the third-party backup provider.
- The encryption key must not be included in the backup or the archive. However, encoded references may be included if multiple encryption keys are used over time, such as saying that a particular backup set uses encryption key #6.

[1] The encryption of Microsoft Office Open XML format files like .docx and .xlsx uses AES-128 by default. If stronger encryption is desired, a Windows registry setting needs to be updated to set the default key length to 256 bits for AES-256.

If a backup set or archive of sensitive data needs to be shipped from one MorphoTrust facility to another MorphoTrust facility or a third-party backup facility, the sensitive data must follow the above conditions and be hand-carried, if possible. Otherwise, a reputable shipping company that can track its shipments should be used.

If there is a leakage or spill of any sensitive information to unauthorized individuals, the procedures for handling this case are in:

- **PRC-00312-A** *Information Spills and Cleanup Policy*

4.14 Technology Security Policy

For compliance with the ECP, MorphoTrust has the following technology control plan to prevent unwanted leakage of technology assets outside of the company and the country:

- **PLN-00088-A** *MorphoTrust USA, Inc. Technology Control Plan*

4.15 Database Security Policy

In many areas of MorphoTrust, sensitive information is stored in databases, usually within either the MorphoTrust network or within the customer's environment. Many of these databases contain large amounts of PII data, and so their security is paramount.

All logins to databases in the following environments must use strong passwords that are given only to MorphoTrust personnel with a legitimate need to know:

- MorphoTrust databases with company sensitive information (such as HR, Finance, and Accounting databases); or
- Deployed databases in customer UAT or production environments; or
- UAT or production databases with customer data in them that are hosted within MorphoTrust or by MorphoTrust in a third-party facility; or
- MorphoTrust Help Desk databases with customer service request information; or
- MorphoTrust Engineering development and testing databases with real (as opposed to fake) PII data in them; or
- Internal MorphoTrust databases for storing intellectual property, documentation, configuration management information, and QA information, or any other type of information used to create MorphoTrust products, programs, solutions, and services.

Internal databases used for Engineering development and testing that contain fake PII data or data from the MorphoTrust developers or testers can use shared strong passwords for ease of development and testing, since the risk of PII data loss is low. All such internal databases must reside on a MorphoTrust managed network. All database logins must have strong passwords, including the database administration accounts.

For any given customer, databases for engineering development and QA testing should use different passwords whenever possible and practical. Production databases must use different passwords from both the engineering development databases and the QA testing databases. If possible, UAT databases should use different passwords than the production databases, subject to the requirements, limitations and constraints of the customer. All UAT and production databases across all customers should not have any passwords in common, unless the passwords are set by the customers and by coincidence one or more passwords are the same.

Database usernames may be the same across any databases as necessary or desired. Common usernames pose a low security risk and can make the management of the database more efficient, reliable, and less prone to error.

Application access to the various internal MorphoTrust databases may use application-level user management, authentication management, and authorization management to control access to these databases, according to the level of risk associated with the information in those databases, as determined by MorphoTrust **Management**.

4.16 Systems Development and Maintenance Policy

Software applications are developed or acquired to provide efficient solutions to both MorphoTrust business problems and customer identity management opportunities. These applications can store, manipulate, retrieve and display information used to conduct MorphoTrust business or customers' business. Both MorphoTrust and its customers will become dependent on these applications, and it is essential the data processed by these applications be accurate. It is also critical that the software that performs these activities be protected from unauthorized access or tampering.

To ensure that security is built into all MorphoTrust information systems, all security requirements, including any need for rollback arrangements, must be identified as much as possible during the requirements phase of a project and justified, agreed to and documented as part of the overall business case for both a MorphoTrust information system and one that is built to a customer's specifications.

Controls in systems and applications can be incorporated in many places and serve a variety of purposes. The specific control mechanisms should be documented at the application level. If possible, the security measures that are implemented should be based on the threat and risk assessments of the information being processed and cost/benefit analysis.

4.16.1 Input Data Validation

An application's input data must be validated to ensure it is correct and appropriate including the detection of data input errors. The checks that are performed on the client side must also be performed at the server to ensure data integrity and to prevent possible injection attacks (such as SQL injection attacks). When setting up a system, checks should be made to verify and validate parameter settings and any static data that the system needs to operate. Wherever possible, application software should help the user verify and correct data fields, characters, and validate the completeness of data and check any range/volume limits.

4.16.2 Control of Internal Processing

Data that has been entered correctly can be corrupted by processing errors or through deliberate acts. Checks and balances must be incorporated into systems to prevent or stop an incorrect program from running. Application design must ensure that controls are implemented to minimize the risk of processing failures leading to a loss of data or system integrity. Consider the use of correction programs to recover from failures and access to add and delete functions to make changes to application data and to ensure the correct processing of data.

Separate OS-level processes and services which perform the internal data processing should use appropriate, and preferably unique, identities to allow for monitoring and logging purposes. Unique machine or device identification mechanisms should be used as well so any failures in internal processing can be identified by their process/service identity and the machine identity.

4.16.3 Message Integrity and Protection

When important or sensitive information is to be transmitted electronically, it is necessary to incorporate one or more mechanisms that will detect unauthorized changes to the content of a transmitted electronic message. Message integrity must be considered for all applications where there is a security requirement to protect the message or data content. An assessment of threats and risks should be performed to determine if message integrity is required and to identify the most appropriate method of implementation.

Note that message integrity on its own will not protect against unauthorized disclosure of sensitive information. Since MorphoTrust deals with sensitive information, including PII data, on a regular basis, all transmissions of sensitive information across unmanaged networks or between secure networks must use mechanisms to protect the data while it is in transit. Transmission solely within secure networks or customer-secured networks does not require encryption, but it is highly recommended. Transmission through unsecured networks requires encryption. Both transport-level and message-level encryption mechanisms should be considered and an analysis of the risk of data escape/loss versus cost/performance/benefit should be performed to determine the most appropriate method of implementation.

If certificates are used as a protection mechanism, either for transport encryption or message encryption, self-signed certificates must not be used in production environments, unless required by the customer. Production certificates can be obtained either through the customer, or commercial certificate authorities such as Verisign or GoDaddy, or MorphoTrust can create its own private certificate authority for issues its own certificates. MorphoTrust-issued certificates should only be used on private or closed networks that do not have any access via the Internet. If MorphoTrust establishes its own private certificate authority, all certificates created for a particular program, project, or product should be based on a private intermediate certificate authority which is tied to the private root certificate authority. The MorphoTrust **IT Department** would be responsible for the security of the root certificate for the private certificate authority.

4.16.4 Service API Access Controls

Several MorphoTrust systems, especially those intended for sale or customer use, provide an application programming interface (API) by which other programs and services can gain access to perform the desired functions. For service-oriented APIs, suitable identification controls should be used to ensure that the callers of the API are legitimate, either at the user level, the process or service level, or machine level, whichever is appropriate to the API and the overall intended system architecture. Whenever appropriate, service-oriented APIs should allow all API calls to be logged, either by using normal OS-level mechanisms or by using built-in mechanisms. All service API methods should validate their data inputs and handle any problematic data formats or content in a secure way to ensure that no malicious inputs are processed in error by the system.

4.16.5 Cryptographic Controls

Encryption is an important security layer that is used to protect the confidentiality of information. Encryption is an effective tool in mitigating the threat of unauthorized access to data. However, there are other threats, such as a hacker gaining access to an authorized user account or process, where more stringent controls and/or the use of multiple encryption levels must be considered.

Based on a risk assessment, the required level of protection must take into account the length of the cryptographic key employed. Cryptographic strength increases with longer key lengths, however so does processing time. In deciding what is best for the application, the benefits of both stand-alone and enterprise level encryption solutions should be considered. Attention must also be given to the customer regulations, government regulations at the Federal/State/Local levels as appropriate, and national restrictions (e.g., export controls) that may apply to the use of cryptographic techniques, particularly in different parts of the world.

The MorphoTrust policy on data encryption is in:

- **PRC-00233-A** *Data Encryption Policy*

4.16.6 Key Management

A secured environment must be established to protect the cryptographic keys used to encrypt and decrypt information. Keys must be securely distributed and stored. Access to these keys must be restricted to only (a) those individuals who have a business need to access the keys and (b) any special service accounts that require the keys to encrypt or decrypt the information. Compromise of a cryptographic key would cause all information encrypted with that key to be considered as unencrypted information.

The MorphoTrust policy on key management is in:

- **PRC-00233-A** *Data Encryption Policy*

4.16.7 Protection of Test System Data

For the QA test environment, QA test data is intended to test the expected behavior of software, systems and applications. QA test data is developed to test a comprehensive set of conditions and outcomes, including exception processing and error conditions to demonstrate accurate processing and handling of information and the stability of the software, system or application.

Once test data is developed, it must be protected and controlled for the life of the testing. In those cases where QA test data is reused, whenever modifications are made to the software, system or application then the test data must be protected and controlled during the entire useful life. This protection mechanism is essential to ensuring a valid and controlled simulation with predictable outcomes.

If a customer provides or transfers production data to MorphoTrust for testing purposes or for other purposes such as investigative analysis or algorithm training, this data must be treated as PII data and protected with appropriate access controls on a secure network.

Otherwise, production data may be used for QA testing only if the following controls are applied:

- The production data is treated as sensitive information, especially if it contains PII data, and is protected by access controls in the QA environment.
- If the production data is stored in a QA database, the access protections on the database are comparable to what is or would be used in the production environment.
- If the production data comes from a customer's environment or database, then:
  - The customer consents in writing or by email to MorphoTrust using the production data for QA testing.
  - The production data is securely deleted when the QA testing is finished. However, the data may be retained if any additional QA testing (such as regression testing) is expected to be done within a reasonable time and the customer is aware of and agrees to (in writing or by email) this additional QA testing with the production data.
- The production data is stored on a secure network with ACLs and preferably encrypted.

As much as possible, any restrictions or intended use for customer data (production or otherwise) should be documented and maintained in a suitably protected manner by the manager whose group received the data. Historically, many customers have provided test data (production or otherwise) to MorphoTrust for various intended purposes for a number of years. Unfortunately, with changes in MorphoTrust personnel over time, it is possible that the intended use of this data may have become lost or misplaced. If the documentation for the intended use of a customer's data is no longer available or cannot be found, then the data should only be used in a way that could ultimately benefit that particular customer in some way. This usage can include QA testing, regression testing, debugging problems, investigative analysis, and training new or existing algorithms. Typically, the benefit to the customer will come in the form of new software releases or improved configuration parameter settings for better accuracy or performance.

For the UAT environment, it is possible that production data will be loaded into the UAT systems, either to simulate production conditions or in preparation for the UAT environment to be transitioned into the production environment at the end of the UAT period. Any PII data that is under MorphoTrust control in a UAT environment must be protected in accordance with this CSP, subject to the requirements, limitations and constraints of the customer.

4.16.8 System Setup and Installation

For systems which will be deployed into a customer's environment, any systems that are destined for production environments should be hardened sufficiently to allow the applications to perform satisfactorily and to allow reasonable utilities and diagnostics to be run by designated personnel (either customer or MorphoTrust personnel) to investigate and solve issues that arise. This is to reduce the chance that any malware that appears in the customer's environment will have adverse effects on the operation and performance of the MorphoTrust-supplied systems.

The MorphoTrust policy on installation and security for a credentialing system is in:

- **PRC-00124-A** *MorphoTrust USA DL/ID Installation Data & Security Policy*

4.16.9 Change Control Procedures

To minimize the possibility of corruption of information systems used within MorphoTrust or in a customer's production environment, strict controls over changes to these information systems must be implemented. Formal change control procedures for MorphoTrust business applications and network configuration must be developed, implemented and enforced. They must ensure that security and control procedures are not compromised, that support personnel are given access only to those parts of a system necessary to perform their jobs, and that formal agreement and approval processes for changes are implemented.

In addition, access to source code libraries for business applications and customer applications must be controlled to ensure that only authorized individuals have access to these libraries and that access is logged to ensure all activity can be monitored.

The MorphoTrust policy on change management is in:

- **PRC-00085-B** *IT Change Management Policy & Procedure*

4.17 Customer Support Policy

The preferred way for supporting our systems in the customer's environment is having a site-to-site VPN between our CSN and the customer network. This arrangement offers the most control and flexibility for managing the security of the access to the customer's environment, such as who has access, what ports and/or protocols are available, being able to cut off access for someone, and so forth. It has the disadvantage of being more burdensome on the MorphoTrust support personnel because they have to connect through another machine or two to get to the desired machines in the customer's environment. However, with the existing NSA in effect, it is preferable and desirable to have stronger security management controls over easy and convenient access for MorphoTrust support personnel.

It is possible that customers may have policies governing VPN connections, and they may want vendor support personnel (MorphoTrust support personnel, in this case) to use a client-based point-to-point VPN as supplied by the customer. This is acceptable for MorphoTrust support personnel to use this connection method for providing support. Although, while it usually is an easier and more convenient method of connecting to the customer's environment for the MorphoTrust support personnel, point-to-point VPN connections do not offer MorphoTrust the same level of security management as site-to-site VPNs. Effectively, this option transfers the responsibility of VPN security management to the customer, but MorphoTrust is still responsible for notifying the customer of changes to support personnel.

A variation on the point-to-point VPN connection is if the customer provides a split-tunnel VPN to access their network. This should be discouraged strongly as it can bridge the customer's network with the current network that the MorphoTrust support person is on. Normally, this would be the MorphoTrust corporate network, but if the support person is traveling, it could be a less secure network. In order to minimize the chance of any malware coming into either the MorphoTrust environment or the customer's environment, split-tunnel VPNs should not be used if possible. If the customer insists on using a split-tunnel VPN, it must be reviewed and approved by the **CSO** and **ISO** to see if there is some other ways to mitigate the risks, such as using a dedicated machine on an isolated subnet within the corporate network to access the customer's environment.

4.18 Customer Accommodation Policy

Customer environments and their associated security policies (or lack thereof) form a very diverse set of deployment scenarios for MorphoTrust products, services, and solutions. While some customers are very conscientious about security and have various compliance processes and procedures, other customers treat security considerations as lesser priorities. Indeed, some customer legacy systems simply cannot support more modern security protocols and conventions. Furthermore, some customers may not want the level of security that MorphoTrust would use or recommend yet MorphoTrust is contractually responsible for and has control of the security of the system. In these cases, it may be necessary to use a reduced security level, herein called a **security accommodation**, to allow the MorphoTrust system to work in the customer's environment, according to the policy guidelines in the following subsections.

The use of security accommodations should only be done as an exception and not as a normal procedure.

4.18.1 Acceptable Security Accommodations

When a conflict is identified between the security policies in this CSP and the limitations imposed by the customer's environment, the following procedure should be followed by the people in the highlighted roles:

1. The **Responsible Manager** discusses with the customer the possible security accommodations that could allow the MorphoTrust system to operate with the customer's limitations. If a candidate security accommodation is in the list of unacceptable security accommodations (see Section 4.18.2), it cannot be used without the written permission from both the **CSO** and **ISO**. Otherwise, the **Systems Engineer** ensures that each

candidate security accommodation is at least reasonable by modern security practices. Furthermore, the **Systems Engineer** identifies the security risk(s) introduced or exposed for each candidate security accommodation under consideration. If there is any doubt, the **Systems Engineer** should discuss the candidate security accommodation with the **ISO** to see if there are any other options that might be possible.

2. From the set of reasonable candidate security accommodations, the **Responsible Manager**, the **Systems Engineer**, and the customer come to a mutual agreement on the security accommodation that will be implemented. Either the **ISO** or the **CSO** must approve of the security accommodation before it can be implemented. For security accommodations that could affect compliance with the Proxy Agreement, the **FSO** must approve as well.
3. The **Responsible Manager** asks the MorphoTrust **Legal Department** to draft a waiver or release for the security accommodation. If the **Legal Department** has concerns about granting the security accommodation, the **Legal Department** discusses them with the **ISO** or **CSO** and a final resolution is determined. If the final resolution still permits the security accommodation to be made, the **Legal Department** determines what information needs to be in the waiver or release.
4. The **Responsible Manager** sends the waiver or release to the customer for their approval and acceptance. Once the waiver or release is accepted by the customer, the work on implementing the security accommodation may begin.

A copy of the signed or accepted waiver or release along with any supporting documentation should be forwarded to the **CSO** and **ISO** as well as the MorphoTrust **Legal Department**.

The granting of a security accommodation in one situation should be not construed as an implied approval for a similar security accommodation in a similar or related situation. Each security accommodation must be reviewed and approved separately for each situation.

4.18.2 Unacceptable Security Accommodations

No security accommodations can be made in the following circumstances, unless explicitly approved by the **CSO** and **ISO**:

1. Whenever the system needs to interact openly with the Internet. Example: An application includes functionality from Google Maps.
2. Whenever the system needs to interact with any MorphoTrust systems. Examples: The system connects to the CSN or communicates with SIMS.
3. Transmitting user or service authentication information (credentials) in clear text (i.e., unencrypted) over unsecured networks, including the Internet.

Under no circumstances can PII data be transmitted in clear text over any unsecured networks, including the Internet.

4.18.3 Compliance Accommodations

If any new compliance issues are identified, they should be reported to the **CSO** and **ISO** and then addressed as soon as possible. However, if an issue cannot be remedied because of customer limitations, the **Operations Manager** should get a written release from the customer explicitly allowing the lesser security in their environment. (See Section 4.18.1 for more information.) A copy of the release should be forwarded to the **CSO** and **ISO**. The MorphoTrust **Legal Department** can help with drafting the release.

4.19 Compliance Policy

4.19.1 Monitoring

MorphoTrust reserves the right to monitor, inspect, and/or search at any time all information processing systems. Since MorphoTrust information technology equipment and networks are provided for business purposes, MorphoTrust personnel should have no expectation of privacy in the information stored in or sent through these information systems. MorphoTrust **Management** additionally retains the right to remove from its information systems any unauthorized material.

4.19.2 Compliance

Compliance with this Policy is mandatory. Each user must understand his/her role and responsibilities regarding information security issues and protecting sensitive information. The failure to comply with this or any other security policy that results in the compromise of sensitive information, confidentiality, integrity, privacy, and/or availability may result in appropriate disciplinary action, up to and including termination. MorphoTrust will take every step necessary, including legal and administrative measures, to protect its assets and will rely on the **CSO** to monitor compliance with policy matters.

MorphoTrust will conduct a review of compliance with this policy at least annually. Areas where compliance with the policy requirements is not met will be documented and a plan will be developed to address the deficiencies. While a full review across all of MorphoTrust is preferable, spot checks for compliance are also acceptable.

MorphoTrust managers and supervisors will ensure that all security processes and procedures within their areas of responsibility are followed. In addition, all MorphoTrust business units may be subject to periodic reviews to ensure compliance with security policies and standards.

4.19.3 Enforcement and Violation Handling

Any compromise or suspected compromise of this policy must be reported to the **CSO** and **ISO** immediately. The security incident (or event) reports should indicate the risk level of the violation. Access authorization for user accounts involved in a compromise may be suspended during the time when a suspected violation is under investigation. Automated violation reports generated by the various security systems will be forwarded to the appropriate MorphoTrust **Management**, the **CSO**, and the **ISO** for timely resolution. Any violations of security policies may be subject to disciplinary or other appropriate action.

5 REFERENCES

[1] For example, the DoD definition for PII is:

> E2.2. Personal Information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her (e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc.). Such information also is known as personally identifiable information (e.g., information which can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information which is linked or linkable to a specified individual.

This is from Department of Defense Directive 5400.11, May 8, 2007, incorporating Change 1, September 1, 2011. This document is available at http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf. A training presentation on PII for the DoD is available at http://iase.disa.mil/eta/pii/pii_module/pii_module/module.htm.

Also, NIST has a definition for PII in SP 800-122, which is available at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

[2] Secure server rooms can be operated either by MorphoTrust or at government sites. Refer to http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

6 ACRONYMS

ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CM	Configuration Management
CSN	Customer Support (or Solutions) Network
CSO	Chief Security Officer
CSP	Cyber Security Plan
DL	Driver's License
DOB	Date of Birth
DoD	Department of Defense
DSS	Defense Security Service

ECP	Electronic Communications Plan
EIN	Electronic Identification Number
FCS	Factory Control Server
FSO	Facilities Security Officer
HR	Human Resources
IAAS	Infrastructure as a Service
ISO	Information Security Officer
MAC	Media Access Control
LAN	Local Area Network
NASPO	North American Security Products Organization
NIST	National Institute of Standards and Technology
NSA	National Security Agreement
OS	Operating System
PAAS	Platform as a Service
PII	Personally Identifiable Information
QA	Quality Assurance
RADIUS	Remote Authentication Dial In User Service
SAAS	Software as a Service
SIMS	Secure Inventory Management System
SLA	Service Level Agreement
SP	Special Publication
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSN	Social Security Number
TLS	Transport Layer Security
UAT	User Acceptance Testing
USGA	U.S. Government Agencies
VLAN	Virtual Local Area Network

7 CONTACT INFORMATION

Questions concerning this CSP or its accompanying policies may be directed to the MorphoTrust **Information Security Officer** (ISO):

Dr. James Kottas, ISO
MorphoTrust USA, Inc.
296 Concord Road, Suite 300
Billerica, MA 01821
Phone: 978-215-2613
jkottas@morphotrust.com

Any failures to comply with the CSP or any of its accompanying policies must be reported to the MorphoTrust **Chief Security Officer** (CSO):

Dennis Kallelis, CSO
MorphoTrust USA, Inc.
296 Concord Road, Suite 300
Billerica MA 01821
Phone: 978-215-2572
dkallelis@morphotrust.com

8 REVISION HISTORY

Revision	Date	Description	Author(s)
00	2/10/2012	Initial draft to GSC.	James Kottas
01	2/14/2012	Initial approved version to DSS.	James Kottas
02	3/5/2012	Incorporated feedback from MorphoTrust personnel. This will become the customer accommodation policy.	James Kottas
02	3/8/2012	Updated Section 4.9 to remove the reference to PRC-00087-B and updated the reference to PRC-00113-A as these two policy documents were merged.	James Kottas
02	4/9/2012	Added template letter for customer security accommodation notice to Section 4.17.1. Added the list of unacceptable security accommodations to Section 4.17.2.	James Kottas
02	6/15/2012	Updated policy document titles to remove “Corporate” from them.	James Kottas
02	7/18/2012	Updated Section 4.13 to include the handling of large amounts of PII data when received from a customer.	James Kottas
02	7/20/2012	Updated Section 4.12 to add the third paragraph saying that all default passwords must be changed to secure passwords that are compliant with applicable policies.	James Kottas
02	9/7/2012	Updated the end of Section 4.16.3 to allow for a private certificate authority created and maintained by MorphoTrust for issuing certificates on closed networks.	James Kottas
02	9/7/2012	Inserted a new Section 4.17 to establish a policy for customer support. The existing Section 4.17 became Section 4.18, with subsequent sections being renumbered accordingly.	James Kottas
02	10/30/2012	Updated Section 4.18 and its subsections based on feedback from Gary Chan.	James Kottas

Revision	Date	Description	Author(s)
02	11/27/2012	Updated Section 4.12.11 to include a clause that cloud environment can be considered as long as their use does not cause MorphoTrust to become non-compliant with its NSA and proxy agreements, or with state cyber laws and regulations.	James Kottas
02	12/17/2012	Updated Section 4.13 to allow for encrypted PII being transmitted via email.	James Kottas
02	7/7/2013	Changed the CIO on the title page from Robert Stack to John May.	James Kottas
02	7/7/2013	Added small editorial changes to make the content more clear. Done throughout the document. Updated the list of Acronyms in Section 6.	James Kottas
02	7/7/2013	Updated Section 4.10.2 to allow for the FSO to designate another authority for authorizing and approving vulnerability scans.	James Kottas
02	7/7/2013	Updated Section 4.10.5 to suggest the use of RADIUS authentication and access profiles.	James Kottas
02	7/7/2013	Updated Section 4.12.3 to include the use of two-factor authentication whenever possible and practical.	James Kottas
02	7/7/2013	Updated Section 4.12.11 to allow for MorphoTrust-hosted cloud environments.	James Kottas
02	7/7/2013	Updated Section 4.13 to change the minimum encryption level from AES-256 to AES-128.	James Kottas
02	7/7/2013	Updated Section 4.13 to refer to the Information Spills and Cleanup policy, PRC-00312-A.	James Kottas
02	7/8/2013	Update Section 4.18.1 to require either ISO or FSO approval for an acceptable security accommodation.	James Kottas
02	7/15/2013	Changed the FSO to be the more general CSO throughout the document. Updated the FSO signature on the title page to be the CSO. Updated Section 3 to note that for proxy-related cyber issues, the CSO can involve the FSO.	James Kottas
02	9/24/2013	Updated Section 4.18 to clarify the conditions under which a waiver could be required.	James Kottas
02	10/9/2013	Made roles boldface throughout Section 4 to make them more consistent.	James Kottas

Revision	Date	Description	Author(s)
02	10/9/2013	Updated Section 4.18.1 to clarify that any concerns about a security accommodation from the Legal Department need to be resolved before a waiver can be draft. If the concerns cannot be resolved, then no waiver will be possible.	James Kottas

IT BACKUP & RECOVERY POLICY

Document Number: PRC-00084 B

Revision Level: 03

Approval

Robert Stack Chief Information Officer	Robert Eckel President

Users are responsible for making sure that they have the current revision of this document.

TABLE OF CONTENTS

1 Data Storage Overview

- All MorphoTrust systems are backed up on a daily basis via Iron Mountain's Turbo Restore Appliance (TRA). The following rules apply:
- The daily backups are performed on equipment stored in Billerica, MA.
- At the end of the backup process, the information is uploaded offsite to the Iron Mountain Cloud.
- The TRA has a web portal which provides IT personnel access to logs, etc.
- For the purpose of this document all storage (internal or external) is referenced as *storage*. Both internal and external storage are protected equally with hardware (RAID) and redundant hardware components that are capable of supporting enterprise class operations.
- Storage is monitored by both administrators and operations. Monitoring is described in *IT Managing Operations Policy: PRC-00090-B*.

2 Data Access

- Authorized user's access data at the application layer and are bound by the security controls active within the application. Application user access is described in the application control documents.
- In some cases users have access to data on the directory level and have been authorized to do so by the application business owner. Application user access is described in the application control documents**.**
- Remote data access and network security are described in the IT Remote Access and IT Information Security documents.

3 Data Retention

- The daily TRA backups are retained in Billerica for one year, after which it is purged.
- The up-loaded copies residing on the Iron Mountain Cloud are retained for seven years. All backup media will be labeled in accordance with the established MorphoTrust USA standard. At minimum the label will contain "MorphoTrust USA", the date and the sequence number.

4 Backup Monitoring

- All daily backup sessions are monitored by IT staff each day to ensure there are no issues from the backup the night before.

5 Exception Reporting

- Exception reporting occurs thru the storage manager console which alerts administrative staff when backups do not run as scheduled, fail, or in any way not perform as planned.
- All exceptions to the backup schedule are automatically emailed to a mailbox monitored by the Manager of Operations or designee.

6 Recording Backup & Recovery Issues

- All backup failures are noted during the weekly review performed by the Manager of Operations.

7 Restores

- Data restores are managed using the same storage manager systems that are used for the backups.
- IT performs test restores on a quarterly basis.

8 Disaster Recovery

- A disaster recovery contract exists with Iron Mountain.

Information Security: Customer Data Access and Security Policy

Document Number: PRC-00174-A
Revision Level: 07

Approval

Dennis S. Kallelis Chief Security Officer	Robert Eckel President

This documentation contains confidential and proprietary business information of MorphoTrust USA. This document, including copies of all or and part thereof, may not be released or disclosed to persons other than MorphoTrust USA employees except as necessary for business purposes of MorphoTrust USA under an appropriate confidentiality agreement.

Users are responsible for making sure that they have the current revision of this document

Table of Contents

1. Policy Overview

This policy defines the data management environment and assigned roles and responsibilities for protecting customer information from unauthorized access, disclosure, or misuse.

It is the responsibility of every MorphoTrust USA employee who accesses customer data and information to secure and protect customer data.

Many federal and state laws regulate the collection, handling and disclosure of customer data, including the Family Rights to Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, the Federal Privacy Act of 1974, the DHS Real-ID Act, the MorphoTrust USA Proxy Agreement, the National Security Agreement,the NISPOM requirements, provincial & state privacy regulations, Cyber Protect Laws, and other jurisdictional laws.

Exposure of confidential customer data through improper disclosure or security risk is a violation of these laws, and can result in MorphoTrust USA incurring legal liability, financial liability, loss of reputation, and loss of trust.

1.1 Policy Statement

Access to customer data is granted by data custodians and trustees who are required to develop and maintain clear and consistent procedures for access and use of the data, prevent unauthorized access, and protect customer data. Items of information that are collected, maintained, and utilized by the MorphoTrust USA for the purpose of carrying out company business may include customer data.

"Custodians" and "trustees" are considered "Policy Implementers" responsible for understanding and following, but not making policy.

All customer data is classified as "High Critical" and must be consistently protected throughout its life cycle (from its creation/receipt to its destruction/delivery) in a manner corresponding to its sensitivity and/or criticality regardless of where it resides, what form it takes, what technology is used to handle it, and what purpose it serves. Access to non-public data is considered on a "need to know" basis.

The "Director of Manufacturing", and "Tier 3 Lead", are all considered custodians of customer data, with the authority to delegate access to data to eligible personnel and to their office staff as they deem appropriate. The following pre-requisitions are required for all custodians and delegates:

- Successful Background checks
- Data security Training
- Final review & signoff by an authorized agent of the customer

Management, defined as the President, Executive Vice President, Senior Vice President, Vice Presidents are considered "Policy Makers" and are typically not eligible for customer data access.

Sensitive and regulated customer data includes but is not limited to; including Social Security Numbers, credit/debit card numbers, biometrics, biographic data, document numbers, application data, and State drivers' license/non-drivers' identification numbers is to be considered non-public customer data (private).

1.2 Reason for Policy

The purpose of this policy is to ensure the protection of the customer data from accidental or intentional unauthorized access, damage, or disclosure while allowing for the appropriate processing of non-public data in support of company and customer services.

1.3 Applicability of Policy

This policy applies to all data regardless of its media and/or form, and to all those who handle secure information including third party service providers

2. Classification of Data

Use the criteria in the following table to determine which data classification is appropriate for a particular information or infrastructure system.

	PUBLIC	NON-PUBLIC/INTERNAL	NON-PUBLIC CONFIDENTIAL/REGULATED
Sensitivity Level	Open, unclassified	Low to Moderate	High-Critical
Legal Requirements		Protection level of data is set by the owner or custodian	Restricted data, subject to federal, state, and other regulations, including the, FERPA, PCI/DSS, Gramm-Leach-Bliley, HIPAA, Proxy Agreement, NSA, and/or other legal requirements.
Access	Information authorized for release to the public	Employees/ non-employees with a business need to know	Only those individuals with approved access and signed non-disclosure forms
Definition	Public information that can be disclosed without violating an individual's right to privacy.	Institutional information that is intended for use within MorphoTrust USA	Information that MorphoTrust USA and its employees have a legal, regulatory, or social obligation to protect. Unauthorized disclosure would violate individual privacy rights Highly regulated information: Unauthorized disclosure could subject individuals to identity theft and could lead to substantial financial penalties and loss of reputation to MorphoTrust USA.
Data Examples	Course schedules, catalogs, brochures, maps	Research detail or results that are not restricted data, management information; Budget information, private employee information	SSNs, credit/debit card numbers, drivers' license numbers, biographic, biometrics, document data, state-issued non-drivers' ID numbers, protected health information

3. Roles

3.1 Definitions

The following definitions apply to terms used in this policy.

Term	Definition
Senior Management	The President, Executive Vice President, Vice Presidents, are designated as Senior Management • Senior Management members are not eligible for access to non-public information. • The President, Executive Vice President and Vice Presidents are authorized to delegate access to eligible personnel and to their office staff as deemed appropriate by job type function and with appropriate justification, conditional upon successful training as outlined by the curriculum put forth by the CSO.
Data Custodian	An individual who has responsibility for non-public data resources. All non-public data must have an identified Data Custodian. Data Custodians support the mission of customers and MorphoTrust USA and facilitate the conduct of MorphoTrust USA business by ensuring that access to data is granted as needed for legitimate purposes and within the terms articulated by policy to trained personnel.
Data Trustee (Access Administrator)	Each Data Custodian may designate one or more Data Trustees based on job type to execute day-to-day custodial responsibilities. In practice, Data Trustees are those persons primarily responsible for the accuracy, integrity, and privacy of non-public data. The Data Trustee for non-customer data is the appropriate Department Head. The Data Trustee for MorphoTrust USA enterprise-wide corporate summary data is the Chief Information Officer.
Customer	Owner of the secure citizen data.
Functional Areas of MorphoTrust USA Data	The functional administrative areas of MorphoTrust USA data are: Financial, R&D, Human Resources, Manufacturing, Facilities, Security, Program Mgmt, Sales, Marketing, Supply Chain, Federal Systems, Tier 3 Admins, and Information Technology.

3.2 Responsibilities

Area	Responsibility
The President, Executive Vice President	Responsible for sponsoring compliance to policy. Delegating access to non -public data to those eligible (see Data Custodians table).
Chief Security Officer (CSO)	Responsible for Information Security policy. Security incidents are reported to the CSO. Definition of training curriculum for data custodians, trustee and users.

Chief Information Officer (CIO)	Responsible for maintaining the performance of MorphoTrust USA information technology computing resource hardware & software, and the MorphoTrust USA network infrastructure.
Data Custodians	Manage non-public information resources; ensure that access to data is granted only as needed for legitimate purposes and within the terms articulated in this policy; ensure that training and awareness of the terms of this policy are provided; monitor compliance with this policy.
Data Trustees	Data trustees classify data in their functional areas; develop and maintain clear and consistent procedures for access to MorphoTrust USA administrative data; grant and revoke access; maintain an audit trail, i.e., lists showing those granted access to administrative data; periodically review access privileges to ensure that access is still warranted; remove access in a timely manner for employees whose job responsibilities have changed; promote the security of the data in their subject areas. Ensure databases are only installed on systems that are encrypted, in firewalled networks, on systems with current operating system security patches, on systems with virus protection, have default admin passwords removed, and have secure strong passwords to systems.
Customer	Owner of system secure data. Reviewer and final authority for granting access rules to custodians and delegates.

4. Data Custodians

Example of Data Custodians are Director of Manufacutring, Tier 3 Lead Aministration and Chief Security Officer.

5. Auditing & Certification

MorphoTrust USA is certified to the American National Standards Institute’s North American Security Products Organization standard ANSI/NASPO-SA-2008 as Security Class II. NASPO audits MorphoTrust USA yearly for compliance to the ANSI standard so that we can maintain Security Class II Certification. MorphoTrust USA is active in the development of the new International Standards Organization (ISO)’s Security Standard 16215.

All secure data rules must comply with these standards to achieve successful audit results and maintain certifications.

6. Compliance

Violations of this policy will result in appropriate disciplinary measures in accordance with policy, state and federal laws. All staff are encouraged to protect customer data and the companies liability by reporting known problems with securing data, and are encouraged to seek continuous technology improves in protecting database integrity.

7. References

Please refer to the other Security Policies and Procedures for more details.

- Security Governance Policy PRC-00173

- Need to Know Policy PRC-00141
- Privacy Policy PRC-00144
- Classification of Information and Materials Policy PRC-00121
- Corporate IT Security Policy PRC-00112
- Employee Security Screening Policy PRC-00134
- IT Information Security PRC-00089
- IT Physical IT Access Controls PRC-00091
- Liability Policy PRC-00140
- Security Awareness Training Policy PRC-00152
- Security Quick Reference PUB-00185

IT VIRUS PROTECTION POLICY

Document Number: PRC-00093-B

Revision Level: 01

Approval

Robert Stack Chief Information Officer	Robert Eckel President

This document contains confidential and proprietary information of MorphoTrust USA. No part of this document may be reproduced, disclosed, distributed, or used in any form by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage or retrieval – without written permission of MorphoTrust USA.

Users are responsible for making sure that they have the current revision of this document.

TABLE OF CONTENTS

1 Overview:

- The principle concern of this computer virus protection policy is effective and efficient prevention of network virus outbreaks and network security attacks involving computers associated with MorphoTrust USA.

2 Policy:

- All files downloaded to the MorphoTrust USA network potentially harbor computer viruses, Trojan horses, worms or other destructive programs and, therefore, all downloaded files must be scanned for such viruses. Virus detection programs and practices shall be implemented throughout the MorphoTrust USA environment.
- Training must take place to ensure that all computer users know and understand safe computing practices.
- IT administration will be held responsible for ensuring current software is on the network to prevent the introduction or propagation of computer viruses.
- Any activity with the intention to create and/or distribute malicious software by means of the MorphoTrust USA networks is strictly prohibited.
- MorphoTrust USA will employ virus management measures at appropriate ingress and egress points of the company networks. MorphoTrust USA will implement virus control procedures to ensure that all computer servers and workstations are protected against viruses.

3 Procedure:

3.1 Workstation

- All data and/or program files must be scanned for viruses before installation to safeguard MorphoTrust USA networks from infection. This includes shareware and freeware obtained from electronic bulletin boards or on disk (diskette or CD-ROM), custom-developed software, and software received through business sources.
- All data and program files that have been electronically transmitted to an MorphoTrust USA computer from another location, internal or external, must be scanned for viruses immediately after being received.
- All computer media (diskette, CD, etc) is a potential source for a computer virus. Therefore, all media must be scanned for virus infection before it is used in a MorphoTrust USA computer or network server.
- Virus protection software shall be loaded on each desktop computer and server and stay a resident program to constantly monitor for viruses to prevent introduction to the network.

3.2 Email

- All email and attachments to email are scanned to prevent viruses from entering through the email system.
- All emails are filtered prior to entering the MorphoTrust USA network through a best-practice email filtering application. This application uses multiple anti-virus engines and all anti-virus signatures are updated in real-time.
- Reports are generated monthly to ensure compliance.

4 Updating Virus Definitions:

- MorphoTrust USA IT shall configuration the virus protection application to regularly update its virus definitions from the software vendor. This process should be monitored by way of log files. The applications should be configured to send email alerts to the virus application administrator regarding the status of the virus definition update. In the case of an unsuccessful update the administrator should manually execute the virus definition update.
- Any time there is a change to the virus definition file these update should immediately be pushed to all workstations and servers.

5 Monitoring :

- Logs created during virus updates to servers and workstations in the MorphoTrust USA network should be reviewed for completion status. Any failed updates should be immediately followed up on and updated virus definitions loaded to the failed component.

Sensitive Data Handling and Storage Procedures

Document Number: PRC-00148-A
Revision Level: 05

Approval

John May Chief Information Officer	James Kottas, Chief Privacy & Information Security Officer

Table of Contents

1. Introduction

This policy describes the controls MorphoTrust USA (The Company) employs to protect the sensitive data it collects, handles, and stores as part of its daily business operations. Sensitive data, for the purpose of this policy, includes but is not limited to the following:

- Social Security numbers
- Credit/debit card numbers
- Biometrics
- Biographic and demographic data
- State Identification card numbers

Many federal and state laws regulate the collection, handling and disclosure of sensitive data, including the Family Rights to Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, the Federal Privacy Act of 1974, the DHS Real-ID Act, the MorphoTrust USA Proxy Agreement, the National Security Agreement, the NISPOM requirements, provincial & state privacy regulations, Cyber Protect Laws, and other jurisdictional laws.

Exposure of sensitive data through improper disclosure or security failure is a violation of these laws and can result in MorphoTrust USA incurring legal liability, financial liability, loss of reputation, and loss of trust.

Data Custodians and Trustees

Access to sensitive data is granted by data custodians and trustees who are required to develop and maintain clear and consistent procedures for access and use of the data and prevent unauthorized access.

Custodians and Trustees are considered *Policy Implementers* responsible for understanding and following, but not making policy.

All sensitive data is classified as **High Critical** and must be consistently protected throughout its life cycle (from its creation/receipt to its destruction/delivery) in a manner corresponding to its sensitivity and/or criticality regardless of where it resides, what form it takes, what technology is used to handle it, and what purpose it serves. Access to non-public data is considered on a **Need to Know** basis. Refer to the *Need To Know Policy POL-00141-A* for more information.

The **Director of Manufacturing** and **Tier 3 Lead**, are considered custodians of sensitive data, with the authority to delegate access to data to eligible personnel and to their office staff as they deem appropriate. The following pre-requisitions are required for all custodians and delegates:

- Successful background checks
- Data security training
- Final review and signoff by an authorized agent of the customer

Management, defined as the **President**, **Executive Vice President**, **Senior Vice President**, and **Vice Presidents**, are considered **Policy Makers** and are typically not eligible for sensitive data access.

Applicability

This policy applies to all data regardless of its media and/or form, and to all those who handle secure information including third party service providers.

Classification of Data

The following table classifies the data the Company handles:

	PUBLIC DATA	NON-PUBLIC/INTERNAL DATA	NON-PUBLIC CONFIDENTIAL/REGULATED DATA
Sensitivity Level	Open, unclassified	Low to Moderate	High-Critical
Legal Requirements		Protection level of data is set by the owner or custodian	Restricted data, subject to federal, state, and other regulations, including the, FERPA, PCI/DSS, Gramm-Leach-Bliley, HIPAA, Proxy Agreement, NSA, and/or other legal requirements.
Access	Information authorized for release to the public	Employees/ non-employees with a business need to know	Only those individuals with approved access and signed non-disclosure forms.
Definition	Public information that can be disclosed without violating an individual's right to privacy.	Institutional information that is intended for use within MorphoTrust USA	Information that MorphoTrust USA and its employees have a legal, regulatory, or social obligation to protect. Unauthorized disclosure would violate individual privacy rights. Highly regulated information: Unauthorized disclosure could subject individuals to identity theft and could lead to substantial financial penalties and loss of reputation to MorphoTrust USA.
Data Examples	Course schedules, catalogs, brochures, maps	Research detail or results that are not restricted data, management information; Budget information, private employee information	SSNs, credit/debit card numbers, drivers' license numbers, biographic, biometrics, document data, state-issued non-drivers' ID numbers, protected health information.

Roles and Responsibilities

The following definitions apply to terms used in this policy:

Term	Definition
Senior Management	• Senior Management members are not eligible for access to non-public information. • The President, Executive Vice President and Vice Presidents are authorized to delegate access to eligible personnel and to their office staff as deemed appropriate by job type function and with appropriate justification, conditional upon successful training as outlined by the curriculum put forth by the CSO.
Data Custodian	An individual who has responsibility for non-public data resources. All non-public data must have an identified Data Custodian. Data Custodians support the mission of customers and MorphoTrust USA and facilitate the conduct of MorphoTrust USA business by ensuring that access to data is granted as needed for legitimate purposes and within the terms articulated by policy to trained personnel. Examples are Director of Manufacturing, Tier 3 Lead Administration and CSO.
Data Trustee (Access Administrator)	Each Data Custodian may designate one or more Data Trustees based on job type to execute day-to-day custodial responsibilities. In practice, Data Trustees are those persons primarily responsible for the accuracy, integrity, and privacy of non-public data. The Data Trustee for non-sensitive data is the appropriate Department Head. The Data Trustee for MorphoTrust USA enterprise-wide corporate summary data is the Chief Information Officer.
Customer	Owner of the secure citizen data.
Functional Areas of MorphoTrust USA Data	The functional administrative areas of MorphoTrust USA data are: Financial, R&D, Human Resources, Manufacturing, Facilities, Security, Program Management, Sales, Marketing, Supply Chain, Federal Systems, Tier 3 Admins, and Information Technology.

Responsibilities

Area	Responsibility
The President, Executive Vice President	Responsible for sponsoring compliance to policy. Delegating access to non - public data to those eligible (see Data Custodians table).
Chief Security Officer (CSO)	Responsible for Information Security policy. Security incidents are reported to the CSO. Definition of training curriculum for data custodians, trustee and users.
Chief Information Officer (CIO)	Responsible for maintaining the performance of MorphoTrust USA information technology computing resource hardware & software, and the MorphoTrust USA network infrastructure.
Chief Privacy & Information Security Officer (CPO/ISO)	Responsible for compliance with Local, State, and Federal Privacy Laws. Additionally responsible for the Electronic Communications Policy (ECP) and Cyber Security Plan (ECP) and investigating breaches of same.
Data Custodians	Manage non-public information resources; ensure that access to data is granted only as needed for legitimate purposes and within the terms articulated in this policy; ensure that training and awareness of the terms of this policy are provided; monitor compliance with this policy.
Data Trustees	Data trustees classify data in their functional areas; develop and maintain clear and consistent procedures for access to MorphoTrust USA

	administrative data; grant and revoke access; maintain an audit trail, i.e., lists showing those granted access to administrative data; periodically review access privileges to ensure that access is still warranted; remove access in a timely manner for employees whose job responsibilities have changed; promote the security of the data in their subject areas. Ensure databases are only installed on systems that are encrypted, in firewalled networks, on systems with current operating system security patches, on systems with virus protection, have default admin passwords removed, and have secure strong passwords to systems.
Customer	Owner of system secure data. Reviewer and final authority for granting access rules to custodians and delegates.

2. Data Collection

Authorized personnel should collect only the minimum necessary sensitive information required to perform MorphoTrust USA business. Such personnel must ensure that all decisions regarding the collection and use of sensitive data are in compliance with the law and with MorphoTrust USA policies and procedures.

3. Data Access

The following rules govern the access to sensitive information:

- Authorized personnel only should access sensitive information.
- All employees (including contractors and their agents) working in or having access to manufacturing facilities must be U.S. Citizens who are no dual citizens.
- Authorization for access to sensitive data comes from Corporate Management, and is typically made in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other official authority.
- Staff (employees and contractors) that need to be issued network credentials to customer systems must obtain it through the Security Department of MorphoTrust USA. The Security Department shall track those individuals and inform the customers to remove accounts upon departure of staff from that program and from the need to have credentials. Staff must be background checked by MorphoTrust and refreshed annually if they have access to customer PII.
- Where access to sensitive data has been authorized, use of such data shall be limited to the purpose required to perform MorphoTrust USA business.
- Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.
- Notification of a user's termination or removal of authorized access to sensitive information must be conveyed immediately to the MorphoTrust USA IT group.

4. Data Handling and Transfer

The following rules govern the handling and transfer of sensitive information:

- Sensitive information must not be transferred by any method to persons who are not authorized to access that information. Users must ensure that adequate security measures are in place at each destination when sensitive data is transferred from one location to another.
- Sensitive data must be protected from unintended access by unauthorized users. Users must guard against unauthorized viewing of such information which is displayed on the user's computer screen. Users must not leave sensitive information unattended and accessible.
- Sensitive information must not be taken outside of the company unless the user is authorized to do so, and only if encryption or other approved security precautions have been applied to protect that information.

- Sensitive data should not be transmitted through electronic messaging even to other authorized users unless security methods, such as encryption, are employed.
- Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a PDA, thumb drive, or laptop.
- If sensitive data needs to be transported or transferred using removable or portable media, contact the CSO or ISO to obtain approval. The data must remain encrypted at all times and then be removed from the media once the transportation or transferal is complete. Media with hardware-based encryption are strongly preferred over software-based encryption methods.

5. Storage of Sensitive Data

The following rules govern the storage of sensitive data:

- Physical protection must be employed for all devices storing sensitive data. This shall include physical access controls that limit physical access and viewing. When not directly in use, office, lab, and suite doors must be locked and any easily transportable devices should be secured in locked cabinets or drawers.
- Servers with sensitive data must be in locked server rooms with restricted access. This includes static data and data at rest. Servers must have limited user access to those with a need to know, and be controlled by access and password policies. Servers must be protected by virus and firewall policies.
- Users of laptop and other mobile computing devices need to be particularly vigilant and take appropriate steps to ensure the physical security of mobile devices at all times, but particularly when traveling or working away from MorphoTrust USA. All mobile devices must have full disk encryption that is approved by IT.
- Sensitive information must not reside on laptops or other mobile media.
- Computing Services managed servers storing confidential information shall be regularly scanned for vulnerabilities, patched, and backed up.
- Systems (hardware and software) designed to store and transfer confidential records require enhanced security protections and must be closely monitored.
- Personnel data cannot be stored on PCs or other systems in offices or laboratories. Personnel data (including word documents, spreadsheets and Access databases) that is created on a PC or similar system should be stored on a network drive hosted on an IT managed server and have appropriate access control lists (ACLs) which limit access to only authorized individuals.
- Electronic media storing restricted/sensitive data must be protected by password security. To the extent possible, these devices must employ encryption methods.
- Physical records are to be securely stored in such a manner as to prohibit access by unauthorized personnel. Such methods include locked storage cabinets and file rooms.

6. Data Retention and Disposal

The following rules govern the retention and disposal of sensitive data:

- Retention of Records Containing Restricted and Sensitive data: A schedule describing the records and the official retention period is to be created for each type of record created or maintained by MorphoTrust USA. Please refer to the *Data and Document Retention Policy POL-00296-A* for the schedule.
- Archiving: Personnel records, including sensitive information records, which are not being used for active MorphoTrust USA business, may be archived until retention requirements have been met.
- Storage areas for inactive records must be physically secure and environmentally controlled to protect the records from unauthorized access and damage or loss from temperature fluctuations, fire, water damage, pests, and other hazards.

- The contents of true “Shadow” records should be destroyed after it has been determined that they contain only duplicates of records maintained elsewhere, and do not contain any original materials.
- Off-site storage facilities or locations for sensitive records must be approved by the IT, Security, and Legal Departments.
- Record Disposal: The proper destruction of information is essential to creating a credible records management program. Records containing restricted/sensitive data shall only be destroyed in the ordinary course of business; no records that are currently involved in, or have open investigations, audits, legal holds, or litigation pending shall be destroyed or otherwise discarded.
  - No primary records of any type belonging to MorphoTrust USA may be destroyed until they have met retention requirements established by MorphoTrust USA policies and public records law.
  - When retention requirements have been met, records must be either immediately destroyed or placed in secure locations as described in this section for controlled destruction later.
  - The authorized methods of destruction for non-electronic records are burning where authorized or shredding. The authorized methods of destruction for electronic records are wiping or physical destruction of the electronic media and where possible are done by the appropriate destruction standard of the time.

7. Back Up of Data (Data Storage)

All MorphoTrust systems are backed up on a daily basis using an IT-approved backup mechanism. The following rules apply:

- The daily backups are performed on IT equipment stored in primary MorphoTrust offices.
- All backup attempts, both successful and unsuccessful, will be logged.
- For the purpose of this document all storage (internal or external) is referenced as storage. Both internal and external storage are protected equally with hardware (RAID) and redundant hardware components that are capable of supporting enterprise class operations.
- Storage is monitored by both administrators and operations. Monitoring is described in *IT Managing Operations Policy (POL-00090-B)*.

Data Access

The following rules govern access to sensitive data:

- Authorized users access data at the application layer and are bound by the security controls active within the application. Application user access is described in the application control documents.
- In some cases users have access to data on the directory level and have been authorized to do so by the application business owner.
- Remote data access and network security are described in the *IT Computer and System Use Procedures (PRC-00110-A)*.

Data Retention

The following rules govern the retention of sensitive data:

- All backup media is labeled in accordance with the established MorphoTrust USA standard. At minimum the label will contain “MorphoTrust USA”, the date and the sequence number.

Backup Monitoring

The following rules govern the monitoring of backed up data:

- All daily backup sessions are monitored by IT staff each day to ensure there are no issues from the backup the night before.

Exception Reporting

The following rules describe back up exception reporting:

- Exception reporting must alert administrative staff when backups do not run as scheduled, fail, or in any way not perform as planned.
- All backup failures are noted during the weekly review performed by the Manager of Operations.
- IT performs test restores on a quarterly basis.

Disaster Recovery

See MorphoTrust's Disaster Recovery Plan for more information.

8. Destruction of Electronic Media

This section defines the rules governing the proper disposal of media containing electronic data.

If a drive has classified information on it, it must be sanitized according to the procedures mandated by DoD/DSS. Information on these procedures can be found in the *Information Spills and Cleanup Policy, PRC-00312-A*.

The disposal procedures used depend upon the type and intended disposition of the media. Electronic media may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described in the following paragraphs.

- All electronic media must be properly sanitized before it is transferred from the custody of its current owner. The proper sanitization method depends on the type of media and the intended disposition of the media.
- Overwriting hard drives for sanitization: Overwriting is an approved method for sanitization of hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a random pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented.

  Overwriting consists of recording data onto magnetic media by writing a pattern of fluxes or pole changes that represent binary ones (1) and zeroes (0). These patterns can then be read back and interpreted as individual bits, 8 of which are used to represent a byte or character. If the data is properly overwritten with a pattern (e.g., "11111111" followed by "00000000") the magnetic fluxes will be physically changed and the drives read/write heads will only detect the new pattern and the previous data will be effectively erased. To purge the hard drive requires overwriting with a pattern, and then its complement, and finally with another pattern (e.g., overwrite first with "00110101 ", followed by "11001010", then "10010111"). Sanitization is not complete until the three overwrite passes and a verification pass are completed. The facility's Disk Duplicator is to be used for this purpose utilizing the DOD wipe function.

- **Other Systems:** Systems, media, or devices not covered above must be sanitized using the recommended tools provided by the manufacturer or other procedures outlined in this policy.

Definitions

Degaussing is the process of decreasing or eliminating a magnetic field and is the primary method used by MorphoTrust to destroy electronic media. See *Physical Sanitization* for more information.

Drilling is a method of destroying electronic media by drilling holes through the device. See *Appendix A* for more information.

Destruction of electronic media is the process of physically damaging a medium so that it is not usable by any device that may normally be used to read electronic information on the media such as a computer, tape reader, audio or video player.

Clearing data such as formatting or deleting information removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. Because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing media intended for disposal outside of MorphoTrust USA or transported between facilities.

Physical Sanitization (i.e. Physical Destruction): If the recommended software methods listed above and below are not able to remove the data, a computer will not boot, or the internal hard drive or drives are not accessible, then physical destruction is required. Drives and diskettes that need to be destroyed must be sent to Billerica via secure shipment for destruction. Send all devices to

Security Department
MorphoTrust USA
296 Concord Road, Suite 300
Billerica, MA 01821

Note: Physical destruction IS NOT DEFINED as throwing the medium in a trash can.

Disposal of Hard Drives

The following rules govern the disposal of hard drives:

- Disposal of hard drives to other departments or outside MorphoTrust USA: Prior to disposal, operable hard drives must be overwritten in accordance with the procedures in section 8 of the general policy above. The owner must be able to certify that the hard drive was properly sanitized. Written certification should include the make, model, and serial number of the hard drive and the date that the procedure was performed. Equipment designated for surplus or other disposal must have a label affixed stating that the hard drive has been properly sanitized.
- The label should be a high visibility color that is easily recognizable.
- Transfer of hard drives within the corporation: Before a hard drive is transferred from the custody of its current owner, all electronic media must be sanitized per paragraph 1 above.
- Disposal of damaged or inoperable hard drives: The owner must first attempt to overwrite the hard drive in accordance with the procedures described above. If the hard drive cannot be overwritten, the hard drive must be disassembled and mechanically damaged so that it is not usable by a computer. You can physically destroy the hard drive by drilling holes in it or smashing it. Please be careful and be sure to wear safety equipment, like goggles. See Appendix A for a suggested method.

Disposal of Failed Solid State Drives (SSDs)

Failed SSDs are to be turned over to IT for proper destruction.

- Failed SSDs that are still recognized by the operating system: Should be wiped with an approved wiping utility, preferably using the wiping mechanism built into the drive. If the SSD is still under warranty, IT will ship it back to the vendor for replacement.
- Failed SSDs that are not recognized by the operating system: Will be physically destroyed, regardless of whether or not it is under warranty.

Disposal of Electronic Media Other Than Hard Drives

Transfer of electronic media other than hard drives within a department:

- Before electronic media is transferred from the custody of its current owner, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media such as floppy disks, rewritable CD-ROMS, zip disks, videotapes, and audiotapes should be reformatted if the media type allows it or erased if formatting is not possible.

Disposal of electronic media outside of MorphoTrust USA:

All electronic media other than computer hard drives must be rendered unusable before leaving MorphoTrust USA. Hard drives must be disposed of according to the policy governing them above.

If the contents of a drive have been wiped using software, or the drive has been degaussed, a certified commercial disposal system such as “Shred-it” can be used for complete mechanical destruction of the drive. However, a drive which still contains sensitive data on it must be degaussed first before a commercial disposal system can be used.

9. Auditing and Certification

MorphoTrust USA is certified to the American National Standards Institute’s North American Security Products Organization standard ANSI/NASPO-SA-2008 as Security Class I & II. NASPO audits MorphoTrust USA yearly for compliance to the ANSI standard to maintain Security Class I & II Certification. MorphoTrust USA is active in the development of the new International Standards Organization (ISO)’s Management of Security Printing Processes Standard 14298.

All secure data rules must comply with these standards to achieve successful audit results and maintain certifications.

10. Responsibility

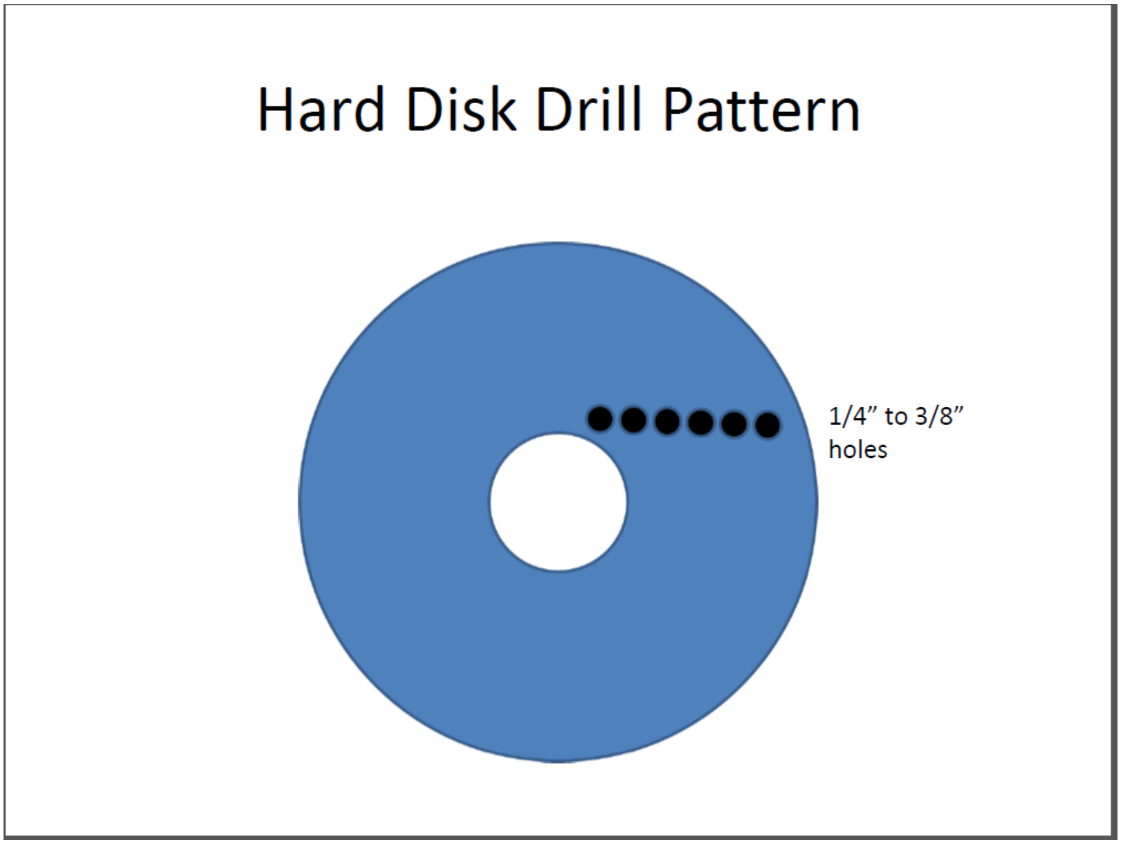
Every MorphoTrust USA employee whose job responsibilities include the maintenance of or use of sensitive data is responsible for implementing and ensuring compliance with this policy and initiating corrective action if needed. In implementing this policy, everyone is responsible for the following:

- Communicating this policy to personnel under their supervision.
- Ensuring that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect personnel/sensitive data.
- Providing education and training in data management principles to employees under their supervision.

All users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. All data users are expected to:

- Access personnel/sensitive data only in their conduct of MorphoTrust USA business.
- Request only the minimum necessary confidential/sensitive information necessary to perform MorphoTrust USA business.
- Respect the confidentiality and privacy of individuals whose records they may access.
- Observe any ethical restrictions that apply to data to which they have access.
- Know and abide by applicable laws or policies with respect to access, use, or disclosure of information.

11. Appendix A – Drilling Pattern to Destroy a Hard Disk



Hard Disk Drill Pattern

1/4” to 3/8” holes

Note: The intent of this drill pattern is to:

- Destroy the drive’s read/write head by having a rough surface at all radii as the disk spins, and
- Maximize the amount of instability when the disk spins at its rated speed.

IT Security

POLICY

Document Number: PRC-000112-A
Revision Level: 03

Approval

Dennis Kallelis Chief Security Officer	Robert Stack Chief Information Officer

This documentation contains confidential and proprietary business information of MorphoTrust USA. This document, including copies of all or and part thereof, may not be released or disclosed to persons other than MorphoTrust USA employees except as necessary for business purposes of MorphoTrust USA under an appropriate confidentiality agreement.

Users are responsible for making sure that they have the current revision of this document

TABLE OF CONTENTS

1. Purpose

MorphoTrust USA is committed to providing a secure work environment that protects the sensitive information that has been entrusted with us by our customers and enables our employees the ability to carry out the mission of the company.

2. Scope

The Corporate Security Policy is designed to manage the security risks that may be present in the environment of MorphoTrust USA. The Corporate Security Policy serves as the overall security program and references other MorphoTrust USA policies relating to security in various aspects of MorphoTrust USA. The program is designed to assure identification of general and high security risks in the area of IT, personnel, building access and the security of confidential information and materials. The program is designed to minimize the risk of secure information or materials related to MorphoTrust USA operations and to develop effective response procedures should a security breach occur.
This program is applicable to all facilities within MorphoTrust USA. Any IT equipment owned or leased and operated by MorphoTrust USA are subject to this policy.

3. Overview

Assessment, communication and training relating to the MorphoTrust USA Security Policies including assessing potential risks relating to the secure operations of all MorphoTrust USA facilities is key to reducing the potential loss of secure information and materials. Employees need to be trained to recognize and report either potential or actual incidents to ensure timely response.

4. Organization and Responsibilities

The Chief Security Officer and the Vice President, Chief Information Officer (CIO) have the corporate responsibilities for the security and privacy of the company. The CSO and CIO are to be notified (via the completion of a Security Incident Report – Appendix A) of any incidents relating to the activities or security incidents that relate to the operation of the Corporate Security Policy.

The CSO and CIO work in collaboration with each department manager to manage all aspects of the Corporate Security Policy.

Department managers must orient new personnel to the department and, as appropriate, to job and task specific security procedures.

Employees, contingent workers and contractors are responsible for learning and following all MorphoTrust USA policies and departmental procedures for security. These policies can be found on the Company SharePoint site as well as in Compli.

The main governing documents that drive and define our information security and privacy access controls are as follows:

- **Need to Know Policy PRC-00141**
- **Privacy Policy PRC-00144**
- **Communications Policy PRC-00123**
- **Classification of Information and Materials Policy PRC-00121**

- **Corporate IT Security Policy PRC-00112 (this document)**
- **Employee Security Screening Policy PRC-00134**
- **IT Information Security PRC-00089**
- **IT Physical IT Access Controls PRC-00091**
- **Liability Policy PRC-00140**
- **Security Awareness Training Policy PRC-00152**
- **Security Quick Reference PUB-00185**

Additional applicable policies exist at the facility level and can be added as needed.

5. Security Events

A Security Event is any attempt to circumvent the security measures or systems protecting MorphoTrust USA IT systems and/or its facilities. All Security Events are to be logged using the Security Incident Report (Appendix A). Security Events include, but are not limited to:

- Unauthorized access to security sensitive data files.
- Unauthorized disclosure of user ID and passwords - especially to third party individuals and organizations.
- Unauthorized copying or transfer to a laptop or removable media.
- Unauthorized removal of security sensitive data files from secure premises.
- A successful or unsuccessful attempt to hack into a file server containing secure data files.
- Corruption of secure data files either by virus attack, user error or other causes.
- Unauthorized re-classification of files and data from secure to non-secure.
- Theft of a server, backup storage unit or Laptop containing security sensitive data.

6. Need to Know

Information of a strategic nature shall only be distributed on a strictly “Need to Know” basis. All personnel are instructed to perform a Need to Know test on all information before distributing or sharing strategic information.

7. Compliance

All MorphoTrust USA employees are required to review, sign off and comply with the Corporate Security Policy. MorphoTrust USA retains the right to modify or change this policy at anytime without notice. If changes are made, employees are expected to review, sign off and adhere to the latest policy as provided by the Chief Security Officer. Adherence to the Corporate Security Policy shall be a condition of employment and of continued employment with the Company. Actions or conduct not in accordance with this policy shall constitute grounds for disciplinary action, including termination of employment.

8. Appendix A

Incident Report on next page.

Security Incident Report

Contact List

Chief Information Officer
Chief Security Officer
President

The completed incident report must be sent to the above email addresses within 24hrs.

Type of Incident (Denial of Service, Espionage, Hoax, Malicious code, Probe, Unauthorized access, Unauthorized use, Stolen/Lost)

Location of the Incident

Address:____
Building:_______________________ Room____________________
Additional Information:_____________________________________

How was the Incident Detected (User, Sysadmin, Help Desk, Communications, etc.)

Who detected the incident (Name): __________________________________
Signature: __________________________________
Time the incident was detected: _____________________________________

Locations of affected system(s):
____
Date / Time Incident Handlers Arrived: ____________________________

Any comments / observations made by the person who detected the incident:

Describe affected information system(s): (One System Per Page)

Hardware Manufacturer	Is affected system connected to the network? **Y N**
Serial Number of CPU	
Corporate Property Number	System Name
O/S Type and version	System IP Address
Service Pack level	MAC Address
Disk capacity (If Known)	
Is affected system connected to a modem **Y N**	← If yes, what is the phone number

Describe physical security of location of affected information system *(locks, alarm systems, building access etc.):*

Additional Comments:

[redacted]

IT REMOTE ACCESS POLICY

Document Number: PRC-00092-B
Revision Level: 09

Approval

John May Chief Information Officer	James Kottas Information Security Officer

Contents

1 Overview

MorphoTrust USA provides remote access for employees and customers to resources on its Local Area Network. This access can be achieved via dial-up, DSL or high-speed Internet connections. The goal of this policy is to outline how employees can access the network data while still protecting that data.

2 Employee Access

Remote employee access is automatically handled through the MorphoTrust USA VPN and is only allowed on company provided/authorized/configured equipment.

No classified information shall be stored locally on these devices, and no Personal Identifiable Information (PII) may be stored on these devices, as described in the *Information Security Customer Data Access and Security Policy PRC-00174-A* and the *Security Governance Policy PRC-00173-A*.

All devices, both MorphoTrust USA provided and personal, must be kept up to date with security patches and utilize passwords or passcodes to access.

Note: Accessing the MorphoTrust USA email system via a personal mobile device grants IT the authority to wipe the device in the case of loss or theft.

Use of these devices shall be subject to inspection by IT at IT’s request.

Cloud backup of mobile devices is not allowed (iPhone data being stored in the cloud, for example).

3 Minimum Home Network Configuration

Personal network configurations used by employees who normally work from home must meet the following minimum standards:

a. Your MorphoTrust USA-issued computer comes with a built-in firewall that is preconfigured on your system and is set to block all inbound traffic from reaching your computer. **This firewall must not be turned off at any time.**

b. Wireless home networks should use at least WPA (Wi-Fi Protected Access) security which requires a reasonably strong password of at least 8 characters with a mixture of letters, numbers and symbols. The use of MAC (Media Access Control) address filtering is strongly encouraged to limit the allowed wireless devices to those in your home.

c. If you purchase your own home networking devices like routers or wireless access points, it is your responsibility to secure those devices. The default passwords that come with home networking devices must be changed and cannot be empty. Please see the *IT Information Security PRC-00089-B* policy for more information on passwords. The complexity of the passwords should follow PRC-00089-B but they do not need to be changed periodically, unless there is suspicion that it might have been compromised or told to unauthorized persons.

4 Remote Control Access

Remote control access is only allowed with MorphoTrust-named personnel. Exceptions to this rule can be granted for trusted third-party vendors (such as Cisco), under MorphoTrust USA IT supervision for diagnostic purposes.

5 General Access Guidelines

Anyone who is not in one of the groups mentioned in the previous paragraph should only access the external website (Webmail, for example).

While wired access (i.e., via your laptop) is the preferred method of access to email and other MorphoTrust USA systems, the use of mobile devices such as smart phones and iPads is allowed so long as they conform to the Company's *Cell Phone and Mobile Device Use Policy (PRC-00237-A*).

It is each employee's responsibility to abide and adhere to all MorphoTrust USA established policies and to control the means by which you have access to such data. Remember, your laptop is a gateway to MorphoTrust USA's network, as well as to the (possible) customer networks you have access to. The means of access (laptop, accounts, passwords, etc.) should be highly guarded.

Do NOT:

- Leave your laptop or mobile device unattended.
- Write down passwords, accounts, etc.
- Use unsecure public web access point. (No Starbucks, Panera, McDonald's, Airports, Hotels Lobbies, etc.) These are public WiFi access points that do not require a password or passcode.
- Leave your laptop in open view in a vehicle.
- Store customer data on your laptop.
- Send customer PII via email.

Do use:

- Common sense and best practices when transporting your laptop. Always lock it in your car trunk and do not leave it unattended.
- When travelling:
  - Obtain a loaner USB cellular modem from IT for secure wireless access. If one of these devices is unavailable, only use your laptop with a wire connection (from your hotel room, for example) rather than over a public, unsecured wireless network. Refer to Section 6 if you are travelling outside the country.
  - Keep your laptop locked up when it is not in use.
- Access the CSN/Customer environments only using a secure, dedicated VPN connection.
- Follow IT Policies for full disk encryption (PGP).

As a general rule, negligent actions on an employee's part that could breach PII by others are grounds for immediate dismissal.

The policies that employees have agreed to are located at http://www.compli.com , the company SharePoint site (Access), and should be reviewed periodically. If you have any questions, please feel free to ask the Chief Security Officer. Always err on the side of caution.

- Make sure your laptop conforms to IT security practices. If you are unsure, please ask IT to check it.
- If your laptop was not built by IT, you are out of compliance. Report it immediately to IT.
- You should always use the secure VPN client issued by IT to remotely access the MorphoTrust USA network.
- If you get a warning or error while trying to connect to the VPN remotely, you should disconnect immediately because a man-in-the-middle attack is active. This is true whether you are accessing over an unsecured network or accessing email via a web browser. Disconnect from the unsecured network immediately and refrain from using any network access at that point.
- When accessing your MorphoTrust email account remotely using a web browser, periodically check to make sure the connection uses "https" at all times. If the browser shows "http," disconnect immediately because a man-in-the-middle attack is active.
- If you don't have a cable lock for your laptop for your office, contact the IT Help Desk who will provide one to you. Lockup your laptop when left in the office overnight, preferably using a laptop lock.
- Check your laptop for PII and remove any PII found. Use the whole disk encryption software to shred it. For example, with PGP Whole Disk Encryption, the PGP Desktop has a PGP Shred function to delete files securely.

6 Interna tional Travel

- You are not allowed to take any of the company's development software code or Subject Contract Information (which includes PII) out of the country.
- You are not allowed to take any export controlled information unless authorized for the destination and end-use by the Export Compliance Officer. Please see the *Technology Control Plan* for additional information on export controls.
- You are not allowed to VPN into the MorphoTrust network from outside of the country.
- You are allowed to use https://mail.l1id.com/ for email only. As stated above, make sure the entire email session continues to use "https" and not "http." If when you first try to connect to the mail server using this URL, you get a warning or error message regarding a certificate, disconnect immediately as a man-in-the-middle attack is active.
- You may not take your company laptop out of the country. Instead get a travel laptop on loan from IT by submitting a request via the Service Manager portal at https://itsupport and upon return to the office, return the travel laptop to IT for sterilization. If you need Microsoft Office installed on the travel laptop, let IT know. Do not transfer files from the loaner travel laptop to company networks or systems after you have returned from your trip. Any files that need to be retained should be emailed to yourself.

- You are allowed to take your company mobile phone on your trip. Notify IT at least a week before you leave so that international calling can be enabled. Otherwise, you will not be able to make or receive phone calls while traveling. Also, if the phone supports wireless networking (WiFi), do not connect the phone to any wireless network while traveling.
- If a portable USB drive is necessary for backup purposes, make sure it is an encrypted drive with AES-256 encryption. This drive must not contain any Subject Contract Information or PII while traveling. When you return from your trip, do not connect this drive to any MorphoTrust equipment. All files will need to be securely deleted and the drive reformatted by IT first. Then the drive will be able to be reused. To preserve any files on the drive, use the travel laptop to email them to yourself first using https://mail.l1id.com/.
- No source code files can be taken outside the country on any kind of portable device.
- Do not connect your devices to a Safran or Morpho affiliate network of any kind (wired or wireless) using any method.
- Be sure that you only connect to known valid WiFi or wired connections. Refer to Section 5 for more information. Do not use WiFi connections that are not secured, that is, they have no password or passcode.

PHYSICAL IT ACCESS CONTROLS POLICY

Document Number: PRC-00091-B

Revision Level: 01

Approval

Robert Stack Chief Information Officer	Robert Eckel President

Users are responsible for making sure that they have the current revision of this document.

TABLE OF CONTENTS

1 Ov erview:

The server room is a vital infrastructure component of MorphoTrust USA. As such, its access shall be restricted to those individuals that have a need to work with the servers in the server room. This is physical access control.

2 Polic y:

- Access to the Server Room is controlled.
- The Server Room is a locked facility.
- The Server Room must have a keycard entry system that monitors and logs who has accessed it and when.
- Daily server room access is restricted to IT department personnel.
- Only authorized individuals are allowed in the Server Room.

3 Procedur e:

- Only authorized individuals are allowed in the Server Room.
- The CIO is the authorization agent.
- The CIO is the only one authorized to add an individual to the access key card list for the Server Room. The CIO makes these requests to the key card agent.
- Contractors requiring access to the Server Room must be authorized by the CIO.
- Contractor’s granted access shall be escorted by an IT department member. Unescorted contractor access requires authorization by the CIO.
- The CIO will regularly review server room access logs.

IT Network Access Controls Procedures

Document Number: PRC-00091-B
Revision Level: 02

Approval

John May Chief Information Officer	James Kottas, Chief Privacy & Information Security Officer

Table of Contents

1. Introduction

This document defines the controls governing access to the MorphoTrust USA (the Company), IT network, both physical and electronic. Access is dealt with on three fronts:

- Physical access to Server Rooms
- Firewall protection
- Connecting devices

The IT Network is a vital infrastructure component of the Company and is housed within dedicated Server Rooms. Access to these rooms and the servers and computers held within it is restricted to those individuals that have a need to work with this equipment.

The IT network, servers, and computers are further protected from unauthorized usage, client generated faults, bandwidth abuse, and virus intrusion by the Company Firewalls.

Only authorized devices may be connected to the network. All devices attached to the MorphoTrust USA IT networked need to be approved by IT Management or the CIO.

2. Server Room Access

The following rules control access to the IT Server Rooms:

- Each Server Room is a locked facility.
- All Server Rooms must have a keycard entry system that monitors and logs who has accessed it and when.
- Daily server room access is restricted to IT department personnel.
- Only authorized individuals are allowed in a Server Room.
- The CIO is the authorizing agent.
- The CIO, the CSO or their designees are the only people authorized to add an individual to the access key card list for the Server Room. These requests are made to the key card agent.
- Contractors requiring access to a Server Room must be authorized by the CIO/CSO/designee.
- Contractors granted access shall be escorted by an IT department member. Unescorted contractor access requires authorization by the CIO and CSO.
- The CIO reviews Server Room access logs quarterly.

3. Firewall

The following rules define the Firewall policy:

- Firewalls shall be put in place where ever there is access to the internet. Remote access using approved IT software and methods may be granted to allow employees access to critical systems within the MorphoTrust USA network.
- Remote access to critical systems, if allowed, requires a two-factor authorization method such as password and biometric (finger or voice print) and/or a token or digital certificate.
- Internal firewalls shall be used to protect critical data from internal intrusions.
- The firewall must be configured for stateful packet filtering with all ports closed until rules and filters have been applied.
- Firewall rules and Packet Filtering logging must be enabled to log all attempts associated with rules and filters.
- Both internal and external firewalls shall include Intrusion Protection Systems and/or Intrusion Detection Systems to both evaluate suspected intrusions and signal alarms.
- Attempted intrusion alarms automatically alert IT management who are responsible for evaluating the attempt and escalating the alarm through the standard procedures, including notifying the CSO.
- External firewalls shall be tested for security weaknesses on a quarterly basis, including ethical hacking.

- The firewall system administrator is responsible for implementing and documenting all rules and filters.
- The initial configuration of the firewall and all changes must be approved by the Change Control Board (CCB) led by the senior-most operations manager and the CIO, in writing.
- Changes to the base firewall infrastructure must go through the MorphoTrust USA IT Change Control Management Process.
- Any operational alterations to the existing firewall must be approved by the CCB and the CIO, in writing.
- All security changes to the firewall must be tracked by the IT Change Control System and all security events shall be tracked in the security log.
- The firewall rules and filters shall be reviewed every quarter by the Manager of Operations and rationalized against 1) service needs and 2) customer requirements.

4. Connecting to the Network

The following rules apply to connecting computers and other devices to the IT network:

- Computers can only be attached to the network if they have virus protection.
- IT network wiring may not be modified or extended beyond the area of their intended use. This applies to all network wiring, hardware, and data jacks.
- The network may not be used to provide Internet access to anyone outside of MorphoTrust USA for any purposes other than those that are in direct support of the corporate mission.
- The IT network is a shared resource. Thus, network use or application use which inhibits or interferes with the use of the network by others is not permitted. (For example, applications which use an unusually high portion of the bandwidth for extended periods of time, thus inhibiting the use of the network by others, are not permitted.)
- Equipment attached to the network must be CE certified and must conform to recognized network standards.
- Equipment attached to the network must not be run in promiscuous mode, except by special arrangement with IT.
- Equipment attached to the network may be monitored for security and network management purposes, and to verify its continued presence on the network.
- Any computer that has been on an outside network must first be brought to IT in order to allow for a complete virus/Spyware scan prior to re-admittance of the computer back onto the MorphoTrust USA network.

5. Additional Information

Please refer to *IT Computer and System Use Procedures (PRC-00110-A)* for further information.

IT MANAGING OPERATIONS POLICY

Document Number: PRC-00090-B

Revision Level: 01

Approval

Robert Stack Chief Information Officer	Robert Eckel President

Users are responsible for making sure that they have the current revision of this document.

TABLE OF CONTENTS

1 Overview

This document covers areas addressed by IT Operations: job monitoring, issue logging, incident notification, backup monitoring, and media handling.

- The Network Administrator monitors exceptions with jobs and system exception notices for Linux and Windows servers.
- The administrator also monitors the backup storage manager for backup process exceptions and tape mounts.

Table 1:IT center locations

Server Rooms	Location
MorphoTrust USA HQ	Billerica, MA
Indiana	Ft. Wayne

2 Policies

2.1 Monitoring of event logs & server health

- Server operating systems (Linux and Windows) log events to their system logs which are collected for administrator review and event detection monitoring using ELM software.
- Maintain a current network diagram of hard production cards. (CSN)

2.2 Events are logged to server system logs as they occur.

- Network staff monitors the various consoles described in table 2 that report system errors that require intervention.
- Automated Error handling and paging will manage alerts for the administrators. Errors are automatically filtered and notification sent depending on severity.
- If documentation exists, the operator may refer to the document to determine how to react to the displayed error.

Table 2 (below) describes the monitoring activity and supporting systems for responding to errors.

Table 2: Operations Monitoring

System/application	Monitoring mechanism	Support system
Linux and Windows server health	ELM software	Network administrators

2.3 Reporting issues/incidents

- A list of primary contacts for each application or infrastructure team located at HQ is maintained by the IT organization. The list is used to determine who to contact to manage an issue that the network support staff person cannot handle.
- An escalation procedure exists so that if the network support staff fails to respond to the problem, users escalate to the Head of the IT Department.

2.4 Logging of issues

- All issues are logged by the Network Administrator as per the Change Management Policy. A report of issues logged is created at the end of each day and emailed to the IT staff.
- Issues are categorized based on severity and the severe issues are discussed with the CIO

2.5 Software Solutions

- Monitoring software (What's Up) has been deployed and is configured to immediately send email alerts to the appropriate personnel upon detection of high risk events such as virus detection and denial of service activities.
- Security administrators will take appropriate action to mitigate disruption due to these events.

3 Documentation

3.1 Network

- A topology of the network environment has been created to diagram the configuration of the MorphoTrust USA network.
- The documentation is updated promptly to reflect any changes that occur within the environment.

3.2 Database

- Full documentation for any database within the environment will be maintained. This documentation will include data structures, data dictionary, and configuration information.
- This documentation will be updated promptly upon any changes made to the database.

3.3 Tools and applications

- All tools and applications within the environment will have documentation on use and configuration.
- The latest versions of these documents will be readily available to all administrators of these systems.

4 Training

- Users and administrators of the various systems will be trained in the appropriate use and configuration of system implementation procedures, tools and applications as appropriate for their job descriptions.
- Management will periodically review to ensure that appropriate training is available and utilized.
- Training will be made available for all new versions of existing applications and systems as well as for the introduction of new systems.
- New employees will be trained in the use and operations of all relevant systems and applications.

IT INFORMATION SECURITY POLICY

Document Number: PRC-00089-B

Revision Level: 06

Approval

Eric Ammon IT Manager	John May Chief Information Officer
Dennis Kallelis Chief Security Officer	Robert Eckel President

TABLE OF CONTENTS

1 Overview

- This policy provides the security measures to be used for all password protected systems, applications and devices.
- The CIO is responsible for implementing password rules. Variances from this policy must be approved by the CIO in writing.
- The CIO is responsible for maintaining the appropriate approval/change documentation.
- This policy does not grant user rights.
- System rights are granted by the system administrator. Those system rights granted beyond public rights are determined by employee activation (human resources), department (functional rights) and line management (user rights).

2 Passwords

- Passwords are confidential information. Password security is enabled when user passwords are confidential among users and unknown to system administrators.
- Credentials cannot be exchanged between users.
- Open communication regarding passwords is discouraged. Users should not leave password information in the workstation (e.g. post notes, etc.)
- System administrators must force the user to change the initial password immediately after the initial user logon session.
- If an employee or third party is careless with password information, password changes should be forced immediately.
- System administrators are responsible for monitoring, tracking, and following-up on unsuccessful logon attempts.
- System administrators are responsible for configuring the operating system environment according to the password rules in this policy and are to provide training to users for password changes and security. Such rules include:
  - Password history enforced at 5 passwords
  - Maximum password age: 60 days
  - Passwords are not stored using reversible encryption
  - The account lockout threshold is set to five (5) invalid logon attempts
  - The account lockout duration is set to 30 minutes, after which the account lockout counter is reset
  - 15 minute time-out for windows screen lock
- Super user passwords will be generated and provided to System Administrators upon approval from the Director of IT Infrastructure. Super user passwords are subject to the password rules defined in the password table below.

2.1 Vendor Defaults

All vendor-supplied default passwords must be changed before any computer or communications system is connected to a Company network or used for Company business. This policy applies to passwords associated with end-user IDs, as well as passwords associated with system administrator and other privileged users.

3 Dual Access & Biometric Access Controls

- Certain computers containing secure material and processes may require the use of two or more passwords, each known by a separate individual, and/or fingerprint scans to access.

- The facilities manager and/or the Chief Security Officer, in cooperation with the CIO, shall identify which systems require such access.

4 Workstation and Application Timeouts

- All servers, workstations and applications in the MorphoTrust USA environment will be configured to lock out the user after 15 minutes of inactivity. This is set through the GPO (Group Policy Object) within Active Directory within the domain.
- All servers should be locked prior to leaving the server.

5 Data encryption

- Any data, sensitive in nature, that is being transmitted external of the MorphoTrust USA network and not using the established VPN for transmission will be encrypted.
- No sensitive data may be transmitted to Safran/Morpho affiliates.

6 Access Review

- On a quarterly basis a listing of all user privileges of systems and applications will be provided to the owner of each system.
- A review of appropriateness will take place by the system owner with adjustments being made immediately.
- Access requests are to come from the employee's manager to IT.

7 Network & System Access

- Network and System accounts are created by a security administrator after receiving an approved request from human resources. The user account's access is specified in the request and access is approved/granted per the specifications. An initial password is issued which automatically prompts the user to change the password on their first login attempt. Password structure, expiration, and reuse limitations are described below:

System/ Application	**Length**	**Characters**	**Expiration Interval**	**Depth**
Systems:	Min. – 8 Max. – System Determined	Alpha-numeric – minimum 1 numeric	60 days	5
Applications:	Min. – 8 Max. – Application Determined	Alpha-numeric – minimum 1 numeric	60 days	5

- Workstation/Laptop administrator logon is created during the operating system install. A password is specified by the system administrator during setup. The password does not expire so that multiple system administrators may service the system. All local system passwords should be the same and should conform to the guidelines noted above.
- **Note:** application administrators may have system administrator security access so that they may install software and restart the server. Application administrators may not log a server onto the domain. They must contact a domain administrator to do so.
- Initial password assignment:
    - **Domain Login**: Initial passwords must be changed on first login via software enforcement
    - **Network devices**: Initial passwords are changed during device setup
    - **Firewall devices**: Initial passwords are changed during device setup

8 Disposal of Equipment

- All computer equipment must be sent to IT to ensure that any sensitive information or licensed software is physically destroyed, or securely over-written, prior to disposal or re-use.

IT FIREWALL POLICIES AND PROCEDURES

Document Number: PRC-00088-B

Revision Level: 05

Approval

John May Chief Information Officer	Robert Eckel President

TABLE OF CONTENTS

1 Overview:

The IT network, servers, and computers are the backbone of our corporate business. These must be protected. The MorphoTrust USA firewall must be controlled and managed to ensure this protection.

2 Policy:

- Firewalls shall be put in place where ever there is access to the internet. Remote access using approved IT software and methods may be granted to allow employees access to critical systems within the MorphoTrust USA network.
- Remote access to critical systems, if allowed, requires a two-factor authorization method such as password and biometric (finger or voice print) and/or a token or digital certificate.
- Internal firewalls shall be used to protect critical data from internal intrusions.
- The firewall must be configured for state full-packet filtering with all ports closed until rules and filters have been applied.
- Firewall rules and Packet Filtering logging must be enabled to log all attempts associated with rules and filters.
- Both internal and external firewalls shall include Intrusion Detection Systems to both evaluate suspected intrusions and signal alarms.
- Attempted intrusion alarms automatically alert IT management who are responsible for evaluating the attempt and escalating the alarm through the standard procedures, including notifying the CSO.
- External firewalls shall be tested for security weaknesses on a quarterly basis, including ethical hacking.
- The firewall system administrator is responsible for implementing and documenting all rules and filters.
- The initial configuration of the firewall and all changes must be approved by the Change Control Board (CCB) led by the senior-most operations manager and the CIO, in writing.
- Changes to the base firewall infrastructure must go through the MorphoTrust USA IT Change Control Management Process.
- Any operational alterations to the existing firewall must be approved by the CCB and the CIO, in writing.
- All security changes to the firewall must be tracked by the IT Change Control System and all security events shall be tracked in the security log.
- The firewall rules and filters shall be reviewed every quarter by the Manager of Operations and rationalized against 1) service needs and 2) customer requirements.

IT Electronic Communication Policy

Document Number: PRC-000113-A

Revision Level: 02

Approval

Dennis Kallelis Chief Security Officer (CSO)	Robert Stack Chief Information Officer (CIO)

Users are responsible for making sure that they have the current revision of this document.

TABLE OF CONTENTS

1 Purpose

This policy establishes standards for the proper use of MorphoTrust provided electronic mail (email) services.

2 Scope

This policy applies to:

- All electronic mail systems and services provided or owned by MorphoTrust USA.
- Transactional information associated with email records (such as email headers, summaries, addresses, and addressees) as well as the contents of those records.
- All users of email services, including:
  - Full and part-time employees
  - Contractors authorized to use MorphoTrust USA-owned equipment or network resources
  - All other users of MorphoTrust USA information technology resources
- All MorphoTrust USA email records in the possession of any company email user.

3 Details

3.1 E-mail

Email is an efficient and timely communications tool that is provided by MorphoTrust USA to its employees and contractors to assist them in supporting the company's functions and conducting business within its own organization, with government and private business partners, and with the public. Appropriate use of the email system can enhance productivity and communication, but inappropriate use can conflict with MorphoTrust USA policies and compromise availability of the system for all. This policy defines requirements and prohibitions for the appropriate use of the email system or any messaging system.

Principles

- Use of the email system constitutes consent to abide by all elements of this policy.
- Any electronic mail address or account assigned by MorphoTrust USA is the property of the company and under management control of the CIO.
- Email messages are the equivalent of letters sent on official letterhead, and must therefore be written in a professional and courteous tone. If an email signature is being utilized, it must adhere to the policies set forth by the MorphoTrust USA Marketing Department.
- MorphoTrust USA email is public communication and therefore, senders and receivers of email can have no expectation of privacy and are subject to company inspection and legal discovery.

- All emails between MorphoTrust USA employees and Safran/Morpho employees are automatically logged and stored by the server.
- Faxes between MorphoTrust USA employees and Safran/Morpho employees is prohibited.

Unacceptable Behavior

- Use of company communications systems to set up personal business, send chain letters, promote political causes or outside organizations, or any other non-job-related solicitations.
- Forwarding of company messages to external sources whether they are company confidential or not.
- Distributing, disseminating, or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.
- Distributing, disseminating, or storing images, text or materials that might be discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment.
- External internet hosted services that do not offer any business value or pose an excessive risk. For example, some services are allowed (ex: LinkedIn) others are not allowed (ex: Facebook, Twitter, MySpace) during normal working hours.
- Accessing copyrighted information in a way that violates the copyright. Also, the sending or receiving of trade secrets, proprietary financial information, import/export information, personal identifiable information (PII) or similar materials without prior authorization.
- Breaking into the company's or another organizations email system or unauthorized use of a password/mailbox.
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- Transmitting unsolicited commercial or advertising material
- Undertaking deliberate activities that waste staff effort or networked resources
- Introducing any form of computer virus or malware into the corporate network

3.2 Monitoring

In order to ensure compliance with this policy, the company reserves the right to use monitoring software in order to check upon the use and content of emails.

3.3 Sanctions

Failure to comply with these guidelines will result in sanctions ranging from disciplinary procedures such as verbal and written warnings, through to dismissal.

IT DISASTER RECOVERY POLICY

Document Number: PRC-00095-B

Revision Level: 02

Approval

Robert Stack Chief Information Officer	Robert Eckel President

Users are responsible for making sure that they have the current revision of this document.

TABLE OF CONTENTS

1 Assump tions

MorphoTrust USA's main IT components reside at the Billerica Massachusetts USA facility. This Disaster Recovery Plan defines the process for protecting and recovering the major IT infrastructure components at MorphoTrust USA Billerica. It does not define the process for individual departments.

This plan defines the steps that are necessary before a disaster strikes. Being prepared is our best action.

The plan also defines the process for recovery after a disaster strikes and the goal of getting back to normal business. Knowing what to do is our best protection.

This plan does not discuss disasters that do not hurt the facility, such as snow storms. Normal business today allows for the employees to work at a distance via email, the web, their home computers, and VPN. This document only addresses recovery of the IT components, not of the human resource issues of personnel outside of IT.

This plan covers the case of the Billerica Center being damaged or non-operational. This assumes that the backup location in Fort Wayne, is still operational and can be utilized in the recovery process.

Depending on the level of disaster (power outage to complete destruction), data and application loses shall range from minimal to substantial. Some data may not be recoverable depending on the level of the disaster and the time since the last back-ups were moved off site. Hence a disaster is a loss of time, information, money, and opportunity. The time to recover directly affects all of these items.

Individual departments are responsible for ensuring that their data and applications are part of the IT facility. Unauthorized systems must not exist on the network.

2 Pre-disa ster Procedures

Proactive protection and duplication of data is the key to preparedness.

Systems in the IT facility shall be protected via:

- Secure locked facility
- Air conditioning
- Emergency lighting
- Fire detectors and alarms
- Security Audit Trail of entry and exits
- Password protected systems
- Battery back up UPS systems
- Antivirus systems
- Firewalls
- Back up of data and applications on servers
- Back up of user systems on site
- Off site data storage
- Application inventory
- Automated system status alarm mechanisms
- Change Management policy
- Skilled and knowledgeable IT staff

The following procedures have been written to ensure this happens as regular business practice.

- IT Physical IT Access Controls Policy and Procedure
- IT Firewall Policy and Procedure
- IT Remove Access Policy and Procedure
- IT Computers on the Network Policy and Procedure
- IT Virus Protection Policy and Procedure
- IT Backup and Disaster Recovery Policy and Procedure
- IT Information Security Policy and Procedure
- IT Managing Operations Policy and Procedure
- IT Change Management Policy and Procedure
- IT Manage Performance Policy and Procedure
- IT Electronic Communications Policy and Procedure

2.1 Bac kups

All systems shall be backed up according to the IT Backup Recovery Policy. (PRC-00084-B**).**

All operating systems and applications are backed up on a daily basis.

Incremental backups will be considered for development, QA, and pilot systems.

IT shall follow the policies and procedures contained within the system & database backup & recovery guide.

.

2.2 Onsite Storage

All daily system backups are kept on the Iron Mountain Turbo Restore Appliance (TRA) for a period of one year.

2.3 Offsite storage

Daily backups are uploaded to the Iron Mountain Cloud once complete. These off site backups are retained for a period of seven (7) years..

IT is the authorized contact with Iron Mountain to request backups older than one year..

2.4 Retention

All backups are retained on site for one year. Uploaded backups are retained on the Iron Mountain Cloud for a period of seven (7) years. Monitoring

Daily backup sessions are monitored by the IT staff to ensure that errors are resolved in as timely a manner as possible, and that tape mounts are satisfied.

IT uses the storage manager console to monitor backups and to administrate the backups should they require intervention.

Exception reporting occurs thru the storage manager console which alerts administrative staff when backups do not run as scheduled, fail, or in any way not perform as planned.

All exceptions to the backup schedule are automatically emailed to a mailbox monitored by the Network Administrator.

2.5 Auditing

All backup failures are recorded within the MorphoTrust USA Helpdesk application.

2.6 Restoring

Data restores are managed using the same storage manager systems that are used for the backups.

2.7 Remote Access

The IT systems can be managed, if necessary, remotely via VPN login. In cases where the building is not accessible and the IT facility is still up and running, the IT administrators can log in and manage the systems. Likewise all users have remote web access to email and can VPN to perform their daily task, including time cards and expense reports. This enables MorphoTrust USA to continue operations at a distance.

2.8 Recovery Services

If the Billerica facility is destroyed or inaccessible for a period of time, the systems can be rebuilt from the Iron Mountain Cloud at MorphoTrust USA facility in Fort Wayne or at a restoration facility with ample resources.

2.9 Training for Disaster

IT and Management must know the plan's details: who is in charge of making IT decisions and support IT staff and their actions taking place during recovery. Other department staff and contract IT experts are required at this time and expenditure is assumed to be automatically pre-authorized in time of crisis.

2.10 Continuous Disaster Drill Training – Be prepared to respond.

Regular audits of backups are performed. Quarterly staff review of the disaster plan must occur in order to enable preparedness in time of crisis. Likewise, this plan must be updated as technologies change and as systems alter.

3 Post Disaster

A disaster is defined as any event, either natural or man-made, that results in either a loss of systems functions or integrity of the facility, including but not limited to:

- Breach of IT systems resulting in the loss of power and/or functionality
- Flooding
- Physical breaches resulting in the loss of perimeter integrity
- Theft of secure data and/or materials.

3.1 Disaster Assessment and Response

At the moment of a crisis that affects IT, the CIO needs to make fast assessment and decisions. Key to the fast response is constant knowledge of the state of all IT components. Once an evaluation assessment is complete actions must be taken to return the system to functional.

Restoring the physical security of the facility must be of the highest priority. The designated breach manager will work with the local police authorities to guard the facility from further damages or breaches while waiting for the MorphoTrust USA contracted security firm personnel to arrive on scene and assume responsibility for protecting the property.

MorphoTrust USA has under contract a national security firm with the ability to deploy uniformed, armed guards to our facilities in a matter of hours in the event of a disaster, either natural or man-made.

3.2 Setting Priorities

The CIO is empowered to set and establish IT disaster and action priorities.

IT Management is empowered to set recovery task priorities to get the business back up and running. IT Management is responsible for informing the users (if possible) of that status of IT infrastructure during disaster recovery.

Priority always goes to getting the main business back up and running. This typically is the corporate information sharing components like email, the web page, and VPN.

Critical systems such as sales orders fulfillment, financial systems, and accounting are always priority systems. Secondary Priority IT systems are the applications and servers for development and marketing.

4 Disabling non-priority Services

Disaster response and recovery often includes the disabling of non-priority IT services. This includes shutting down services,

- ♦ to prevent the spread of a greater disaster
- ♦ to protect corporate information
- ♦ to utilize resources to bring backup downed systems
- ♦ to reuse systems for higher priorities
- ♦ to relocate systems

4.1 Key Jobs Positions IT and Executives and Departments

In disasters that are large enough to affect multiple groups or involve a long recovery time, IT Management shall consult with the Executive Team, but not be limited in its response by having to wait for someone. When the Executive Team is not available for immediate response, then the CIO sets the priorities.

5 Responsibilities

5.1 Authority and Authorization to Spend

The CIO is authorized to make decisions to get systems up and running. When the CIO executive is unreachable, and critical systems are down, the CIO is pre-authorized to make expenditures related to system recovery. This includes immediate outside services. The CIO is the designated Breach Manager.

6 Decision Making

6.1 Access to Plan

This plan is available to all IT employees and resides on the IT department’s SharePoint site.

6.2 Access to Contacts

Emergency contact list and numbers are t maintained and accessible through the IT Department’s SharePoint site. This list also contains vendors, contacts, and numbers that can be used during emergencies. This list is maintained and reviewed quarterly by IT Management.

6.3 Salvaging

The CIO is authorized to decide what systems/hardware can be salvaged and if not how to properly dispose of destroyed equipment.

7 Relocation of systems

The CIO is authorized to make decisions to get systems up and running. When the CIO’s executive is unreachable and critical systems are down, the CIO is pre-authorized to make expenditures related to system recovery. This includes immediate outside services.

8 Relocation of personnel

IT personnel may need to relocate to hot sites in order to reconstruct systems and to reactivate business. The CIO is authorized to send staff or hire temporary contract staff to get these emergency systems activated.

9 Finance/Purchasing

The financial system administrators are responsible for getting the financial system back into operation for their users. The IT staff shall work in cooperation with the financial system staff to facilitate this task.

10 Development

Development is responsible for reconstructing their laboratory system in times of a disaster. Once the main IT systems are back up and operational, the IT staff shall assist the development teams in their reconstruction.

Therefore the development teams are responsible for knowing what their software application tools are, what their test and development environments are, and how to reconstruct them.

IT is responsible for getting the development servers and applications that are part of the IT server room back up.

Development users are responsible for getting their own office PCs data restored in case of disaster.

11 Cus tomer Support

Customer Support is to work closely with IT to restore their necessary services. These services include the resumption of phone service, Applix database access, and the ability to access remote networks.

12 Return to Normal Business

Returning to normal business is the goal of this disaster recovery approach. Senior management has determined that at this time it is acceptable for this process to take up to five (5) business days to accomplish.

13 Plan updates

This is a living document and needs to be reviewed quarterly. Updates are to be made as technology changes and the environment evolves. IT Management is responsible for informing the IT staff of changes and keeping the document updated and publicly available to the IT staff.

IT POLICIES
COMPUTERS ON THE NETWORK

Document Number: PRC-00086-B

Revision Level: 01

Approval

Robert Stack Chief Information Officer	Robert Eckel President

Users are responsible for making sure that they have the current revision of this document.

TABLE OF CONTENTS

1 Overview:

- The IT network is the backbone of corporate business. The IT network must be protected. This includes protection from unauthorized usage, client generated faults, bandwidth abuse, and virus intrusion.

- Only authorized devices may be connected to the network. All devices attached to the MorphoTrust USA IT networked need to be approved by IT.

2 Policy:

- Computers can only be attached to the network if they have virus protection.

- IT network wiring may not be modified or extended beyond the area of their intended use. This applies to all network wiring, hardware, and data jacks.

- The network may not be used to provide Internet access to anyone outside of MorphoTrust USA for any purposes other than those that are in direct support of the corporate mission.

- The IT network is a shared resource. Thus, network use or application use which inhibits or interferes with the use of the network by others is not permitted. (For example, applications which use an unusually high portion of the bandwidth for extended periods of time, thus inhibiting the use of the network by others, are not permitted.)

- **Equipment attached to the network must be CE certified and must conform to recognized network standards.**

- **Equipment attached to the network must not be run in promiscuous mode, except by special arrangement with IT.**

- **Equipment attached to the network may be monitored for security and network management purposes, and to verify its continued presence on the network.**

- **Any computer that has been on an outside network must first be brought to IT in order to allow for a complete virus/Spyware scan prior to re-admittance of the computer back onto the MorphoTrust USA network**.

IT Computer and System Use Policy

Document Number: PRC-00110-A

Revision Level: 10

Approval

John May Chief Information Officer	Robert Eckel President

Table of Contents

1. Introduction

This document describes the controls employed to protect MorphoTrust USA's (The Company) IT network equipment and, by extension, the sensitive information entrusted to us by our customers. Only authorized devices may be connected to the network and must be approved by IT Directors or the CIO.

This policy applies to all MorphoTrust USA IT equipment (either owned or leased). The following topics are addressed:

- Vendor Passwords
- Passwords and Dual and Biometric Access Controls
- Network and System Access Accounts
- Virus Protection
- Use of Company Equipment and Software
- Internet Use
- Remote Access
- International Travel
- Encryption
- Privacy

Refer to the Cell Phone and Mobile Device Policy POL-00237-A for information about such devices.

2. Vendor Passwords

All vendor-supplied default passwords must be changed before, or shortly thereafter, any computer or communications system is connected to a Company network or used for Company business. This policy applies to passwords associated with end-user IDs, as well as passwords associated with system administrator and other privileged users.

3. Passwords

Network and System accounts are created by a security administrator after receiving an approved request from human resources. The user account's access is specified in the request and access is approved/granted per the specifications. An initial password is issued for the account which automatically prompts the user to change the password on their first login attempt. Password structure, expiration, and reuse limitations are subject to change as needed and are described below:

System/ Application	Length	Characters	Expiration Interval	Depth
Systems:	Min. – 8 Max. – System Determined	Alpha-numeric – minimum 1 numeric	60 days	5
Applications:	Min. – 8 Max. – Application Determined	Alpha-numeric – minimum 1 numeric	60 days	5

The following rules apply to the issuance and use of passwords:

- Passwords are confidential information. Password security is enhanced when user passwords are confidential among users and unknown to system administrators.
- Credentials cannot be exchanged between users.
- Users should not leave password information in the work area (e.g. sticky notes, etc.)
- System administrators must force the user to change the initial password immediately after the initial user logon session.
- If an employee or third party is careless with password information, password changes should be forced immediately.
- System administrators are responsible for monitoring, tracking, and following-up on unsuccessful logon attempts.
- System administrators are responsible for configuring the operating system environment according to the password rules in this policy and are to provide training to users for password changes and security. Such rules include:
    - Password history enforced at 5 passwords
    - Maximum password age: 60 days
    - Passwords are not stored using reversible encryption
    - The account lockout threshold is set to five (5) invalid logon attempts
    - The account lockout duration is set to 30 minutes, after which the account lockout counter is reset
    - 15 minute time-out for windows screen lock
- Super user passwords will be generated and provided to System Administrators upon approval from the Director of IT Infrastructure. See the *Passwords* section for more information.
- Workstation/Laptop administrator logon is created during the operating system install. A password is specified by the system administrator during setup. The password does not expire so that multiple system administrators may service the system. All local system passwords should be the same and should conform to the guidelines noted above.

Note: Application administrators may have system administrator security access so that they may install software and restart the server. Application administrators may not join a server to the corporate domain. They must contact a domain administrator to do so.

4. Dual Access and Biometric Access Controls

Certain computers containing secure material and processes may require the use of two or more passwords, each known by a separate individual, and/or fingerprint scans to access.

The facilities manager and/or the Chief Security Officer, in cooperation with the CIO, shall identify which systems require such access.

5. Virus Protection

This section describes the virus protection efforts the Company employs to prevent network virus outbreaks and network security attacks involving computers associated with the Company. The following rules apply:

- All files downloaded to the MorphoTrust USA network potentially harbor computer viruses, Trojan horses, worms or other destructive programs and, therefore, all downloaded files must be scanned for such viruses. Virus detection programs and practices shall be implemented throughout the MorphoTrust USA environment.
- Training must take place to ensure that all computer users know and understand safe computing practices.
- IT administration will be held responsible for ensuring current software is on the network to prevent the introduction or propagation of computer viruses.
- Any activity with the intention to create and/or distribute malicious software by means of the MorphoTrust USA networks is strictly prohibited.
- MorphoTrust USA will employ virus management measures at appropriate ingress and egress points of the company networks. MorphoTrust USA will implement virus control procedures to ensure that all computer servers and workstations are protected against viruses.
- All Windows-based computers, including workstations, laptops, development servers, production servers, and tablets that run Windows, and whether physical or virtual machines, must run a managed client version of antivirus software that has been approved by IT. Allowable exceptions are:
    - If a customer provides a customer-owned Windows computer as part of a contract with MorphoTrust, this computer can use the antivirus software as provided or installed by the customer. This antivirus software must be well-known and approved by IT. If the computer does not contain any antivirus software, the standard MorphoTrust antivirus software must be used.
    - Any other special cases must be reviewed and approved by both the IT and Security Departments.
- Non-Windows-based computers should use antivirus software that is approved by IT whenever possible.

Virus Procedures for Workstations, Laptops/Tablets, and Development Servers:

- All data and/or program files must be scanned for viruses before installation to safeguard MorphoTrust USA networks from infection. This includes shareware and freeware obtained from electronic bulletin boards or on disk (diskette or CD-ROM), custom-developed software, and software received through business sources.
- All data and program files that have been electronically transmitted to a MorphoTrust USA computer from another location, internal or external, must be scanned for viruses immediately after being received.
- All computer media (diskette, CD, etc.) are potential sources for computer viruses. Therefore, all media must be scanned for virus infection before it is used in a MorphoTrust USA computer or network server.
- Virus protection software that is centrally managed by IT shall be loaded on each desktop/mobile computer and development server, regardless if it is virtual or physical, and stay a resident program to constantly monitor for viruses to prevent introduction to the network. Any exceptions must be approved by both the IT and Security Departments.

Virus Procedures for Production Servers:

- Virus protection software that is centrally managed by IT shall be loaded on each production server and stay a resident program to constantly monitor for viruses to prevent introduction to the network. Any exceptions must be approved by both the IT and Security Departments.

Email Virus Procedures

- All email and attachments to email are scanned to prevent viruses from entering through the email system.
- All emails are filtered prior to entering the MorphoTrust USA network through a best-practice email filtering application. This application uses multiple anti-virus engines and all anti-virus signatures are updated in real-time.
    - The whitelist for the email filtering application should be reviewed at least once a year to verify that each whitelist entry is still valid.
- Reports are generated monthly to ensure compliance.

Updating Virus Definitions

- MorphoTrust USA IT shall configuration the virus protection application to regularly update its virus definitions from the software vendor. This process should be monitored by way of log files. The applications should be configured to send email alerts to the virus application administrator regarding the status of the virus definition update. In the case of an unsuccessful update the administrator should manually execute the virus definition update.
- Any time there is a change to the virus definition file these update should immediately be pushed to all managed computers.

Monitoring Update Logs

Logs created during virus updates to servers and workstations in the MorphoTrust USA network should be reviewed for completion status. Any failed updates should be immediately followed up on and updated virus definitions loaded to the failed component.

6. Use of Company Equipment

When MorphoTrust USA supplies an employee or contractor with software, hardware, information and/or other materials to perform MorphoTrust USA business, the title and all rights and interests to these items remains with MorphoTrust USA. In such instances, possession by an employee or contractor does not convey ownership or any implication of ownership. All such items must be promptly returned to MorphoTrust USA when an employee or contractor separates from the company, or when so requested by their manager. .Company-owned laptops and portable devices along with demo equipment may be removed from MorphoTrust USA facilities with the approval of Management. For company-owned desktops, workstations and servers, as well as any special equipment, written Management approval is required.

Hardware

In general, MorphoTrust USA computer and communication systems are intended to be used for business purposes only. Occasional use of this equipment for personal items must be limited and must not interfere with normal work productivity, business activity, consume company resources/bandwidth or violate any other company policies.

Inappropriate use of MorphoTrust USA computer systems includes the unauthorized use of test or network probing mechanisms for the detection of network or system vulnerabilities. The possession or the usage of these tools without the written approval of the CIO, CSO, or ISO is prohibited. Any use that conflicts with any Human Resources policies is considered inappropriate.

Software

Employees may not change the operating system configuration or install new software in such a way as to weaken the security of the system on any MorphoTrust USA-supplied computer hardware without the written approval of the Security Department. All installed software must be used in accordance to its license agreement and must be reviewed and approved by IT. Automatic updates of previously approved software are normally fine, but new products should always be approved by IT.

Installation of personally owned software is discouraged but allowed with the advance written permission of the employee's immediate Manager as well as the CIO or the Director of IT. A copy of the license must be kept with the system at all times to ensure compliance. Copying or "burning" of software in a manner that is not consistent with the vendor's license is strictly forbidden.

Email

All MorphoTrust USA emails are scanned prior to delivery into the local mailbox by a third-party, anti-virus/anti-spam hosted application. This automatic scanning does not apply to personal web mail from outside entities such as Hotmail or Yahoo. This practice helps defend against new virus attacks that do not yet have a definition created. If a user is unsure of whether or not an email attachment might be infected, they must contact the IT Support Team (and do not forward the email itself as this could cause a spreading of virus). Please reference the *MorphoTrust USA Electronic Communications Plan PLN-00090-A* for more details regarding the use of email.

Principles

- Use of the email system constitutes consent to abide by all elements of this policy.
- Employees must not open email attachments or click on links in emails unless they are from an expected and trusted source.
- Any electronic mail address or account assigned by MorphoTrust USA is the property of the company and under management control of the CIO.
- Email messages are the equivalent of letters sent on official letterhead, and must therefore be written in a professional and courteous tone. If an email signature is being utilized, it must adhere to the policies set forth by the MorphoTrust USA Marketing Department.
- MorphoTrust USA email is public communication and therefore, senders and receivers of email can have no expectation of privacy and are subject to company inspection and legal discovery.
- All emails between MorphoTrust USA employees and Safran/Morpho employees are automatically logged and stored by the server.
- Faxes between MorphoTrust USA employees and Safran/Morpho employees is prohibited.

Unacceptable Behavior

Using Company communications systems (including email) for any illegal, immoral, indecent, or objectionable purpose is unacceptable and grounds for dismissal. If you are in any doubt about the appropriate use of email please check with your manager. Likewise, the following uses of Company communications systems is unacceptable:

- To set up personal business, send chain letters, promote political causes or outside organizations, or any other non-job-related solicitations.
- Forwarding of company messages to external sources whether they are company confidential or not.
- External internet hosted services that do not offer any business value or pose an excessive risk. For example, some services are allowed (ex: LinkedIn) while others are not (ex: Facebook, Twitter, MySpace) during normal working hours.
- Accessing copyrighted information in a way that violates the copyright. Also, the sending or receiving of trade secrets, proprietary financial information, import/export information, personal identifiable information (PII) or similar materials without prior authorization.
- Breaking into the company's or another organizations email system or unauthorized use of a password/mailbox.
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.
- Transmitting unsolicited commercial or advertising material.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus or malware into the corporate network.

Note: The Company monitors all email, both inbound and outbound.

Note: All email between MorphoTrust USA employees and Safran/Morpho Affiliate employees is logged and must not include confidential information or content of state/federal/local contracts/software/databases or export control information.

7. Internet Use

The use of MorphoTrust USA Internet resources for personal purposes is permissible as long as the incremental cost of the usage is minimal, no MorphoTrust USA business activity is preempted by the personal use, and the usage does not cause a hostile working environment or set a poor behavioral example. Employees must not employ the Internet or other information systems in such a way that the productivity of other employees is eroded.

MorphoTrust USA is not responsible for the content that employees may encounter when they use the Internet. If an employee inadvertently connects to a web site containing objectionable content, they must promptly move to another site or terminate their session. These sites include but are not limited to, sites that contain sexually explicit, racist, sexist, violent or other potentially offensive material. Employees should not intentionally connect to web sites that contain offensive material (this includes through a VPN connection) while at work or at home or anywhere else using company equipment or systems.

The ability to connect with a specific web site does not in itself imply that employees of MorphoTrust USA are permitted to visit that site. MorphoTrust USA may, at its discretion, restrict or block access to web sites as well as block the downloading of certain file types that are likely to cause network service degradation. These types include graphic and music files.

Note: Internet access from production networks is either forbidden or heavily controlled, by design.

Note: Corporate network access is disabled for all employees on a Leave of Absence.

8. Privacy

Employees must have no expectation of privacy when using information systems at MorphoTrust USA. To manage and enforce security as well as other policies, MorphoTrust USA may log, review, and otherwise utilize information stored on or passed through its systems. This information includes but is not limited to user activity such as telephone numbers dialed and web sites visited.

9. Remote Access

The Company provides remote access for approved employees and contractors to resources on its Local Area Network. This access can be achieved via dial-up, DSL or high-speed Internet connections. The goal of this section is to outline how remote users can access the network data while still protecting that data.

Minimum Home Network Configuration

Personal network configurations used by employees who normally work from home must meet the following minimum standards:

- Your Company-issued computer comes with a built-in firewall that is preconfigured on your system and is set to block all inbound traffic from reaching your computer. This firewall must not be turned off at any time.
- Wireless home networks should use at least WPA (Wi-Fi Protected Access) security which requires a reasonably strong password of at least 8 characters with a mixture of letters, numbers and symbols. The use of MAC (Media Access Control) address filtering is strongly encouraged to limit the allowed wireless devices to those in your home.
- If you purchase your own home networking devices like routers or wireless access points, it is your responsibility to secure those devices. The default passwords that come with home networking devices must be changed and cannot be empty. Please see Section 3, *Passwords* for more information. The complexity of the passwords should follow these guidelines but they do not need to be changed periodically, unless there is suspicion that it might have been compromised or told to unauthorized persons, or if you host a publicly accessible service over the Internet.

Rules

- Remote employee access is automatically handled through the MorphoTrust USA VPN and is only allowed on company provided/authorized/configured equipment.
- No classified information shall be stored locally on these devices, and no Personal Identifiable Information (PII) may be stored on these devices, as described in the *Sensitive Data Handling and Storage Policy PRC-00148-A* and the *Security Governance Policy PRC-00173-A*, unless explicitly approved by the CSO or ISO
- All devices, both MorphoTrust USA provided and personal, must be kept up to date with security patches and utilize passwords or passcodes to access.
- While wired access (i.e., via your laptop) is the preferred method of access to email and other MorphoTrust USA systems, the use of mobile devices such as smart phones and iPads is allowed so long as they conform to the Company's *Cell Phone and Mobile Device Use Policy (PRC-00237-A)*.
- Use of mobile devices shall be subject to inspection by IT at IT's request.
- Cloud backup of mobile devices is not allowed. For example, iPhone data is not allowed to be stored or synchronized with Apple's iCloud service.
- It is each employee's responsibility to guard the means of access (laptop, accounts, passwords, etc.) to the Company's systems.
- Negligent actions on an employee's part that could breach PII by others are grounds for immediate dismissal.
- Make sure your laptop conforms to IT security practices. If you are unsure, please ask IT to check it.
- If your laptop was not built by IT, you are out of compliance. Report it immediately to IT.
- You should always use the secure VPN client issued by IT to remotely access the MorphoTrust USA network.
- If you get a warning or error while trying to connect to the VPN remotely, you should disconnect immediately because it is possible that an attack such as a man-in-the-middle attack could be active. This is true whether you are accessing over an unsecured network or accessing email via a web browser. Disconnect from the unsecured network immediately and refrain from using any network access at that point.

- When accessing your MorphoTrust email account remotely using a web browser, periodically check to make sure the connection uses “https” at all times. If the browser shows “http,” disconnect immediately because it is likely that a man-in-the-middle attack is active.
- If you don’t have a cable lock for your laptop for your office, contact the IT Help Desk who will provide one to you. Lock up your laptop when left in the office overnight, preferably using a laptop lock.
- Check your laptop for PII and remove any PII found. If available, use the whole disk encryption software to shred it. For example, with PGP Whole Disk Encryption, the PGP Desktop has a PGP Shred function to delete files securely.
- If your laptop or mobile device, regardless if it is either personal or corporate property, receives classified information, it must be sanitized according to the *Information Spills and Cleanup Policy, PRC-00312-A*.
- No VPN connections can be made from MorphoTrust equipment or from the MorphoTrust network into personal machines, or any other machines or devices that have not been approved for access either by the MorphoTrust IT Department or Security Department, or by MorphoTrust’s Customers.

Note: Accessing the MorphoTrust USA email system through any means other than browsing to Outlook Web Access via a personal mobile device grants IT the authority to wipe the device in the case of loss or theft.

DO’s and Don’ts

Don’ts

- Leave your laptop or mobile device unattended.
- Write down passwords, accounts, etc.
- Use unsecure public web access point. (No Starbucks, Panera, McDonald’s, Airports, Hotels Lobbies, etc.) These are public WiFi access points that do not require a password or passcode.
- Leave your laptop in open view in a vehicle.
- Store customer data on your laptop.
- Send customer PII via email.

Do’s:

- Use common sense and best practices when transporting your laptop. Always lock it in your car trunk and do not leave it unattended.
- When travelling obtain a loaner USB cellular modem from IT for secure wireless access. If one of these devices is unavailable, only use your laptop with a wire connection (from your hotel room, for example) rather than over a public, unsecured wireless network.
- Refer to section 10, International Travel, if you are travelling outside the country.
- Keep your laptop locked up when it is not in use.
- Access MorphoTrust production environments like the CSN and Customer environments only using a secure, dedicated VPN connection.

Remote Control Access

Remote control access is only allowed with MorphoTrust-named personnel. Exceptions to this rule can be granted for trusted third-party vendors (such as Cisco), under MorphoTrust USA IT supervision for diagnostic purposes.

10. International Travel

The following rules apply to MorphoTrust USA employees and contractors traveling outside of the United States or its territories, either for business or personal pleasure:

- You are not allowed to take any of the company's development software code or Subject Contract Information (which includes PII) out of the country.
- You are not allowed to take any export controlled information unless authorized for the destination and end-use by the Export Compliance Officer. Refer to the *MorphoTrust USA Technology Control Plan PLN-00088-A-06* for additional information on export controls.
- You are not allowed to VPN into the MorphoTrust network from outside of the country.
- You are allowed to use *https://mail.morphotrust.com/* for email only. As stated above, make sure the entire email session continues to use "***https***" and not "***http***." If, when you first try to connect to the mail server using this URL, you get a warning or error message regarding a certificate, disconnect immediately as a man-in-the-middle attack could be active.
- You may not take your company laptop out of the country. Instead, get a travel laptop on loan from IT by submitting a request via the Service Manager portal at *https://itsupport* and upon return to the office, return the travel laptop to IT for sterilization. If you need Microsoft Office installed on the travel laptop, let IT know. Do not transfer files from the loaner travel laptop to company networks or systems after you have returned from your trip. Any files that need to be retained should be emailed to yourself.
- You are allowed to take your company mobile phone on your trip. Notify IT at least a week before you leave so that international calling (roaming) can be enabled. Otherwise, you will not be able to make or receive phone calls while traveling. Also, if the phone supports wireless networking (WiFi), do not connect the phone to any wireless network while traveling.
- If a portable USB drive is necessary for backup purposes, make sure it is an encrypted drive with AES-256 encryption. This drive must not contain any Subject Contract Information or PII while traveling. When you return from your trip, do not connect this drive to any MorphoTrust equipment. All files will need to be securely deleted and the drive reformatted by IT first. Then the drive will be able to be reused. To preserve any files on the drive, use the travel laptop to email them to yourself first using *https://mail.morphotrust.com/.*
- No source code files can be taken outside the country on any kind of portable device.
- Do not connect your company devices to a Safran or Morpho affiliate network of any kind (wired or wireless) using any method.
- Be sure that you only connect to known valid WiFi or wired connections. Refer to Section 5 for more information. Do not use WiFi connections that are not secured, that is, they have no password or passcode, or they use WEP for security

11. Encryption

Whenever sensitive data (Customer information, customer data, company confidential, and company restricted data) is sent over a public computer network (Internet), encryption methods authorized by IT must be used to protect it. All laptops or portable data storage devices must utilize, at a minimum, whole disk encryption, to ensure that if the device is lost or stolen, no unauthorized access is possible.

The use of physical security measures such as safes, locking furniture, hard drive locks, CPU locks and locking office doors is recommended as a supplementary measure to protect sensitive data.

IT Change Management Procedure

Document Number: PRC-00085-B
Revision Level: 05

Approval

John May Chief Information Officer	Robert Eckel President

Table of Contents

1. Objectives

To define a policy and procedures that, when implemented, protects the integrity of IT's business and infrastructure systems and services and their underlying components. To ensure that changes to these services are recorded, assessed, and implemented in a controlled manner with mitigated risk for MorphoTrust USA.

2. Scope

This procedure applies to the IT Change and Configuration Management processes for all production business and infrastructure systems and services at all MorphoTrust sites globally. The procedures cover the process by which service additions, modifications, or removals are requested, evaluated, approved, and implemented.

3. Overview

IT Services may be comprised of one or more of the following components:

- Software (including database)
- Hardware (including environmental and electrical components)

All changes to services or systems' state must be recorded. These records must be maintained and archived until after annual audit review has been completed.

Beyond IT management review, business stakeholders who depend on these services and systems must also review and agree to all proposed changes prior to changes being implemented.

4. Roles

The head of Infrastructure Services, typically a director within IT, serves as the chairperson for the Change Control Board (CCB). The Chairperson is responsible for providing oversight for the Configuration Management process and assuring process adherence.

5. Types of Changes

There are four types of changes to IT Systems, as follows:

a. Routine/Standard
b. Normal
c. Major
d. Emergency

The following table details the Change types and their requirements:

Change	Description	Characteristics	Required
Standard	Work which is part of routine, recurring maintenance and/or support changes under applicable procedures.	Change that is well understood and does not alter baseline Business requirements/functionality of Service. ➢ Risk is well understood ➢ No impact on other Services ➢ May include repair ("break fix") activities classified as identical or equivalent changes (e.g. like-for-like swap)	Pre-approval by IT Manager/Director
Normal	Changes that are susceptible to some level of risk and that require assessment and approval	Changes or additions to configurable elements without significantly altering the business requirements. ➢ Little or no impact to the state of the computerized system or software ➢ Requires few resources and minimal time to complete ➢ Risk of change to Service is generally assessed as low	Approval IT Manager/Director or CIO Notification to Impacted Users
Major	Changes that have a high impact risk potential and that require assessment, approval and outages to existing services	Changes that considerably alter a system's requirements or that require a sizable number of resources and amount of time to implement ➢ Changes will alter system requirements and create	Approval by CCB, IT Manager/Director, CIO, and Business Sponsor or Executive

		substantial new functionality or capability ➢ Large number of resources and substantial amount of time required ➢ Substantial estimated cost to the organization, often large, capitalized projects	Notification to Impacted Users
Emergency	Unplanned changes requiring immediate action	Required to: ➢ Restore a Service Protect electronic records/data, product or IT hardware ➢ May also be required to meet an urgent business need such as modifications necessary to meet a regulatory requirement ➢ Protect electronic records/data, product or IT hardware ➢ May also be required to meet an urgent business need such as modifications necessary to meet a regulatory requirement, or to mitigate an urgent security issue such as a malware threat or a spill of sensitive information	Approval by IT Manager/Director or CIO Notification to Impacted Users

Note: Only Significant changes require user acceptance as defined in the Software Development Life Cycle (SDLC).

6. Further Change Requirements

The following rules also apply to Changes:

- Any new additions or changes to any system or device managed by the IT organization such as network, system hardware, storage, operating systems, databases, applications or telecommunications equipment and software, shall adhere to the change management policy and follow the change management procedures.
- Any changes to the power or environment affecting the data center must be communicated by facilities personnel to the Head of IT (CIO) or their representative. No changes may occur until the IT Infrastructure change management procedures are followed.
- All non-emergency changes to occur within the IT environment must be documented, discussed, and pre-approved by the CCB.
- The head of Infrastructure Services chairs the Change Control Board meeting and is accountable for management of the meeting. S/he acts as the "Enterprise Change Manager".
- Users who could possibly be affected by a system outage during maintenance shall be proactively notified whenever possible.
- The CCB serves in an advisory role. The final decision for approval of change resides with the Head of Infrastructure Services.
- All non-emergency changes must be submitted to the IT Change Control system in advance of review and follow the IT Change Control policy/procedure.
- Emergency Change Control Requests (CCRs) result from a major security breach, a significant outage impacting the business, or an outage impacting a significant number of employees (e.g. a site), and necessitate urgent action. Emergency CCRs require the approval of the CIO (or their designee) prior to implementation. The CCB subsequently reviews the emergency CCR at the next meeting to ensure documentation was completed, the CCR process was followed, and to identify any lessons learned that could prevent similar emergency CCRs in the future.
- Identification – Any employee identifying a need for a change can initiate a CCR.

7. Procedure for Non-Emergency Changes

- **Complete the Online Change Request Form -** The Initiator must complete all fields in the appropriate CCR form prior to submitting to their Manager or Lead for approval and CCB processing. The Manager or Lead must approve all CCRs before CCB review. Depending on the Change type, CCRs are approved as outlined in the Types of Changes chart above.
- **CCR Pre-Processing** – For each CCR submitted. The responsible Manager(s), Team Lead, and CCB Chair will review the request and approve, reject, or send for review as outlined in the Types of Changes chart above.
- **New Request Review** – all new requests will be reviewed weekly by end of day Wednesday for changes being made that next week. When a significant change is submitted, a CCB meeting is scheduled and chaired by the Director of Infrastructure Services.
- **Time Frame** - In order to allow adequate time for review, CCR's should be completed at least 2 days prior to the CCB.
- **Notification** - As a condition of CCB approval, all routine CCRs and scheduled maintenance windows, which require an outage, require notification to system users. An announcement of the change will be sent out from the IT Service Desk to the affected parties at least seven (7) days prior to the scheduled outage.
- **CCB Meeting** – When any change above a standard change is being scheduled, the IT Head of Infrastructure Services (or alternate) shall schedule and chair the CCB. The following personnel (or their delegates with authority/accountability to act on their behalf) are required to attend all CCB's:
    - The Chair
    - Director of Application Services
- Applications/Development/Network/Systems/Security/Help Desk Leads and the senior managers representing these departments.

- Initiators of all CCRs coming before a specific CCB meeting.
- Attendance of other IT personnel is optional. These meetings can be in person or by conference calls.
- The initiating Manager or Team Lead will approve the CCR for review by the CCB.
- Every meeting will begin with a recap of any due or past due open actions from the last meeting. The CCB will then act on all outstanding CCRs. After this review is complete, each Change initiator shall present a status summary for each newly submitted CCR. Concerns will be discussed prior to CCB vote. Mandatory attendance CCB members are allowed one vote: **Approve**, **Place on Hold**, or **Reject**. In cases where agreement cannot be reached, the Chair will decide the outcome. The board shall not be prevented from acting upon an item due to lack of attendance by members.
- **Dispositions** - There are three possible outcomes for any Change proposal:
  - **APPROVED**. In this case, it shall be noted in the CCR Comments Field and action will be assigned to update the baseline and a target implementation time defined.
  - **ON HOLD**. The change will be held until pending the completion of action items.
  - **REJECTED WITH COMMENTS**. Comments are always required when a Change is being recommended for disapproval. In this case, the minutes shall clearly state **REJECTED**, and appended with the date and initials.

8. Procedure for Emergency Changes

- For changes that are deemed to be an emergency, the change must be approved by at least a director/appointee of IT or the CIO.
- **Emergency Notification** – In an emergency, the impacted systems should be brought back online as soon as possible. Notification is made immediately to the IT Directors, CIO and impacted users.
- **End of Emergency Notification** – When the emergency is over, notification is made immediately to the IT Directors, CIO, and the impacted users that the emergency is over.

  Once the emergency is over, the person involved in the emergency completes the Change Request Form - The Initiator must complete all fields in the appropriate CCR form prior to submitting to their Manager or Lead for approval and CCB processing. The Manager or Lead must approve all CCRs before CCB review. Depending on the Change type, CCRs are approved as outlined in the Types of Changes chart above.

- **CCR Pre-Processing** – For each CCR submitted. The responsible Manager(s), Team Lead, and CCB Chair will review the request and approve, reject, or send for review in the next CCB meeting.
- **Emergency Request Review** – all new emergency requests will be reviewed weekly.
- **Time Frame** – All emergency CCRs must be completed within 2 days of the emergency.
- **Procedure Violations** – Failure to follow this process can potentially impact customer satisfaction and puts MorphoTrust at risk. As such, all process violations, which include any implementation of a change prior to CCB approval, will be reported to the Director of IT and the CIO. At their discretion, consequences may include formal disciplinary action up to and including termination of employment.

9. Definitions

TERM	DEFINITION
Business Services	An IT Service that directly supports a Business Process, as opposed to an Infrastructure Service which is used internally by the IT Service Provider and is not usually visible to the Business.
CCB	See Change Control Board
Change	The addition, modification or removal of anything that could have an effect on IT services. The Scope should include all IT Services and underlying Configuration items.
Change Control Board	The Change Control Board is a group of Information Systems, Quality, and Business area representatives and, in certain cases, external Service providers that have expertise or an otherwise vested interest in the change request under consideration.
Change Control Request (CCR) Form	The form that identifies and initiates the Change process, filled out by the Initiator.
Change Management	The process by which service additions, modifications, or removals are requested, evaluated, approved, implemented, and reviewed. The change may be to the service itself or any supporting service or component of the service.
Change Type	A repeatable way of dealing with a particular Category of Change. A Change Type defines pre-defined steps that will be followed for a Change of this Category. Change Types may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require management approval (e.g. major software Release).
Configuration	A generic term, used to describe a group of Configuration Items (CI) that work together to deliver an IT Service, or a recognizable part of an IT Service. Configuration is also used to describe the parameter settings for one or more CIs.
Configuration Manager	Role responsible for providing oversight for the Configuration management process. Assures process adherence, efficiency and effectiveness.
Configuration Management Database (CMDB)	A database used to store Configuration Records throughout their Lifecycle. The CMDB stores Attributes of CI and Relationships with other CIs.
Enterprise Change Manager (ECM)	The role responsible for oversight across all regional change managers and acts on and chairs the CCB for all changes that have multi-site impact. The Enterprise Change Manager governs the IT Change & Configuration Management program.
Infrastructure Service	An IT Service that is not directly used by the Business, but is required by the IT Service Provider so they can provide Business Services. For example Directory Services, naming services, or communication services.
Major Change	Any Change above a Standard Request that has a higher risk of impact and affects a number of users that must be notified.

REMOVABLE MEDIA POLICY

Document Number: PRC-00150-A

Revision Level: 01

Approval

Dennis Kallelis Chief Security Officer	Robert Eckel President

Users are responsible for making sure that they have the current revision of this document.

TABLE OF CONTENTS

1 Introduction

This policy outlines the steps to be taken to ensure control over the removal of sensitive media and data from secure facilities by way of removable recording media, including but not limited to:

- Disks
- Cassettes
- Hard drives
- CDs
- Flash drives

2 Policy

All removable media on workstations within the Central Production facility will be disabled, except for those employees who prepare

- Backups
- Software upgrades
- Copy security logs for audit review

Such personnel responsible for the above are restricted to:

- Managers or their approved designees
- Card System Engineers
- Manufacturing Engineers
- Backup and update IT staff

The Chief Security Officer must approve the management personnel with the above permissions.

Proper security will be maintained on all backup and update media. Refer to the MorphoTrust USA IT Backup and Recovery Policy for more information.

3 Updating Production Systems

Production equipment must be periodically maintained, updated, and tested as necessary. These functions can be performed by the personnel identified above, so long as they have prior approval of the CSO.

Data used in these processes, while not sensitive in and of itself, is installed on sensitive and secure production systems and equipment. Data can be loaded from removable media by the approved managers/engineers, so long as the media meet the following requirements:

- Be approved by the CIO
- Employ, at a minimum, whole disk encryption
- Remain in the possession of the manager/engineer at all times
- Never be used for any other purpose on any other machine or system
- At no time is any PII to be placed on to the removable media