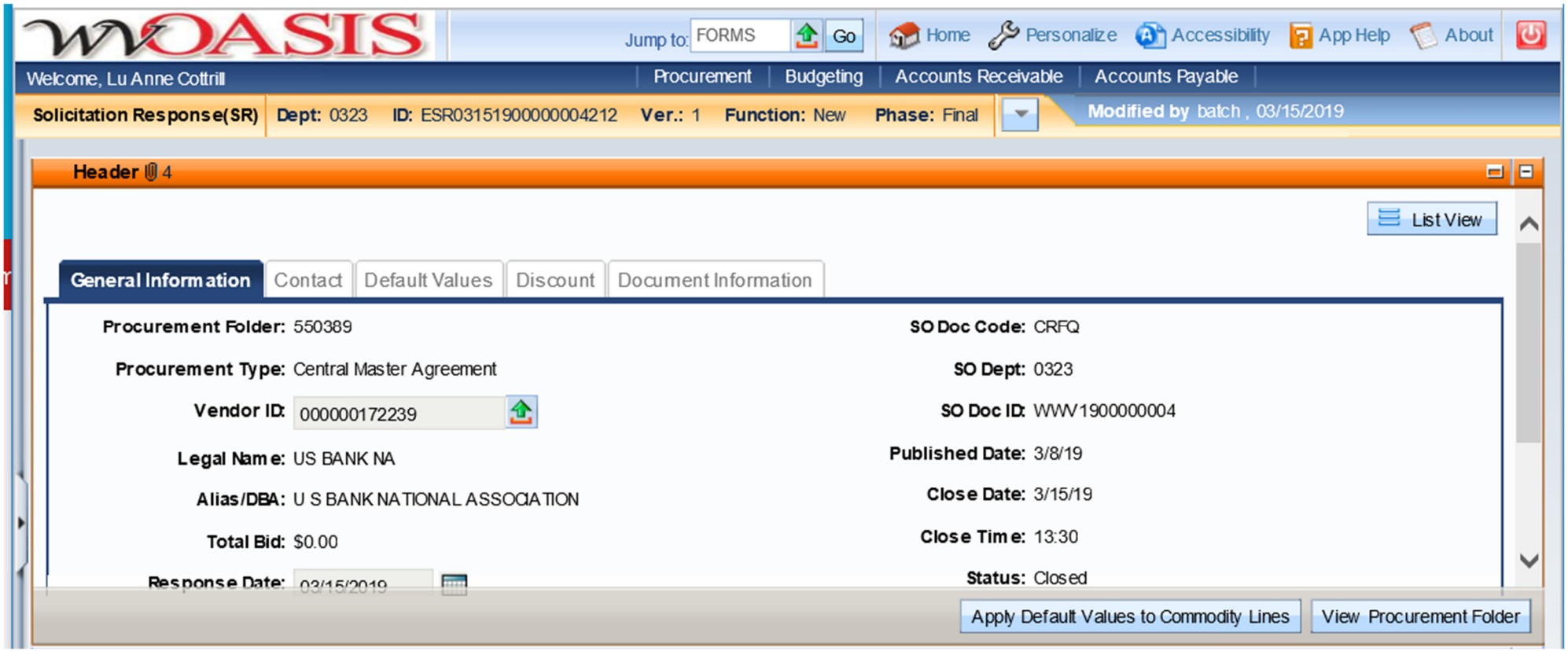
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency 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.


WVOASIS
Jump to: FORMS Go
Home
Personalize
Accessibility
App Help
About
Welcome, Lu Anne Cottrill
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR)
Dept: 0323
ID: ESR03151900000004212
Ver.: 1
Function: New
Phase: Final
Modified by batch , 03/15/2019
Header 4
List View
General Information
Contact
Default Values
Discount
Document Information
Procurement Folder: 550389
Procurement Type: Central Master Agreement
Vendor ID: 000000172239
Legal Name: US BANK NA
Alias/DBA: U S BANK NATIONAL ASSOCIATION
Total Bid: $0.00
Response Date: 03/15/2019
SO Doc Code: CRFQ
SO Dept: 0323
SO Doc ID: WWV1900000004
Published Date: 3/8/19
Close Date: 3/15/19
Close Time: 13:30
Status: Closed
Apply Default Values to Commodity Lines
View Procurement Folder

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

State of West Virginia
Solicitation Response

Proc Folder : 550389

Solicitation Description : Addendum 2 - Banking services

Proc Type : Central Master Agreement

Date issued	Solicitation Closes	Solicitation Response	Version
	2019-03-15 13:30:00	SR 0323 ESR03151900000004212	1

VENDOR

000000172239

US BANK NA

U S BANK NATIONAL ASSOCIATION

Solicitation Number: CRFQ 0323 WWV1900000004

Total Bid : $0.00 **Response Date:** 2019-03-15 **Response Time:** 08:16:45

Comments: See attachments.

FOR INFORMATION CONTACT THE BUYER

Michelle L Childers

(304) 558-2063
michelle.l.childers@wv.gov

Signature on File **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	Banking Services				$0.00

Comm Code	Manufacturer	Specification	Model #
84121500			

Extended Description : Vendor MUST complete the ATTACHED Pricing Page, Exhibit A. If bidding electronically, vendor is to put $0.00 on the commodity line in WVOasis, complete the Excel pricing page, and upload into WVOasis as an attachment. Only pricing submitted via Exhibit A pricing page will be evaluated for award.

Comments: ECR @ 1.25% with Balances offset service charges.

Banking Services Proposal
Presented to

WorkForce West Virginia

March 15, 2019

Tim Rieder
Senior Vice President
Relationship Manager
614.232.2081
tim.rieder@usbank.com

David Sullender
Vice President
Treasury Management Consultant
937.640.7610
david.sullender@usbank.com

March 15, 2019

Michelle Childers
Senior Buyer
WorkForce West Virginia
1900 Kanawha Boulevard, East
Building 3, 3rd Floor, Suite 300
Charleston, West Virginia 25305

Dear Michelle,

On behalf of U.S. Bank, thank you for the opportunity to respond to your request for proposals (RFP). We value our strong relationship with The State of West Virginia, which began in 2015. We currently provide ACH processing and Corporate Payment Systems (Pcard Program, and we are looking to expand our partnership with a long-term, strategic approach focused on achieving your financial goals.

As your dedicated Relationship team, we're committed to your success. We collaborate to uncover any challenges and bring proactive ideas and strategies to help you grow and prosper. For enhancements, we'll work with you from the solutions design phase, throughout implementation and into the future.

You receive ongoing support from your designated Commercial Customer Service (CCS) team in Cincinnati Ohio. Your CCS bankers are familiar with your program and needs. They offer a premier level of service, including timely, thorough and responsive measures to ensure your satisfaction.

U.S. Bank will always choose to do what's best for WFWV. We believe in doing the right thing every day. Our strong ethical business practices earned us the honor of being named one of the 2019 World's Most Ethical Companies® by the Ethisphere Institute for the fifth consecutive year.

We have an attractive offer that includes waiving the first three months of service fees, competitive state pricing and ECR of 1.25%.

Our proposal offers you the security of knowing you partner with one of the strongest-performing banks in the nation. This security is combined with state-of-the-art technology, future-focused innovation and a personalized Relationship team. The pricing we offer is intended to be competitive and reflects our serious interest in growing and strengthening our partnership.

Sincerely,

Tim Rieder
Senior Vice President
Relationship Manager

David Sullender
Vice President
Treasury Management Consultant

Table of Contents

Exhibits

1. Cover Page
2. Designated Contact
3. Addendum Acknowledgement
4. Disclosure of Interested Parties
5. Purchasing Affidavit
6. Exhibit A - Pricing Page
7. Sample Account Analysis
8. National Premier Availability Schedule
9. FDIC Certificate
10. Insurance Certificate 1
11. Insurance Certificate 2
12. Master Services Agreement with Appendix A&B
13. USB Services Terms and Conditions
14. Your Deposit Agreement

Electronic Only Exhibits

The Document below contains certain nonpublic information deemed proprietary and confidential, so it was emailed directly to WFWV and it not included in print.

15. Security Posture

Executive Summary

As WFWV's current financial partner, U.S. Bank is well-positioned to meet all your banking needs. This RFP process provides the opportunity to outline the current services we provide and present long-term recommendations for enhanced efficiencies. Our recommendations are based on our extensive collaboration. We continually work to understand your requirements, limitations, goals and capabilities.

Government banking expertise

For more than 150 years, U.S. Bank has provided financial services to government entities. Our extensive work in partnership with organizations of all shapes and sizes gives us a unique perspective in meeting the public sector's needs.

Our Government Banking division provides banking services, treasury management solutions, card products or corporate trust services to all 50 states. We provide primary banking services for Idaho, Kansas, Maine, Minnesota, Montana, Nebraska, Oregon Utah, Washington and Wisconsin. Other significant banking relationships include the states of Alaska, Arkansas, California, Colorado, Connecticut, Indiana, Iowa, Kentucky, Maine, Michigan, Missouri, Nevada, Ohio, Pennsylvania, South Dakota, Tennessee and Texas.

We offer a wide range of deposit, treasury management, trust, investment and payment processing products to meet the needs of state, cities, counties, towns, school districts and other governmental or public organizations. We also provide government-specific interim financing for construction products, equipment financing, temporary cash flow financing, term financing, pooled financing programs and registered warrants.

Your relationship manager, Tim Rieder, advocates for you in the marketplace, working to understand how new technologies create better functionality and provide you an economic advantage. You can expect timely responses to operational, pricing and technical questions, as well as other general inquiries, on a day-to-day basis. Your Relationship team also includes product specialists, debt finance bankers and a CCS group – a team of highly-skilled and experienced representatives ready to process both your routine and complex service requests with efficiency and accuracy.

Improved payment efficiencies

As part of our commitment to process improvements and payment efficiencies, U.S. Bank presents our Working Capital Consultation. This free-of-charge, on-site session with you allows us to understand more about your process flow, from procurement to payment. Our experts listen and advise based on your unique business model for maximum productivity, flexibility and control. We recommend solutions based on optimizing the entire, tiered payables process. Partnering across all payment types in a Working Capital Consultation can be among the most transformative exercises your payables process can undergo.

Proactive risk mitigation

Proactive risk mitigation is one of our primary focuses, including employment of fraud prevention measures, increased data security and enhanced disaster readiness, which ensures continuity of service. As your banking partner, we have the highest financial stability, strong technical and industry knowledge, and the ability to help guide you through industry and technology changes.

Superior customer service

Our CCS group supports a wide variety of government clients, providing prompt depository and treasury management support. Highly skilled and extensively trained, your service staff responds to both routine and complex inquiries through online access to our systems and product databases.

The U.S. Bank difference

Our commitment to government banking expertise, improved payment efficiencies, proactive risk mitigation and superior customer service creates the foundation for our future growth. These principles set us apart and solidify U.S. Bank as the most trusted choice in the banking industry. We are confident you will find our focus on your long-term success unmatched and look forward to a strong partnership.

3. GENERAL REQUIREMENTS:

3.1 Contract Items and Mandatory Requirements: Vendor shall provide Agency with the Contract Items listed below on an open-end and continuing basis. Contract Items must meet or exceed the mandatory requirements as shown below.

3.1.1. The financial institution must provide WFWV with the following benefit accounts.

3.1.1.1 Unemployment Compensation Payment Account to be used to pay Unemployment Benefits to claimants.

3.1.1.2 Trade Readjustment Account used to pay claimants that are affected by Foreign Competition.

3.1.1.3 Disaster Unemployment Act account used to pay claimants that are unemployed due to a type of disaster (i.e. Business was flooded).

3.1.1.4 Special Account used to pay for court costs for appeals and other costs not associated with benefit payments. Funding for this account comes from a transfer from the Unemployment Compensation Clearing Account A.

3.1.1.5 Trade Adjustment Assistance Act account to pay participants registered in the training program.

3.1.1.6 Alternate Trade Adjustment Assistance account to pay participants registered in the Trade Adjustment Assistance Program that are over the age of 55.

U.S. Bank can meet the mandatory requirements and contract terms as outlined.

3.1.2 The financial institution must provide WFWV with the following services for the benefits accounts shown in 3.11.

3.1.2.1 The financial institution must provide WFWV with online access to all accounts. WFWV must have the ability to view account balances and account activity, transfer funds between accounts, issue stop payments, and receive ACH payments.

SinglePoint® enables WFWV to achieve new levels of efficiency by bringing our powerful banking services together into one easy-to-use website with a single point of access for all of your global treasury management service needs. A fully integrated, wholly-owned online suite of treasury management services, SinglePoint does not require dedicated PCs or software installation.

With SinglePoint, you can monitor account activity; view, manipulate and download images; transfer and manage payments, including disbursements via Zelle; process and deposit collections; prevent fraud; and manage your employees' system use. The following services are available within SinglePoint and are accessible with the same user login ID and password.

Monitor Account Activity

- Account reconciliation
- Adjustments
- Cash forecasting
- Image access
- Information reporting
- Lockbox wholesale
- Returned item decisioning
- Reports file delivery
- Account services
- Asset-based loan information reporting
- General ledger reconciliation
- Image file delivery
- Lockbox image look
- Mobile SinglePoint
- U.S. Bank VantagePoint™

Transfer and Manage Money

- ACH adjustments
- ACH origination
- Cash vault
- Electronic cash letter deposit
- On-Site Electronic Deposit
- Wire transfer
- Disbursements via Zelle
- ACH additional services
- Book transfer
- Check payables
- Investments
- Trust transfer
- Real-Time Payments

Act Globally

- Foreign Exchange Web (FX Web)
- International ACH
- International remittance calculator
- International wire transfer
- Global trade
- International information reporting
- International request for transfer

Prevent Fraud

- ACH positive pay
- IP whitelist service
- Reverse positive pay
- IBM® Security Trusteer Rapport™
- Issue maintenance
- Positive pay (previous day, same day, payee)
- Stop payments

Control Access and Stay Informed

- Customer service
- External messaging
- Personal settings
- System administration
- Dashboard
- LaunchPoint
- Service guide

You initiate ACH, account transfer and wire transfer services from separate pages in SinglePoint. Our systems are integrated, so each transaction type requires only the information unique to that type of transaction. The remaining fields are checked and populated from a common data source.

Reports and transmissions can be scheduled through SinglePoint at any time throughout the day. Reports are delivered via transmission or secure email at the specified time. Fax and email reporting allows users to receive current and/or prior day reporting at a preset time without logging in. Certain time-critical functions, such as Positive Pay approvals and Positive Pay decisions, can also be accessed via a web-enabled mobile device through Mobile SinglePoint.

U.S. Bank Mobile SinglePoint

Mobile SinglePoint is a version of SinglePoint designed specifically if you're always on the go and need access to cash management tools when you're away from a computer. You can view key balance information on both domestic and international accounts from a mobile device. You can also view current day reports, such as ACH Summary and Detail, Wire Detail and/or Lockbox Summary.

SinglePoint External Messaging

Alerts and notifications through SinglePoint External Messaging enhance process efficiencies by utilizing over 200 unique messages that can be configured and routed to various destinations, including email addresses and SMS messages to mobile devices, ensuring key items receive attention. External Messaging is available for one low monthly fee. You can set up as many users and accounts as you like, and each user can set up as many alerts and notifications as they wish.

SinglePoint Information Reporting

SinglePoint Information Reporting enables WFWV to manage your financial position with superior reporting tools. SinglePoint Information Reporting displays account summary, detail and transaction information for accounts and transactions online. Benefits can include:

- **Simplify daily account reconcilement**—You can view current and previous day transaction and balance summary totals, including interim collected balance and Controlled Disbursement totals. Drilling down to account details for an individual transaction is easily accomplished. Users can view images of paid checks, returned checks and deposited returned items. You can also review incoming wire detail and return wires online.
- **Transfer funds easily from your account summary view**—If you use SinglePoint Book Transfers, you can view your previous day or current day account summary and take action within Information Reporting to immediately transfer funds between accounts.
- **Search for transactions**—SinglePoint allows you to search by account, transaction type, date range, amount and transaction reference (such as check number). Users can view, sort and print search results in PDF or comma separated value (CSV) formats and drill down to transaction detail within the application. Search also allows for wire returns.
- **View standard and special reports in various formats**—Standard reports include five previous day and 10 current day reports, including the highly useful ACH and Wire Detail reports. With SinglePoint you can quickly select report dates with the clickable calendar tool. Report formats include browser, PDF and text for human readable reports and BAI2 and CSV to integrate with internal systems.
- **Customize reports with robust filtering**—Users employ the report builder to select accounts, date ranges and data fields like transaction types, as well as save and name personal report filters, then reuse and share with other users.
- **Manage delivery of reports via email or transmission**—You can set up delivery schedules of previous, current day and custom reports on your accounts to be delivered to an email address or transmission mailbox.
- **Decision your current day returned items**—Your employees can easily review returned items, view images and decide to charge back or redeposit eligible items or request a reversal, and view their decision history.

Data Retention

Previous day data is retained for 60 calendar days and current day data is retained for 10 calendar days. Additional retention periods of 90 days, six months, 12 months, 18 months and 24 months are available for an additional account-level charge.

System Administration

Your designated SinglePoint system administrator serves as your security manager. The system administrator:

- Creates and deletes SinglePoint users
- Requests and maintains tokens, required to initiate payment transactions
- Sets and modifies user payment and transaction quantity limits
- Assigns user access to services and accounts
- Assigns initiation and approval entitlements
- Resets own and other users' passwords when necessary (regular users can change their own passwords)

We offer a dual system administration option upon set-up for added control. With this option, all changes to user access or limits require a second system administrator approval to process.

You can determine which accounts, services, functionality and limits each user sees and uses. Administrators can add, copy and reuse user profiles to streamline the set-up of new users. They can also modify user entitlements, account access and transaction limits at any time with immediate updates. The system allows you to change user status for interim periods, as well as assign entitlements by service area, function and account access. You can also set user payment limits for ACH, book transfers and wire transfers.

To assist you in monitoring system usage, we also offer the following audit features:

- User activity audit reporting for all services
- Token maintenance and status reports
- User profile reports
- Account profile reports
- Service profile reports

Security

SinglePoint protects account information with the most current and proven technology available, including:

- Two-way 128-bit encryption
- SSLv3
- Individual client IDs, passwords and digital signatures
- VeriSign time based tokens are required for users to access payment services (ACH and wire transfer). Tokens are pre-programmed to produce a new numerical code every 60 seconds. One token is assigned to each user at your site.
- By default, all entitlements must be approved by a second system administrator. You must complete additional paperwork to waive the dual approval requirement.

An optional IP white listing security feature is available if you want to restrict user access to allow only specific IP addresses or IP address ranges.

No organization is immune to criminal activity. Find four steps you can take to reduce the risk of payments fraud on Financial IQ. bit.ly/StopPaymentsFraud

The application also uses a tool called Passive Monitoring, which detects anomalies in web traffic between user PCs and our application. These anomalies include user PC viruses. Once detected, we contact users to communicate viruses were identified and advise on corrective measures to clean the user PCs.

3.1.2.2 WFWV will send a report electronically by 8 PM EST Monday through Friday containing all checks written against the account on a daily basis. On a daily basis, the financial institution must provide WFWV a report listing, if any, exceptions of checks that do not match the electronic file. The report should be submitted to WFWV by 11AM EST on a daily basis. WFWV will respond to any exceptions by 12 PM EST, or within one hour of receipt of the exception report, the "default" will be to honor those exceptions. However, WFWV reserves the right to change the "default" at any time. The financial institution must pay all benefit checks written on WFWV's accounts when presented for payment unless there are exceptions that are deemed to be invalid after investigation.

With ACH positive pay, each day WFWV is able to review a list of these non-matching transactions and decision them. LaunchPoint or External Messages can alert you of exceptions requiring decisions — WFWV can either pay the item, allowing it to post or return exception items back to their originator. As a default, SinglePoint will also Return All exception items that have not been decisioned by 7 p.m. CT on their effective settlement date. This means exception items will be returned unless WFWV instructs U.S. Bank, through SinglePoint, to handle an exception item differently. WFWV can introduce additional security to your ACH positive pay processing by using ACH Positive Pay Dual Authorization. With dual authorization, approvals can be required for all exception and authorization actions or only for actions related to items over a customer-specified dollar threshold, called the zero-approval amount.

3.1.2.3 The financial institution must on a monthly basis provide separate electronic transmittals of the monthly check reconciliation data for each account specified m the transmittal. Content must be provided to the financial institution by WFWV prior to delivery. The checks shall be listed ingroups of me hundred items with the subtotals as well as a grand total at the end of the listing. Also, the financial institution must provide online access of the imaged copies of all checks cleared or via CD Rom if online access is not available. All items required by this paragraph must be provided by no later than the ninth calendar day of the following month said checks are paid. The Management. Information Systems (MIS) Division reserves the right to accept or reject electronic transmittals provided the financial institution. Transmittals rejected will be returned to the financial institution with problems identified and the financial institution will have five (5) calendar days to provide a corrected file.

U.S. Bank Account Reconciliation delivers WFWV prompt and accurate computer-generated reports on paid and outstanding checks. Our services reduce your clerical work, help reduce fraud and give you more time. Our services are designed to fit with your computerized accounting system and provide you flexible reporting options for a wide variety of accounting cycles. We provide your information via hard copy report, data transmission or online through SinglePoint Account Reconciliation.

We offer full ARP and full positive pay services. While this set of services is optional, we strongly recommend you take advantage of the positive pay service as a component of your overall ARP package. Positive pay is the best and most affordable protection against fraudulent check activity. If you choose not to use

positive pay, you are responsible for and more susceptible to, fraudulent activity within your accounts.

U.S. Bank Full Account Reconciliation

U.S. Bank Full Account Reconciliation provides a set of comprehensive reports listing all outstanding and paid checks, along with all other check activity. With full reconciliation, you simply forward us the register information on all checks issued, along with a list of deleted or cancelled items. Your issue information is compared to your account activity to produce the reports. Since we automatically adjust and correct misencoded items, this service virtually balances your checking account for you. Flexible cutoff times allow you to customize the statement period. Below is a listing of reconciliation information availability following statement cutoff:

- **Bank statements**—Eight business days through U. S. Mail. Two business days through SinglePoint.
- **Canceled checks**—10 business days (checks).
- **CD-ROM**—Five business days.
- **Reconciliation information**—Eight business days through U. S. Mail. Due to automated balancing, 99 percent of reconciliation reports are available on SinglePoint by the second business day.

3.1.2.4 The financial institution is not required to sort in numeric order and deliver to WFWV all checks paid on each account. Checks, instead, will be destroyed after 45 calendar days.

U.S. Bank retains physical checks on-site for three days. Checks are then destroyed, with images stored off-site for seven years.

3.1.2.5 The number of items processed will be furnished to WFWV by the financial institution on the at 12 C.F.R. § 204.4] and furnished to WFWV and will be subject to verifications by WFWV. The earnings rate will be calculated by the institution and will be subject to verification by WFWV.

WFWV's bank statements is available online two business days after month end. Account analysis statements are available online through SinglePoint by the seventh business day of the month (eighth business day by mail). The fees are due by the 10th business day of the month.

The FDIC pass through charges has been replaced with the Deposit Coverage Fee. The Deposit Coverage Fee is charged monthly and is calculated using the average monthly ledger balance (per $1,000). WFWV's Deposit Coverage fee is $0.05 per $1,000 and your Earning Credit Rate is 1.25%. Please see the **Exhibit** section for **Exhibit A – Pricing Page**.

3.1.2.6 Each month, the financial institution must provide the information necessary for WFWV to complete the United States Department of Labor Form ETA 8413, for the Benefit Payment Account attached hereto as "Attachment A" and will compare the compensable service charges (Expense Analysis) with the institution's total interest earnings (Income Analysis). The financial institution agrees to supply the required information by no later than the 15th calendar day of the subsequent month. In the event the 15th calendar day of the month falls on a weekend; the financial institution agrees to supply this analysis on the preceding Friday. On the form ETA 8413, the financial institution will provide FDIC

cost for Line 16 Other Costs. Lines 17 and 18 may include service fees. The FDIC cost must be listed separately on the invoice. The only service charges allowable in any resulting contract shall be the charges quoted in the attached Pricing Page, (Exhibit A).

U.S. Bank understand and can provide Attachment A on or before the 15th of the month. However, this is a manual process. The same information is provided both online and in paper form from our account analysis statement. This is a preferable reporting method due to automation lacking human intervention that could cause manual reporting errors. Please see the **Exhibit** section for a **Sample Account Analysis.**

3.1.2.7 The financial institution must allow WFWV the right to open up to four (4) additional accounts in the event that the Department of Labor would start a new program that necessitates segregating funds in separate outside accounts.

Additional accounts for WFWV can easily be opened and services added as desired.

3.1.2 The financial institution must provide WFWV with the following clearing accounts.

3.1.3.1 Clearing Account A – Funds flowing from this account will be the employer contributions to the unemployment compensation system and checks will be written for employer refunds.

U.S. Bank understands your request for WFWV's Account A and will open a non-interest-bearing account for employer contributions to flow through.

3.1.3.2 Clearing Account B – This special clearing account will be established for the same-day processing of federal monies. No checks will be written on this account.

U.S. Bank understands your request for WFWV's Account B and will open a non-interest-bearing account for federal monies to be process through.

3.1.4 The financial institution must provide WFWV with the following services for the clearing accounts listed in 3.1.3.

3.1.4.1 The financial institution must provide daily armored/car/courier services for transporting of all deposits from Workforce West Virginia located at 1900 Kanawha Blvd., East, Building 3, 4th Floor, Charleston, WV by 3:00 PM EST to their location.

WFWV will contract directly with the vendor for your armored car services.

3.1.4.2 The financial institution will credit WFWV for all deposits on the financial institution's ledger on the same day that the deposit is delivered.

We will deposit your funds on the same day received for ACH, Wire and On-US items. Please see the **Exhibit** section for our **National Premier Availability Schedule.**

3.1.4.3 The financial institution, by 10:30 AM, EST on the day following the deposit pick-up, will; (1) process the deposit checks through the proof WFWV and sort such deposit checks by zero-, one-, and two-day clearing times; and

(2) provide WFWV with the collected balance, upon request. The financial institution will send an email each morning to WFWV of the total cash balance on hand to the Assistant Director of FAM, Accounting Section and his designee(s) for all benefit and clearing accounts. WFWV will be responsible for determining the amount of transfer to the trust funds from the Clearing Account A. Said transfer will be made in increments of one hundred dollars.

As promulgated by State Code, 21 A-8-S which states Clearing Account: upon the receipt of payments and ether moneys payable into clearing account fund under this chapter, shall immediately be deposited in the clearing account.
http://www.legis.state.wv.us/wvcode/Code.cfm?chap=21a&art=8#08

When the armored car arrives at one of our highly secured cash vaults, your deposits are entered into our automated vault system, assigned a unique reference/trace number, verified and deposited directly into your checking account. Deposits received by the specified cutoff time are credited the same day. If a discrepancy exists in a deposit, we adjust your account and provide prompt notification regarding the discrepancy. The system tracks each cash deposit from receipt to verification, allowing us to monitor the status of each deposit.

Our sophisticated tracking system creates an audit trail, which aids in customer service follow-up, quality control and error tracking. Our vault systems have built-in counterfeit detection and each processing station has camera surveillance. Cash delivery addresses are programmed into the automated vault system to avoid fraud.

Using a unique password, you can order coin, currency and supplies at any of our cash vaults through our Audio Response Unit (ARU) available 24/7. SinglePoint Cash Vault gives you the alternative of automation and convenience. You can place cash and supply orders online and monitor each location's ordering history.

WFWV will use our cash vault in Charleston with the cutoff time of 3 p.m. ET.

3.1.4.4 The financial institution will debit or credit to the account any insufficient funds checks and deposit errors and will return items with associated debit and credit slip to WFWV by messenger by 3:00 PM EST each day.

U.S. Bank understands and agrees to follow these instructions for insufficient funds and deposit errors. This information will be available in SinglePoint for your review by 8 a.m. ET.

3.1.4.5 The financial institution must receive and accept ACH Credit electronic payments from employers and Third-Party Administrators (TPAs) for employer contributions and deposit the funds into the Clearing Account A. The financial institution must accept addendum records in NACHA CCD+ format from the TPAs, balance settlement totals daily against deposits posted to the account per NACHA Operating Rules, and provide the information embedded in the addendum records to WFWV, electronically, via a secure FTP site. Information such as employer, employer ID number, amount of payment and quarter/year the payment applies to, etc. The financial institution may be required to adjust procedures to conform to technical requirements. The financial institution must identify the TPA and deposit amount on the daily e-mail to WFWV.

Yes, SinglePoint can display remittance information associated with received ACH or Financial EDI transactions. WFWV can access the following reports from the special reports menu to view remittance information detail:

- ACH Transaction Capture
- ACH Received Item
- EDI Remittance
- ACH Addenda Reporting (BAI)
- ACH Healthcare Remittance

Each report summarizes remittance information and provides enough detail to update internal accounts receivable systems.

We can also transmit a NACHA formatted file of received ACH transactions, which includes addenda.

U.S. Bank will meet this requirement providing all the information required by WFWV is included in the addenda records. Additionally, WFWV must provide file specifications for the electronic transmission to secure FTP site.

3.1.4.6 The financial institution must provide WFWV with online access to all clearing accounts. WFWV must have the ability to view account balances, daily deposits, and account activity, to transfer funds between accounts, and receive ACH payments.

Absolutely, SinglePoint provides browser-based access to account information. All of this information is available to WFWV in SinglePoint. Certain time-critical functions can be accessed via web-enabled mobile devices through Mobile SinglePoint, as well as mobile device specific apps.

3.1.4.7 The number of items processed will be furnished to WFWV by the financial institution on the monthly account analysis and will be subject to verification by WFWV. The earnings rate will be determined by the institution.

U.S. Bank understands and agrees. SinglePoint offers your account analysis statements online as part of the Special Reports module. Statements are available on the seventh business day each month and, like our paper statements, contain 12 months of history summarizing balances, earnings credit and net service charges. WFWV will get and ECR of 1.25%.

3.1.4.8 Each month, the financial institution must provide the information necessary for WFWV to complete the United States Department of Labor Form ETA 8414, for the Clearing Account A, attached hereto as "Attachment B", and will compare the compensable service charges (Expense Analysis) with the institution's total interest earnings (Income Analysis). The financial institution agrees to supply the required information by no later than the 15th calendar day of the subsequent month. In the event the 15th calendar day of the month falls on a weekend; the financial institution agrees to supply this analysis on the preceding Friday. On the form ETA 8414 the financial institution will provide FDIC cost for Line 16 Other Costs. Lines 17 and 18 may include service fees and

CCD+ addendum file fees associated with accepting deposits from a TPA. The FDIC cost and fees associated with TPA payments must be listed separately on the invoice. The only service charges allowable shall be the charge quoted in the attached Pricing Page (Exhibit A).

U.S. Bank understand and can provide Attachment A on or before the 15th of the month. However, this is a manual process. The same information is provided both online and in paper form from our account analysis statement. This is a preferable reporting method due to automation lacking human intervention that could cause manual reporting errors. Please see the **Exhibit** section for a **Sample Account Analysis.**

The FDIC pass through charges has been replaced with the Deposit Coverage Fee. The Deposit Coverage Fee is charged monthly and is calculated using the average monthly ledger balance (per $1,000). WFWV's Deposit Coverage fee is $0.05 per $1,000 and your Earning Credit Rate is 1.25%. Please see the **Exhibit** section for **Exhibit A – Pricing Page**.

3.1.4.9 The financial institution must only charge a single fee for ACH credits, which includes the associated addenda records. Therefore, an ACH credit with me addenda record would be charged the same fee as an ACH credit with multiple addenda records. The financial institution will also charge for the delivery of the NACHA CCD+ formatted file containing ACH credit transactions and the associated addenda record(s).

U.S. Bank agrees and will charge only a single fee for ACH credits which includes the associated addenda records.

3.1.4.10 The financial institution must not charge for ACH items originating from the WV Treasurer identified as Company ID 1556000814.

U.S. Bank understand this request and will not charge for ACH items for company ID 1556000814.

3.1.4.11 The financial institution will charge a fee for ACH debits and debit blocks.

U.S. Bank agrees. Please see **Pricing Page** in the **Exhibits** section.

3.1.4.12 The financial institution shall agree that the highest daily ledger balance or the highest daily deposit, whichever is greater, in all accounts less the federally insured amount of $250,000.00 or the current prevailing amount or the corresponding month of the preceding year will be collateralized so that such amount is never greater than 90% of the market value of collateralization. The collateral shall be equal to the sum of all account balances for WFWV. The determination of the initial collateralization will be a function of the daily ledger balance or the highest deposit; whichever is greater, for the corresponding month of the preceding year. According to West Virginia State Code 5A-3-(8) http:wwwlegis.state.wv.us/WVCODE/Code.cfm the financial institution agrees that liquidated damages shall be imposed at the rate of $100.00 per day for failure to provide collateral requirements. This clause shall in no way be considered exclusive and shall not limit the State or WFWV's right to pursue any other available remedy. The Executive Director may waive this assessment in his judgment, if circumstances beyond the Control of

the financial institution caused the collateral deficiency. Any such circumstances must be documented in writing and submitted to the Executive Director for consideration.

U.S. Bank understands. U.S. Bank's Collateral Management department within our Corporate Treasury Division is responsible for tracking deposits and monitoring collateral. U.S. Bank pledges and maintains qualified securities as deposit collateral in compliance with the state of West Virginia Government Code and other applicable laws.

3.1.4.13 Withdrawal or substitution of any collateral pledges as security may be permitted with the approval of the West Virginia State Treasurer. Chapter 12, Article I, Section 4 of the West Virginia code states, "All pledge securities must be delivered to the safekeeping agent designated by the State Treasurer Office."

U.S. Bank understands.

3.1.4.14 Acceptable forms of collateral must be in accordance with those provided in the Collateral Policy and Procedures Manual of 2009 as provided by the Office the West Virginia State Treasurer. http://www.wvsto.com/dept/CashMgt/Documents/Outside%20Bank%20Accounts%20Policies%20and%20Procedures%20-%20Revised%203-4-10.pdf

U.S. Bank understands.

3.1.4.15 The financial institution must have the capability of receiving and transmitting monies by wire. Said monies received by the financial institution will be considered immediately collectable and available for transfer.

U.S. Bank understands and accepts wire transfers. You can view incoming and outgoing wire transfers in real-time via SinglePoint. All details related to the transaction are available to view, print or export. We will credit your account for all incoming wires received before 6 p.m. ET each business day. Said moneys received will be considered collected and available for transfer as needed. Our wire transfer department will stay open to receive and process incoming wire transfers in the event the Federal Reserve wire hours are extended.

3.1.5 The financial institution must provide WFWV with data transmission solutions that meet WFWV's requirements which do the following.

3.1.5.1 Data File Transmittal- provide a secure Communication Protocol site to transfer data and electronic reports to and from the financial institution and State WFWV office.

3.1.5.2 Security Design and Safeguard Features - Include design features that safeguard against fraud, abuse, and waste.

3.1.5.3 Right of Privacy of Clients-Protect the right of privacy of all WFWV clients.

3.1.5.4 Use of Tested State-of-the-Art Techniques - Use tried and State-of- the-Art techniques as opposed to untested technology that may or may not be successful.

The financial institution will receive a daily file Sunday through Friday from WFWV of checks written and checks voided that day. This file will be electronically transmitted to the bank Record layout below:

Record Code	**X (1)**
"C" for checks written	
"V" for checks voided	
Account number	**9 (10)**
Check number	**9 (10)**
Check amount	**9 (8) V99**

This file will be used by the financial institution to supply a daily reconciliation for WFWV. It will also be utilized to ensure that no fraudulent checks are cleared.

Monthly check reconcilement transmittal:

Field	Data Type	Size
Check Number	**Numeric**	**7**
Amount	**Numeric**	**8.2 (000000000.00)**
Clear Date	**Numeric**	**8**

U.S. Bank Data Transmission Service offers WFWV a variety of methods to transfer your data files to and from U.S. Bank, which enables you to send and receive data in an efficient and secure manner. You get faster account updates and the convenience of sending and receiving transaction information when you wish, using the method of your choice. File level encryption options can be used in conjunction with channel level encryption.

Data Transmission supports the following communication options:

- Internet-based Hypertext Transfer Protocol Security (HTTPS)
- AS2
- File Transfer Protocol over SSL (FTPS)
- SSH File Transfer Protocol (SFTP)
- Virtual Private Networks (VPN) using FTP-SSH or FTP-SSL client
- IBM/Sterling's CONNECT:Direct

The internet-based transmission methods incorporate 128-bit SSL, DES3 or AES 256-CBC encryption to ensure secure communication over the internet. The encryption method is tied to the transmission communication method selected, but all offer comparable security features. File level encryption is also available.

You control the delivery time of your data; data files can be pushed to you or held until you connect to retrieve the data. Our system is available for file transfers 24/7. Many of our supported transmission options offer you the ability to predefine recurring transfers and schedule them for automatic processing. We can accept transmissions directly from your systems, which eliminates the need to handle tapes, cartridges and diskettes. Internet-based transmission methods offer you the option of reducing telecommunication charges associated with other types of data transmissions.

Data Transmission fully complements our comprehensive line of treasury management products, such as ACH, account reconciliation, positive pay and lockbox services. Our data transmission specialists can assist you in determining which data transmission method best meets your requirements and establishing connectivity with our system. Our data transmission specialists are available 24/7.

U.S. Bank receives many requests every year from customers wanting to understand various elements of our Information Security program. Our high-level document, the **U.S. Bank Information Security Posture**, should address many of these common questions, and is attached in the **Exhibit** section.

3.1.6 The successful vendor will be completely responsible for implementation and the transition from the current banking system. This section details specifics of the tasks involved.

Implementation Overview

To help make your transition to U.S. Bank smooth and efficient, we designed an implementation process that includes a dedicated team of professionals. Our team ensures a successful onboarding experience. During the implementation process, we spend the time and resources to build a solid foundation for a successful relationship between WFWV and U.S. Bank. As your dedicated business partner, we work to understand your organization and provide solutions to support your business needs. You can rely on our commitment, accessibility and responsiveness.

Your primary U.S. Bank contact is your relationship manager Tim Rieder, who works with your U.S. Bank implementation team. This team includes the following individuals:

- **Implementation resource**, The IR plays a critical role in orchestrating the entire implementation process and is your primary contact during this phase. They distribute and obtains appropriate documentation from your organization to implement new services; works closely with various operations departments within U.S. Bank; and coordinates the technical team for system testing and training. Their level of experience and commitment will ensure your implementation is accurate and is completed within the established timeframes.
- **Treasury management consultant, Dave Sullender**—He works with your organization to identify the appropriate solutions to help your organization manage cash and improve efficiencies. He will also keep you informed of new or emerging technologies, which may impact the way you do business.
- **Treasury management associate,** The TMA works closely with Dave Sullender to establish the identified products and services.

Although there are many people involved in implementing treasury management services, you will always have one contact you can call with questions during your implementation process — your implementation resource. After successful implementation, you are assigned a Commercial Customer Service team for ongoing product and account support.

The process for establishing products and services with us may consist of the following phases:

- Scheduling a discovery meeting to ensure we have an in-depth understanding of your workflows and related cash flows to appropriately finalize the solution set.

- Gathering pertinent information necessary to complete documentation to establish accounts and implement services. Documentation is pre-filled by U.S. Bank where possible.
- After obtaining all required customer information, we send you applicable documentation, including service agreements, user guides and other materials as necessary.
- The agreements and/or applicable questionnaires are completed and received by the implementation resource, which marks the start of the service setup.
- Assembling the implementation team, who will work with your employees throughout the process.
- Developing an implementation strategy designed to achieve the production date you specify.
- Coordinating a kick-off meeting in which key stakeholders from U.S. Bank and WFWV are introduced, documentation can be presented for execution and the preliminary timeline is discussed and agreed upon.
- Facilitating weekly touch point meetings with key stakeholders throughout the process to ensure benchmarks are on track and any issues are quickly resolved.
- During setup, we test data transmissions for you using ARP, lockbox or ACH direct transmissions.
  - U.S. Bank first tests for connectivity through a telecommunications handshake.
  - Next, customer test files are transmitted for each applicable service to ensure the data is properly received.
  - Upon successful testing, we select a production date.

3.1.6.1 The vendor will perform a walk-through-through immediately after the bid is awarded and will identify, in writing, necessary changes to WFWV's current banking operations.

U.S. Bank understands and agrees.

3.1.6.2 The vendor will provide one-time on-site training consisting of eight (8) hours at 1900 Kanawha Blvd., East, Building 3, 4th Floor, Charleston, WV for a maximum of twenty (20) people on the usage of required online banking services and transmissions of files at no additional cost to WFWV.

U.S. Bank understands and agrees.

3.1.6.3 WFWV will be responsible for making networking changes deemed necessary and agreed upon by WFWV.

U.S. Bank agrees.

3.1.6.4 WFWV will name a project manager who will be responsible for assembling WFWV project team and will be the focal point for all project issues.

U.S. Bank understands and agrees.

3.1.7 The vendor will be responsible for testing all aspects of the new banking system prior to implementation. All test results will be documented in writing by the financial institution and will be verified and subject to acceptance by WFWV.
3.1.7.1 Testing will minimally consist of the following:

1. **Transmission of electronic files to and from the vendor and WFWV.**
2 **Online activities to test transactions.**
3. **Connectivity tests (i.e. password access, data lines, etc.)**

U.S. Bank understands and agrees.

3.1.7.2 Test results will be documented in writing, presented to WFWV for review and subject to their written approval.

U.S. Bank understands and agrees.

3.1.7.3 The vendor must provide service coverage during the hours of 9:00 AM to 5:00 PM EST Monday through Friday

Commercial Customer Service teams provide customer service each business day from 8 a.m. to 8 p.m. ET.

3.1.7.4 The vendor must provide two (2) hour call back during regular business hours of 9:00AM-5:00PM EST.

Commercial Customer Service (CCS) has a strong commitment to customer satisfaction. We promise:

- To be accessible between published servicing hours — you do not have to leave a message — phone calls are answered in person.
- To provide a same-day response to voice mails, faxes and emails received before 4 p.m.
- To take ownership of your request and follows it through to resolution.
- You always have access to multiple knowledgeable Commercial Customer Service bankers who will take responsibility for the request, even if your regular contact is unavailable.
- To provide same-day completion of monetary banking transactions* initiated through Commercial Customer Service.

*Wire transfers must be received by 4 p.m. ET due to risk management controls and Federal Reserve deadlines. All other monetary transactions must be received by 4 p.m.

3.1.7.5 The vendor must establish a primary operating facility at a single site through use of existing facilities, expansion of facilities or acquisition of a new facility.

U.S. Bank understands and agrees.

3.1.7.6 Unless herein specifically provided otherwise, the vendor must ensure that all required monthly reports must be received by WFWV by the 15th day of the month subsequent of the reporting period. For example, a report for the month of February must be received by WFWV by March 15th. In the event the 15th calendar day of the month falls on a weekend; the financial institution agrees to supply this analysis on the preceding Friday.

WFWV can pull reports from SinglePoint when you are ready for the information. Deposit reporting data is available each day at 4 a.m. ET.

3.1.8 The vendor must provide the following mandatory requirements.

3.1.8.1 The Federal Deposit Insurance Corporation (FDIC) must insure the financial institution. Proof of deposit insurance must be provided within forty-eight (48) hours of notice of award.

Our FDIC number is 6548. Please see the **Exhibit** section for a copy of our **FDIC Certificate.**

3.1.8.2 The financial institution shall implement any FDIC Depositors Insurance Fund fee at the prevailing current published rate and charge through monthly analysis of qualifying accounts.

The FDIC pass through charges has been replaced with the Deposit Coverage Fee. The Deposit Coverage Fee is charged monthly and is calculated using the average monthly ledger balance (per $1,000). WFWV's Deposit Coverage fee is $0.05 per $1,000.

3.1.8.3 The financial institution must have Automated Clearing House (ACH) receiving financial institution capabilities.

U.S. Bank has capabilities to receive ACH files. Regionally, U.S. Bank belongs to and serves on the Board of Directors for the Upper Midwest Automated Clearing House Association (UMACHA) and the Western Payments Alliance (WesPay). We are also a member of the Electronic Payment Network Association.

According to the 2017 NACHA ranking U.S. Bank is:

- The fifth largest origination bank, with 715,414,329 million ACH transactions in 2016, up 2.2 percent from 2016.
- The fifth largest receiving bank, receiving 627,118,864 ACH items in 2016, up 5.7 percent from 2016.

3.1.8.4 The financial institution must conform to National Automated Clearing House Association (NACHA) rules.

U.S. Bank is in compliance with NACHA rules.

3.1.8.5 The financial institution must comply with all Federal and State Banking Regulations.

As a federally regulated financial institution, U.S. Bank provides products and services subject to examination by various regulatory agencies, including the Office of the Comptroller of Currency (OCC), the Consumer Financial Protection Bureau (CFPB) and the Federal Reserve (FRB). These institutions regularly examine our internal controls to ensure they meet federal standards and comply with applicable law.

As your primary U.S. Bank contact, your relationship manager will work with you on any changes that affect you directly.

3.1.8.6 The State shall have full and free use of all systems, products, and deliverables supplied by Purchase Order resulting from this CRFQ.

U.S. Bank understands and agrees.

3.1.8.7 Workforce West Virginia will supply their own check drafts.

U.S. Bank understands and agrees.

3.1.8.8 Deposit Insurance (DIF)fess will be assessed to qualifying accounts at the standard published monthly rate.

The Deposit Coverage Fee is charged monthly and is calculated using the average monthly ledger balance (per $1,000). WFWV's Deposit Coverage fee is $0.05 per $1,000. Please see the **Exhibit** section for **Exhibit A – Pricing Page**.

4. CONTRACT AWARD:

4.1 Contract Award: The Contract is intended to provide Agencies with a purchase price on all Contract Items. The Contract shall be awarded to the financial institution that provides the Contract Items meeting the required specifications for the lowest overall total cost as shown on the Exhibit A.

4.1.1 Vendor should include with their bid a copy of any Software Terms and Conditions that the State of West Virginia or the Agency will have to agree or accept as a part of this solicitation. This information will be required before Purchase Order is issued.

In the **Exhibit** section we have provided our **Master Services Agreements Appendix A & B, Terms and Conditions** and **Your Deposit Agreement**.

4.2 Pricing Pages: Vendor must complete and submit with their bid response Exhibit "A" (Pricing Pages) in its entirety as failure ·to do so may result in their bid being disqualified. Vendor should type or electronically enter the information into the Pricing Pages to prevent errors in the evaluation. The vendor should also put their "Total" in wvOASIS Pricing Section Commodity Line. The pricing page must not be altered in any way, this will result in a vendor being disqualified. Multiple pricing sheets may result in a vendor being disqualified.

The Pricing Pages contain a list of the Contract Items and estimated purchase volume. The estimated purchase volume for each item represents the approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.

Vendors who wish to respond to a Centralized Master Agreement Requisition (CRQM) online may submit information through the State's wvOASIS Vendor Self Service (VSS) Vendors should download the Exhibit "A" Pricing Page that is attached separately to CRQM and published to the VSS. Vendors Must complete this form with their pricing information and include it as an attachment to their online response with an Attachment Type of "Pricing". The Pricing Page attachments (Pricing) are then downloaded by the Buyer during the scheduled bid opening/or bid evaluation.

If unable to respond online please submit the Exhibit "A" Proposal Form/Pricing Pages with your bid prior to the scheduled bid opening date.

Please see **Exhibit A Pricing Page** in the **Exhibit** section.

5. ORDERING AND PAYMENT:

5.1 Ordering: Vendor shall accept orders through wvOASIS, regular mail, facsimile, e-mail, or any other written form of communication. Vendor may, but is not required to, accept on-line orders through a secure internet ordering portal/website. If Vendor has the ability to accept on-line orders, it should include in its response a brief description of how Agencies may utilize the on-line ordering system. Vendor shall ensure that its on-line ordering system is. properly secured prior to processing Agency orders on-line.

U.S. Bank has an automated coin and currency order service for our cash vaults, which utilizes the Glory VAS and Comp-U-Order automated systems to reduce cash deposit processing time and speed collection as an enhancement to your treasury management functions. Armored carriers deliver cash and check deposits to our highly secured cash vaults. The amount of cash deposit is entered into the system and assigned a trace number. The deposit is tracked by the systems from receipt to verification, allowing us to constantly monitor the status of all deposits. Cash deposits are sent to the verification area while check deposits go to item processing for deposit to your account.

The Glory Comp-U-Order automated phone ordering system and SinglePoint Cash Vault online ordering allow change orders to be placed 24/7. Standing change orders, containing pre-determined denominational values and pre-scheduled delivery days, may be setup through our cash vaults to avoid manually placing daily orders by telephone or web. Standing change orders allows you to set change order amounts to ensure local locations are not ordering excessive amounts and avoid any fraud.

Security is of utmost importance to our cash vaults. We have camera surveillance throughout. The Glory VAS System has built-in counterfeit detection.

Change Orders

Orders may be placed 24/7 on Comp-U-Order or SinglePoint Cash Vault. Weekend orders, including Monday inventory, must be ordered by the Friday deadline for all vaults with a one business day lead time. You must make all arrangements with your courier for change order delivery.

5.2 Payment: Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

U.S. Bank understands and agrees.

6. PERFORMANCE:

Vendor and Agency shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already included herein by Agency. In the event that this Contract is designated as an open-end contract, Vendor shall perform in accordance with the release orders that may be issued against this Contract.

U.S. Bank understands. Your Relationship Manager, Tim Rieder, will meet with WFWV as frequently as you would like. Your relationship manager, Tim Rieder, is your primary contact for our partnership. Tim works with your treasury management consultant, Dave Sullender, to support you and your overall relationship. Your relationship team advocates for you in the marketplace, working to understand how new and emerging technologies will create better functionality and provide you an economic advantage.

You can expect timely responses to operational, pricing, technical questions and other general inquiries on a day-to-day basis.

7. PAYMENT:

Agency shall pay the flat fee per line item, as shown on the Pricing Pages, for all Contract Services performed and accepted under this Contract. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

U.S. Bank understands and agrees. When delivered via one of our online services, such as SinglePoint Information Reporting or EDI (available in the ANSI ASC X12 822 format), your account analysis is available the seventh business day of the month. If the analysis is mailed, mailing is generally completed by the eighth business day of the month, with the DDA being charged on the 10th business day of the month.

8. TRAVEL:

Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately.

U.S. Bank understands and agrees.

9. FACILITIES ACCESS:

Performance of Contract Services may require access cards and/or keys to gain entrance to Agency's facilities. In the event that access cards and/or keys are required:

9.1 Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.

9.2 Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost or stolen.

9.3 Vendor shall notify Agency immediately of any lost, stolen, or missing card or key.

9.4 Anyone performing under this Contract will be subject to Agency's security protocol and procedures.

9.5 Vendor shall inform all staff of Agency's security protocol and procedures.

U.S. Bank understands and agrees. Please see the **Exhibit** section for our completed **Designated Contact** form.

10. VENDOR DEFAULT:

10.1 The following shall be considered a vendor default under this Contract.

10.1.1 Failure to perform Contract Services in accordance with the requirements contained herein.

10.1.2 Failure to comply with other specifications and requirements contained herein.

10.1.3 Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

10.1.4 Failure to remedy deficient performance upon request.

10.2 The following remedies shall be available to Agency upon default.

10.2.1 Immediate cancellation of the Contract.
10.2.2 Immediate cancellation of one or more release orders issued under this Contract.
10.2.3 Any other remedies available in law or equity.

U.S. Bank understands and agrees.

11. MISCELLANEOUS:

11.1 Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager: Tim Rieder
Telephone Number: 614.232.2081
Fax Number: 614.849.3444
Email Address: tim.rieder@usbank.com

11.2 The terms "must", "will," "shall," "minimum," "maximum" or "is/are required" identify a mandatory contract requirement. Decisions regarding compliance with any mandatory requirements shall be at the sole discretion of the Purchasing Division. Failure on the part of the financial institution to meet any of the mandatory specifications shall result in disqualification of the bid.

U.S. Bank understands.

11.3 Attachments A & B are example only showing what information the successful institution will submit to our agency so that we can be in compliance with reports required by the Department of Labor. This form cannot be altered.

U.S. Bank understands.

11.4 Costs and charges not specifically identified in the pricing pages of this CRFQ will not be allowed.

U.S. Bank understands. All costs are identified in **Exhibit A – Pricing Page**.

Exhibit A - Pricing Page for WorkForce West Virginia Banking Services **REVISED FOR ADDENDUM 2**

(Note: All quantities are estimates.)

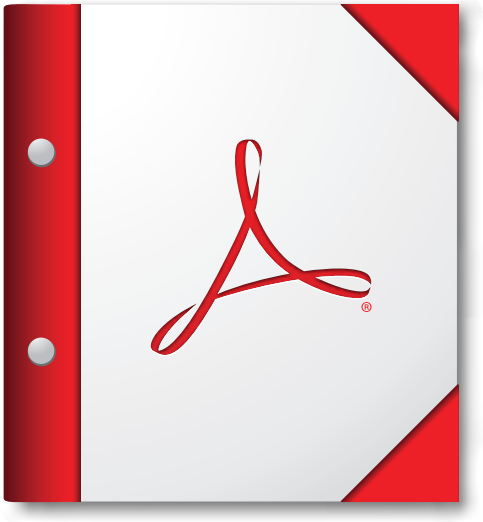
3/06/2019 Revised

	Unit of Measure	Unit Cost	Monthly Est. Qty	Month per Year	Extended Cost
3.1.1 Banking Services for six (6) Benefit Accounts					
1. Price per draft presented, edited, and paid *(Note: Estimated at 60,000 per calendar year.)*	Per Draft	0.015	5,000	12	900.000
2. Stop payment per draft *(Note: Estimated at 360 per calendar year.)*	Per Draft	7.83	30	12	2818.800
3. Daily Balance/Reporting On-line	Service Fee	25.31	21	12	6378.120
4. Daily Reconcilement and Exception Report	Service Fee	39.23	21	12	9885.960
5. Other *(Note: Check-Imaging Cd ROM.)*	Per Draft	0.0495	5,000	12	2970.000
6. Total for Benefit Accounts prior to Earnings Credit Rate Reduction *(Note: Add lines one (1) through five (5).)*					22952.880
7. Earnings Credit *(Note: Average ledger balance estimated at 1,350,000 per month.)* **Vendor must enter rate as a decimal** *Example: 3.5% entered in cell as .035.*	Percent/Rate	0.0125	1,350,000	1	16875.000
8. Total for Benefit Accounts after Earning Credit Rate Reduction *(Line six (6) minus line seven (7).)*					6077.880
3.1.3. Banking Services for two (2) Clearing Accounts					
9. Price per draft presented, edited and paid (Note: Deposits are made on a Daily Basis estimated to be 87,000 per calendar year.)	Per Draft	0.015	7,250	12	1305.000
10. Price per Deposit/Item associated with CCD+ Addendum file accepted from TPA's. Files and deposits in Clearning Account A to be received on a quarterly basis *(Note: Estimated to be six (6) per quarter or 24 per year.)*	Per Deposit/Item	0.005	200	12	12.000
11. Price per CCD+ Addendum file accepted from TPA's Files and Deposits in Clearing Account A to be received on a quarterly basis. *(Note: Estimated to be six (6) per quarter or 24 per year.)*	Per File	0	2	12	0.000
12. Price per CCD+ Addendum file from TPA's balanced to deposit, and information transmitted to WorkForce West Virginia. Files and deposits in Clearing Account A to be received on a quarterly basis. *(Note: Estimated to be six (6) per quarter or 24 per year.)*	Per File	1011.87	2	12	24284.880
13. Price per draft for ACH debits and debit blocks.	Per File	0.005	7,250	12	435.000

14. Price for Authorized ACH Company ID.	Flat Fee	0	1	12	0.000
15. Price for ACH Debits Received.	Flat Fee	0.005	1	12	0.060
16. Daily Balance/Reporting On-line	Service Fee	8.43	21	12	2124.360
17. Total for Clearning Accounts prior to Earnings Credit Rate Reduction *(Note: Add line nine (9) through sixteen (16).)*					28161.300
18. Earnings Credit *(Note: Average ledger balance estimated at 1,670,000 per month.)* **Vendor must enter rate as a decimal** *Example: 3.5% entered in cell as .035.*	Percent/Rate	0.0125	1,670,000	1	20875.000
19. Total for Clearing Accounts after Earnings Credit Rate Reduction *(Note: Line seventeen (17) minus line eighteen (18).)*					7286.300
20. FDIC Deposit Insurance Fund (DIF) *(Note: Average ledger balance estimated at 3,020,000 per month.)* *(Note: FDIC Fee to be accessed to qualifying accounts at the standard published monthly rate. EXAMPLE: 9.1333% per $1,000 on avergae ledger balances.)*	Rate	0.00005	3,020,000	1	151.000
21. Earnings Credit *(Note: Average ledger balance estimated at 3,017,118 per month.)* **Vendor must enter rate as a decimal** *Example: 3.5% entered in cell as .035.*	Percent/Rate	0.0125	3,017,118	1	37713.975
22. Total FDIC for both Benefit and Clearing Accounts after Earnings Credit Rate Reduction. *(Note: Line twenty (20) minus line twenty-one (21).)*					-37562.975
23. Daily Armored Car/Courier Service (See Section 3.1.4.1 of RFQ for pickup location and time.)	Flat Daily Rate		22	12	0.000
GRAND TOTAL *(Note: Add lines eight (8); line nineteen (19); and line twenty-two (22); and line twenty-three (23)).*					-24198.795

VENDOR IS REQUIRED TO ENTER THEIR TOTAL COST IN WVOASIS PRICING SECTION COMMODITY LINE A. IN ADDITION, VENDOR MUST ALSO SUBMIT THE EXHIBIT "A" PRICING PAGES PER THE DIRECTIONS IN SECTION 4.2 OF THE SPECIFICATIONS.

(NOTES VENDOR SHOULD BE AWARE OF: (1) WorkForce West Virginia supplies its own check drafts. (2) Costs/charges not specifically identified above will not be allowable. The above list contains all items for which the successful vendor will be permitted to charge under any resulting Purchase Order. (3) Attachments A & B are for example only showing what information the sucessful vendor will submit to the agency so that the agency will be in compliance with the reporting requirements from the Department of Labor.)



For the best experience, open this PDF portfolio in Acrobat X or Adobe Reader X, or later.

Get Adobe Reader Now!

U.S. Bancorp
Information Security Posture

Version: September 2017

Table of Contents

Introduction

U.S. Bancorp[1] has a legal and ethical responsibility to ensure its information is secure and private, is current and maintained accurately, and is available to authorized recipients when needed. U.S. Bancorp is also expected to obtain and process information fairly, keep it only for specified and lawful purposes, process data only in ways compatible with the purposes for which it was given initially and ensure data kept is adequate, relevant and not excessive. Moreover, data is not retained longer than necessary for compliance with legal, regulatory, and operational requirements.

To do this, U.S. Bancorp maintains an Information Security Program founded on a set of principles described within this document. U.S. Bancorp recognizes that some principles and associated controls may not be applicable to, or appropriate for every business environment.

U.S. Bancorp is committed to protecting the confidentiality, integrity, availability and privacy of customer data. Our reputation rests, in part, upon securely maintaining our customers' information assets. U.S. Bancorp understands the importance of safeguarding all the information entrusted to us, regardless of who owns that information. All partner data is classified as "U.S. Bancorp Confidential" or "U.S. Bancorp Customer Confidential," as are our trade secrets and customers' personal information.

U.S. Bancorp also understands the importance of demonstrating our intent. This document provides a high-level overview of our security posture, which describes the commitment and resources we apply to information security.

This document is not intended to replace the documents needed to demonstrate compliance with federal regulations. The BITS Standardized Information Gathering ("SIG") Questionnaire was developed as an industry-wide response to those entities seeking more information from financial institutions on their security practices, including compliance with all applicable laws, rules and regulations. Contact your U.S. Bancorp business representative to obtain a copy of U.S. Bancorp's responses to the SIG. If a thorough evaluation of U.S. Bancorp's security controls and practices is required, the SIG questionnaire should be used.

Security Program and Principles

It is U.S. Bancorp's legal and ethical responsibility to ensure its information is protected from unauthorized disclosure, is maintained accurately and is available to authorized recipients when needed. U.S. Bancorp maintains an Information Security Program which relies on the following security principles:

- **Information and Information Systems are Assets:** U.S. Bancorp information assets are protected from disclosure, modification, deletion or loss in accordance with the sensitivity of the information and the risks associated with its disclosure to unauthorized individuals.

- **Information Security Risk Management**: U.S. Bancorp's Information Security Program aligns with *de facto* standards to manage well-known and well-understood risk. The program maintains processes to assess and manage risks to the security of U.S. Bancorp information as new threats emerge and as technology and business practices change. Compliance with information security policy is critical to managing information security risk.

- **Legal, Regulatory, and Contractual Compliance**: U.S. Bancorp's Information Security Program supports compliance with applicable laws, regulations and contractual requirements. U.S. Bancorp has mapped its information security policies to applicable legal, regulatory and contractual requirements including Gramm-Leach-Bliley Act ("GLBA"), Payment Card Industry ("PCI"), Health

[1] As used herein, U.S. Bancorp refers to U.S. Bancorp and U.S. Bank.

Insurance Portability and Accountability Act (“HIPAA”), Sarbanes-Oxley Act (“SOX”) and the National Institute of Standards and Technology (“NIST”) Cybersecurity Framework.

- **Layered Security (Defense in Depth)**: U.S. Bancorp’s Information Security Program includes technical components at all levels of the infrastructure to significantly reduce the likelihood a weakness in one area does not lead to a compromise. Procedural controls are put in place wherever responsibility for security activities are assigned. Managerial controls ensure responsibilities are carried out and technical and procedural controls are functioning as designed.

- **Preference for Preventive over Detective Controls**: Wherever feasible, reasonable controls are implemented to prevent security problems. Detective and corrective controls are used as a second layer of verification for primary preventive controls, as appropriate, and as a substitute for preventive controls only where preventive controls are not feasible or not yet in place.

- **Restricted Access to the Enterprise Network**: Ensuring access to information assets is restricted to authorized individuals requires minimizing the number of ways individuals may gain network access. A limited number of control points are maintained and their exclusive use enforced. Restricted access methods include dial-in access, employee access to internal resources within the network via the Internet virtual private network (“VPN”), secure business partner access to U.S. Bancorp applications via the Internet, internal network access and administrative access to resources within the network.

- **Isolation of Critical and Sensitive Resources within the Enterprise Network**: Assets are classified according to their business criticality and sensitivity, and security resources are allocated to provide the greatest protection for the most critical (Mission Critical) and most sensitive (U.S. Bancorp Confidential and U.S. Bancorp Customer Confidential) assets. Network design (network segmentation, resource isolation) and access controls support this protection priority.

- **Restricted Access Based on Level of Trust**: Access to information assets is controlled based on the level of trust of the individual seeking access and the security of the access path. Internal employees using U.S. Bancorp-supported PCs within the network are more trusted than business partners connecting via the Internet; business partners are more trusted than prospective customers; etc. In general, the level of trust diminishes as the level of U.S. Bancorp control over the individual seeking access and the access path is reduced, and as U.S. Bancorp’s ability to verify the level of security of the accessing party and the access path decline. Access to assets within the network is reduced as the level of trust diminishes.

- **Business Control of Business Information Resources**: Although within enterprise operations, Technology and Operations Services (“TOS”) maintains custody of information assets, business management controls their security. The Information Security Program establishes and maintains processes for information ownership and access authorization to ensure adequate segregation of function through business control over business information assets.

Least Privilege and Access based on Business Need: To ensure information confidentiality, availability and integrity, access to information resources are provided on a need-to-know and need-to-use basis, according to job roles and functions defined by the information owner. Where privileged access is required for those in custodial roles (generally, TOS) or business line IT staff responsible for the processing, storage, transmission, backup and secure handling of information), such access is limited — to the extent possible — to the level needed within the specific role of each individual. Such individuals are educated on the risks and responsibilities related to having this access and agree to comply with restrictions on their

use of privileged authority.

- **Secure Application Design and Development**: U.S. Bancorp's Information Security Program includes steps throughout the application life cycle (design, development, deployment, maintenance and retirement) to ensure the protection of information assets accessible through business applications.

- **Protection of Information Assets in the Custody of Third Parties**: When U.S. Bancorp information assets are placed in the custody of third parties, U.S. Bancorp retains responsibility for their protection to meet business, legal, regulatory and contractual requirements. It vests that responsibility with its third party relationship owners, who ensure contractual agreements provide for the protection of such assets (consistent with enterprise security policy) and guarantee U.S. Bancorp the right to verify the protection of its assets through its own audit processes or receipt of reliable third party assessments.

- **Support of and Consistency with Other U.S. Bancorp Information Protection Practices:** U.S. Bancorp's Information Security Program is a critical component of U.S. Bancorp's overall information protection program. It supports U.S. Bancorp's overall information protection objectives and is coordinated with other related programs, such as enterprise privacy, compliance, and risk management programs, to ensure clarity of purpose and a consistent message to all U.S. Bancorp employees and contractors responsible for protecting customer and U.S. Bancorp information assets.

U.S. Bancorp's Information Security Program is based on these security principles, which are the foundation of U.S. Bancorp's Information Security Program. U.S. Bancorp requires employees and contractors to apply these underlying principles when protecting information, where applicable.

Risk Management

U.S. Bancorp's Information Security Program is designed to identify, quantify (where possible), prioritize and mitigate risks to acceptable levels with the objective of maintaining the security management of enterprise information assets and intellectual property. In addition, the program utilizes a risk model when determining appropriate levels of priorities and actions needed for managing risks classified as Very High, High, Moderate, and Low.

U.S. Bancorp's Information Security Program aligns with de facto standards to manage well-known and well-understood risks. The program maintains processes and methodologies to assess and manage risks to the integrity, confidentiality and availability of enterprise information assets as new threats emerge and as technology and business practices change. The program is governed by information security policies established by approval from the Information Security Steering Committee ("ISSC"). Compliance with information security policies is required in the absence of an approved risk extension.

U.S. Bancorp's Information Security Program implements technical and operational controls at all levels of the technology and business ecosystem to significantly reduce the likelihood a weakness in one area will lead to a pervasive compromise of information assets and intellectual property in other areas. Detective and corrective controls are used as a second layer of verification for primary preventive controls, as appropriate, and as mitigating controls where preventive controls are not feasible, or not yet in place.

While the enterprise Information Security Program requirements and controls are founded upon the principles identified within this document, appropriate requirements and controls for treating information security related risks to enterprise information assets and resources are determined based upon risk assessment activities. The recognition that some associated controls may not be applicable or appropriate for every environment (business lines, departments, and information systems) is a guiding principle for

taking a balanced approach to managing risks across distributed environments.

Security Policy

Information security policies are established and maintained to ensure legal, regulatory and contractual obligations, and our obligations to protect business and customer information are communicated and enforced. Information security policies establish requirements for information protection in alignment with the security program principles and includes maintenance of security configuration baselines for all critical technologies used to store, transmit or process confidential information.

Information security policies are accessible to all employees on the internal corporate web portal and U.S. Bancorp holds all personnel accountable for understanding and complying with those policies. All information security policies are reviewed on an annual basis by the appropriate subject matter experts from Information Security Services ("ISS") and each of U.S. Bancorp's business lines. Policies are then approved by the ISSC. Security policies establish written requirements for U.S. Bancorp Data Loss Prevention practices and other control processes to protect confidential, private and sensitive information through the stages of the information lifecycle.

Organizational Security

U.S. Bancorp's Chief Information Security Officer ("CISO") has oversight of the ISS organization and security operations within U.S. Bancorp, and reports directly to the Vice Chairman for TOS. The CISO has overall management authority and operational responsibility for the U.S. Bancorp Information Security Program. The CISO presents and recommends significant modifications of the Program for approval by the Board or the ISSC. Additionally, the CISO annually reports on the overall status of the Program and U.S. Bancorp's compliance with applicable laws, regulations and contractual obligations. The ISSC provides governance and oversight of ISS' development and implementation of the U.S. Bancorp Information Security Program.

The Information Security Program undergoes annual audits performed by the internal auditors, Corporate Audit Services. U.S. Bancorp's Information Security Program is regularly reviewed by independent auditors and assessors, both internal and external, and federal regulators. Functional areas within ISS are reviewed by auditors to ensure independent and objective assessments of the adequacy, effectiveness, and efficiency of risk extension, transfer and mitigation processes.

The ISS department is comprised of approximately 600 Information Security Professionals organized by functional security teams reporting up to the CISO. Activities are aligned with the overall information security strategy and roadmap which are refreshed on an annual basis.

A formal report and information security strategy are presented to the U.S. Bancorp Board of Directors on an annual basis. Quarterly updates are also provided to the Board regarding progress toward strategic goals and other updates. Monthly metrics are communicated to senior management reflecting key performance indicators of the Information Security Program.

Third Party Agreements

With respect to confidentiality agreements and third parties, non-disclosure agreements ("NDAs") are executed by U.S. Bancorp any time U.S. Bancorp is engaged in dialogue or the exchange of information deemed sensitive or confidential to U.S. Bancorp. The only type of information exchange where an NDA would not be needed would be where information is generally known or available to the public. The NDA/Confidentiality Agreement ensures sensitive or confidential information remains protected, and U.S. Bancorp has legal recourse in the event there is disclosure. NDAs are part of the checklist of artifacts considered during engagements with contractors, third party/hosted data center providers and others.

When a U.S. Bancorp line of business decides to enter into a business arrangement with another entity, it

first determines whether U.S. Bancorp Customer Confidential information will be shared. If so, a security risk assessment is performed on the third party before a contract with the third party is executed. Security risk assessments help ISS determine both the information and physical security posture of third parties. These assessments are extensive and cover the prospective third party's policies, network architecture, computing environment, access control standards, intrusion detection, disaster recovery planning and auditing. As part of the engagement process, third parties must disclose high-level information on security risks and audit findings, correction of any problems discovered, and results of prior assessments.

Asset Management

Technology Assets

U.S. Bancorp has a formal, documented asset management program which tracks the treatment, handling, disposal, destruction and reuse of all assets that contain or possess customer information. The program is approved by management, communicated to the appropriate constituents and maintains appropriate asset management policies. In order to achieve and maintain appropriate protection of organizational assets, all valuable enterprise assets are accounted for, have a designated owner and rules for acceptable use. Owners are assigned responsibility for the maintenance of appropriate controls of assets. The implementation of specific controls may be delegated by the owner as appropriate, but the owner remains responsible for the proper protection of the assets. Each owner is responsible for maintaining an inventory of all critical assets (e.g., hardware, software, licenses) necessary for business continuity protections.

Assets are classified according to their business criticality and sensitivity, and security resources are allocated to provide greatest protection for the most critical (mission-critical) and most sensitive (U.S. Bancorp Confidential and U.S. Bancorp Customer Confidential) assets. Network design (network segmentation, resource isolation) and access controls support this protection priority.

Information Assets

Enterprise information assets are protected from disclosure, modification, deletion or loss in accordance with the sensitivity of the information and the risks associated with its disclosure to unauthorized individuals. U.S. Bancorp has established handling procedures and access controls commensurate with the data for each information classification. Handling practices related to storage provide reasonable protection of information, regardless of form, against unauthorized disclosure. Protection may include hardware, software or other mechanisms to appropriately control access to U.S. Bancorp Confidential or U.S. Bancorp Customer Confidential information. Information classified as Customer Confidential is not to be used or requested in business processes that do not strictly require it.

U.S. Bancorp personnel are not allowed to divulge, use or attempt to access customer information except in a manner consistent with stated services to the customer and for authorized business purposes. Non-Disclosure Agreements must reflect this intent. Customer Confidential information must not be copied from secure locations. This includes dedicated application databases or other locations where access is limited by role and is transferred to locations not managed with the same access controls. However, if the storage is temporary (one day or less) to support a business need, the file is removed or deleted immediately after the business need is fulfilled.

TOS maintains custody of information assets, and business line management controls their security. The Information Security Program establishes and maintains processes for information ownership and access authorization to ensure adequate segregation of duties through business control over business information assets.

Human Resource Security

Security responsibilities are addressed in job descriptions, terms and conditions of employment and required training to ensure employees, contractors, associates and third party users understand and carry out their Information Security Program roles and responsibilities, and are suitable for the roles they are considered for. All employees, contractors, and third parties are trained on their applicable information security responsibilities and required to attest to their commitment to carry out their information security roles and responsibilities. Prior to employment, where required, candidates for employment are adequately screened relative to the sensitivity of their job responsibilities. Disciplinary processes are in place and followed when employees and other applicable parties violate the requirements of the Information Security Program. Responsibilities are in place to ensure that an employee's or contractor's exit from U.S. Bancorp is managed appropriately to ensure ongoing protection of U.S. Bancorp information assets.

New employee orientation addresses information security topics. The onboarding and orientation process is managed by the Human Resources department. Employees are also required to take information security training within their first 90 days on the job in the U.S. Bancorp Global Learning Lab (GLL) system. Courses are automatically assigned pursuant to the employee's role, and monitored for completion. Records of completion are stored within the U.S. Bancorp GLL system. There are additional courses assigned to those employees who use laptops or other media devices in their role. In addition, any security procedures specific to an employee's position or department are reviewed once on the job.

U.S. Bank conducts pre-employment screening for each applicant that receives a conditional offer of employment, independent contractors and employees of temporary staffing agencies assigned to perform services for U.S. Bank (collectively "new hires"). The decision to hire or not hire an external applicant will be made consistent with applicable legal guidelines and U.S. Bank policy.

All new hires must complete a Criminal Background Check as a condition of employment or assignment to U.S. Bank. Screening must be completed within the 90 day period prior to the employee's start date, unless an exception is approved by the Director of Employee Relations and Legal. Screening completed prior to 90 days before start will be repeated within the 90 day window to ensure compliance.

There are also approved termination procedures in place. Upon notice that an individual's employment or contract with the Bank has been terminated, managers are responsible for completing all applicable steps outlined in the Termination Checklist for Managers to ensure timely processing of termination. Access to all systems and facilities is promptly removed, and the Human Resources department is also notified.

Security Awareness and Training

U.S. Bancorp's Code of Ethics and Business Conduct is reviewed during the new employee orientation session and the Code includes information security requirements. Employees are required to complete the Code of Ethics and Business Conduct on-line training within their first 30 days of employment and are required to recertify on an annual basis. The complete Code of Ethics and Business Conduct are located on the U.S. Bancorp Intranet site, and employees are encouraged to read and understand how the Code applies to them. Employees are also informed of the Ethics Hotline should they feel someone is in violation of the Code. Complaints made to the Ethics Hotline are taken very seriously and an investigation is conducted with an expected resolution and/or course of action.

U.S. Bancorp's Security Awareness For Everyone ("SAFE") Program establishes U.S. Bancorp's enterprise information security awareness program to provide guidance for the protection of U.S. Bancorp business information, systems and processes to U.S. Bancorp employees, independent contractors and employees of temporary staffing agencies in support of U.S. Bancorp's Information Security Program. The required courses include specific courses based on an employee's role and access to systems. The training is refreshed annually. Upon completion of the SAFE courses, employees should be able to understand the U.S. Bancorp information classifications and how to handle information in each classification.

Physical and Environmental

To prevent unauthorized physical access, damage, and/or interference to enterprise premises and information, U.S. Bancorp's Information Security Program addresses appropriate physical security requirements, including those related to the areas where critical or sensitive information is processed and handled. A Physical Security Policy is maintained, approved, communicated, implemented and reviewed by auditors on an annual basis.

Physical Access Control

Security perimeters are defined with identification of appropriate access controls. Physical security requirements are commensurate with the identified risks and all critical zones are controlled and monitored via a card access system. U.S. Bancorp has three data centers with active monitoring and security guards on-site 7x24x365. The Security Control Center monitors internal and external data center cameras in real time and retains surveillance videos for 90 days. Any occurrences or incidents on data center property will result in a notification to Corporate Security followed by subsequent investigation and documentation of the event.

Permanent access to restricted areas within buildings is granted only by group assignment and is limited to raised-floor staff, facilities staff and security staff. Any multi-use, multi-tenant buildings grant access to any U.S. Bancorp employee or third party upon manager's request.

Access is managed via access cards or badges and automated card readers. Access reports are reviewed and signed off on a quarterly basis. Both permanent and third party access cards have picture IDs. Other access requests are approved via an active and valid incident ticket documenting the issue or an approved Change record and are handled using temporary access cards. Temporary cards and usages are audited on a daily basis (Monday - Friday) requiring a visitor to sign in and provide appropriate identification. Weekend usages are reviewed the following Monday.

Equipment Protection

Equipment and information systems are protected from physical and environmental threats. Protection of equipment (including equipment used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage, including storage and disposal. Special controls are designed as needed and required to protect against physical threat, such as the appropriate electrical supplies and cabling infrastructures.

The data centers and hosting facilities have FM-200 gas suppression below raised floors and Double Pre-Action Sprinkler Systems which are both tested semi-annually. In addition, portable hand held fire extinguishers are available above raised floors and are inspected monthly and serviced annually.

Communications and Operations Management

To ensure secure operation of information and information systems, responsibilities and procedures for the management and operation of information systems are established. This includes the development of appropriate operating procedures, where necessary. Segregation of duties is implemented, where appropriate, to reduce the risk of negligent or deliberate system and information misuse.

To minimize the risk of system failures and ensure the availability of adequate capacity and resources, operational requirements of new systems are established and tested prior to acceptance and use. System and network controls are required to prevent and detect the introduction of malicious code and unauthorized mobile code. Anti-virus/malware technologies are installed and maintained on end-user computers and servers. Anti-malware software is configured to check for and implement updates at least once per day.

Encryption

U.S. Bancorp encryption standards must support the interoperability of diverse communication systems that handle the storage and transmission of information assets across the distributed environment. Standards must also apply acceptable protocols in order to meet compliance objectives for PCI standards and Information Security policies.

All websites and applications storing, or processing customer information, use encryption to protect data in transit and in storage, where feasible. Strong encryption must be used to secure the channel to any user's browser. Unknown or untrusted public encryption keys may not be relied upon to provide security. Application session IDs must be encrypted over public networks.

ISS has established processes to manage the renewal of digital Secure Sockets Layer (SSL) certificates utilized by applications for secure communication, where applicable. Digital SSL Certificates used by production applications and services are monitored to remain within their period of validity (i.e. unexpired) and have a trust chain to an ISS-recognized certificate authority.

Network Perimeter Security

U.S. Bancorp uses Intrusion Detection Systems ("IDS"), both network-based and host-based, to monitor for suspicious traffic at trust boundaries. A "trust boundary" is any place on the network where the level of trust to enter a portion of the network changes. IDS passively monitor the network to ensure perimeter firewalls and defenses are effective. U.S. Bancorp's ISS Global Monitoring and Detection team and Computer Security Incident Response Team ("CSIRT") partner with a global security services provider to provide 24x7x365 security monitoring and incident response services.

Approved security baselines have been fully documented and provide configuration requirements for all core platforms. Exceptions to the baseline are documented and approved. Secure baselines are updated annually and when the threat landscape changes. To ensure ongoing compliance to the baseline, regular control testing is performed.

Network segmentation is documented based on requirements to segregate critical or sensitive information, and utilizes firewalls with strict rule bases to control inbound and outbound traffic to that segment.

A formal process is utilized to grant network privileged access to servers and firewalls that includes management approval; this access is reviewed annually, or more frequently as required. Firewall administration is performed using a secure encrypted connection. Firewalls support stateful inspection which is also known as dynamic packet filtering. Firewall configuration is designed to deny all traffic from untrusted networks and hosts. Internet traffic utilizing protocols such as HTTP, Secure Socket Layer and authenticated VPN sessions are allowed. Changes to the firewall require authorization and changes are logged. Network logs are securely stored and reviewed regularly by monitoring staff. Network firewall rules are reviewed on a semi-annual cycle and updated as appropriate.

By default, web filtering blocks personal email sites. Email systems not controlled by U.S. Bancorp (such as Gmail or Hotmail) may only be used for U.S. Bancorp business following approval of a request establishing business rationale. Only individuals authorized to accept risk on behalf of the business line may approve such a request

Wireless access points to the U.S. Bancorp network are controlled by WPA2 or greater for encryption and authentication. Both the user and machine must be authenticated for U.S. Bancorp network access. In addition, portable automated wireless detection and prevention (WIPS) hardware/software has been deployed to identify prohibited wireless access points and rogue devices on the network. Quarterly scans are conducted on wireless access points.

Data Loss Prevention Program

The Data Loss Prevention ("DLP") Program identifies sensitive data while in motion, at rest, or in use and implements preventative controls such as blocking, notification, quarantine, or encryption. The objective of the DLP Program is to protect sensitive U.S. Bancorp and customer data from being shared with unauthorized parties.

To meet this objective, the DLP Program is responsible for scanning employee internet (HTTP and HTTPS), email (clear text and secure), employee file transfer protocol ("FTP") traffic, file and print servers, SharePoint sites, network attached storage, portable electronic media ("PEM"), cloud, and employee off-line usage (not connected to VPN). Using predefined rule sets the DLP Program will block, quarantine, or encrypt data at rest, in motion, or in use. Additional teams, including but not limited to, CSIRT, Corporate Security and the Enterprise Privacy Office, are engaged as necessary.

The DLP Program also includes the implementation and application of security policies, procedures, and technical solutions to significantly lower the risk of data leakage resulting from unauthorized or non-secure use of PEM.

Portable Electronic Media

PEM includes device types such as CD/DVDs, USB thumb drives, floppy drives and external hard drives with imaging capabilities.

Any distribution of U.S. Bancorp Customer Confidential Information on PEM devices to destinations outside of U.S. Bancorp requires explicit approval and instructions from the Privacy Office. All data classified as U.S. Bancorp Confidential or higher must be encrypted with an approved encryption solution when written to PEM devices, regardless of whether the device will remain internal to U.S. Bancorp, or whether the devices will leave U.S. Bancorp premises.

The technology used to enforce PEM controls is currently enabled via a client-server solution. By default, the technology allows Read Only rights to portable media. Access to write/copy data to portable media is granted by assigning the approved Exception Role to a user's security profile for specific types of PEM devices. A user must demonstrate a business need and receive approval to copy data to PEM devices. In the absence of prior authorization, copying data from U.S. Bancorp managed devices to a PEM device is prohibited by policy and prevented by the technical controls described in this section.

Enterprise Information Technology Service Management

U.S. Bancorp maintains an IT Service Management policy that outlines requirements for Incident, Change, Configuration, and Problem Management.

The policy covers documentation of changes; request, review and approval of proposed changes; pre-implementation testing; post-implementation testing; review for potential security impact; review for potential operational impact; and rollback procedures.

Access Control

Access to information assets is controlled based on the level of trust of the individual seeking access and the security of the access path. Internal employees and contractors using enterprise-supported computer systems within the network are more trusted than business partners connecting via the Internet; business partners are more trusted than prospective customers; etc. Access to assets within the network is reduced as the level of trust diminishes.

To ensure information confidentiality, availability, and integrity, access to information resources is provided

on a need-to-know and need-to-use basis. Where privileged access is required for those in custodial roles, such as Administrator, access is limited — to the extent possible — to the level needed within the specific custodial role of each individual. Such individuals are educated in and agree to comply with restrictions on their use of privileged authority. U.S. Bancorp uses a centralized provisioning system to manage access requests to high-risk systems, approvals and reviews for end users based on the entitlement roles assigned (i.e., job function).

U.S. Bancorp has a formal Access Control policy covering physical and electronic records and includes role-based access for all resources, unique IDs for all individuals, restrictions on the use of Generic IDs and prohibits the sharing of IDs and other access devices. U.S. Bancorp uses the centralized provisioning system to set up new accounts and grant access to high-risk systems and resources. When making modifications to user accounts, the manager of the user is required to approve a request to deactivate the user or change the access rights. Quarterly user access reviews are conducted to validate the appropriateness of user access privileges to systems, applications and networks.

Server administration access requires a second account separate from the user's primary account. All administrator level/elevated privilege accounts are locked if a maximum number of failed authentications are reached.

Privileged Access

Privileged accounts and passwords for such accounts are administered and managed internally by an Information Security Identity and Access Management team. U.S. Bancorp utilizes a privilege account and password management solution where privileged account and passwords are stored and released to authorized persons. The solution ensures that an oversight process exists to monitor accounts with privilege access and changes made by such accounts. It also reduces the likelihood of an administrator performing updates using their personal user account. Administrative account types include, but are not limited to, emergency IDs, application IDs and service accounts.

Requests for administrative accounts are submitted and approved through the centralized provisioning system. To support this high level of security, the solution is designed to ensure segregation of duties and dual control. Dual control requires two authorized individuals to approve the release of a password.

Password Requirements

A formal password policy prohibits password sharing and requires passwords to be changed at initial log in and at periodic intervals. Passwords are required to be encrypted and/or stored in a location or format which does not comprise the security of the data they protect.

Passwords must be complex enough to resist guessing or prediction:

- Passwords must include a combination of letters and numbers or special characters.
- Passwords must not be dictionary words or variations of User ID, Social Security Number, family names, pet names, or any other information readily associated with the user.
- Passwords must not be sequential or predictable variations on date or previous passwords.

Passwords for privileged, administrator and emergency accounts must be stronger (e.g., have greater length, complexity, or other password strength factors) than non-privileged accounts on the same platform. Platform-specific password controls and parameters must be documented in the platform's security baseline documentation.

Remote Access

Employees with prior management approval are permitted to remotely access the network through a secured VPN connection only allowed for employees with a business need. Access is granted through an Exception Role approved by their manager. Two-factor authentication is required for remote access to the computing environment.

Personnel with administrative rights to remotely connect to internal systems utilizing tools such as remote desktop protocol are approved and assigned the appropriate enterprise role to their security profile via the centralized provisioning management system. Remote control of internal systems is performed via U.S. Bancorp-owned equipment, using only authorized tools with approved encryption and access controls.

Information Systems Application Development and Maintenance

U.S. Bancorp's Information Security Program includes requirements throughout the application and system development life cycle (design, development, deployment, maintenance and retirement) to ensure the protection of information assets accessible through business applications. Security requirements for the design and implementation of the information systems supporting the enterprise are identified and agreed upon, where appropriate, prior to the development and/or implementation of information systems.

The Integrated Delivery Methodology ("IDM") is utilized for developing, implementing and maintaining securely configured production systems. The IDM is an integrated view of the project delivery lifecycle customized to U.S. Bancorp. It is a set of policies, guidelines, processes, templates and tools defining how projects are planned, managed and delivered.

Delivery (developing, implementing, maintaining) of secure systems to production is ensured by the combined use of the IDM as a foundation, security baselines, and other security services applicable and relevant to the type of system in question. In addition, U.S. Bancorp ISS personnel participate in the Architecture Review and Project Technology Risk Assessment processes to ensure information security requirements and controls are integrated into development and change management processes. Controls and preventative tools have been implemented to ensure that production data does not enter non-production (i.e., test) systems.

Information Security Architecture

U.S. Bancorp's ISS team works to ensure robust information security architecture. The goals of U.S. Bancorp's information security architecture are to provide:

- Defense in Depth
- Enforcement of established U.S. Bancorp policy
- Secure, authenticated access to resources
- Secure deployment of new systems and services
- Secure management of systems, infrastructure and devices
- A logical framework for identifying and investigating security incidents
- Extensibility and flexibility to adapt to changing technology and needs

Incident Event & Communications Management

Appropriate reporting procedures are identified to ensure information security events and weaknesses associated with information systems are communicated in an appropriate manner allowing timely corrective action to be taken. Responsibilities and procedures are in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement is applied to the response activities and overall management of information security incidents. As necessary,

evidence is collected for root cause analysis and extent of damage, to provide a determination of culpability or to comply with regulatory requirements. Throughout this process the integrity of the evidence is maintained to meet forensic requirements. U.S. Bancorp periodically exercises its Computer Security Incident Response Plan in accordance with regulatory requirements and to ensure procedures are adequate to manage U.S. Bancorp's response to a security incident.

The Global Monitoring and Detection team and CSIRT partner with a Global Security Services Provider to provide 24x7x365 security monitoring and incident response services. The Global Security Operations Center ("GSOC") is staffed around the clock with qualified information security experts. Internally, U.S. Bank maintains a staff of intrusion detection and Security Information and Event Management ("SIEM") experts who are on call 24x7 to investigate any incidents reported by the IDS or escalated by the GSOC provider.

U.S. Bancorp utilizes several different products to identify intrusion attempts. Standard operating procedures exist to monitor suspicious activity and identify use cases for alerting. ISS has multiple controls in place including, but not limited to, Distributed Denial-of-Service ("DDoS") monitoring, web log monitoring, IDS, and malware content controls and file integrity monitoring for high risk systems.

Logs from various security technologies are ingested by the SIEM monitoring tool to alert on anomalies and misuse cases. After an alert is triggered in the SIEM, it is investigated and automatically routed into the security case management tool. A security analyst is assigned to investigate the issue in order to determine which incident response procedure is applicable, per CSIRT guidelines.

Distributed Denial-of-Service (DDoS) Attack Protection

A DDoS attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DDoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Any time U.S. Bancorp detects potential DDoS activity, the CSIRT team works closely with the Enterprise Fraud Team to ensure fraudulent activity is detected. U.S. Bancorp is protected from DDoS attacks through the following:

- **Global Security Operations Center (GSOC):** U.S. Bancorp's 24x7 monitoring by security professionals. GSOC is the first line of support for DDoS attack notifications.
- **Global Security Monitoring and Detection:** ISS' team of security professionals in charge of system deployment, support, configuration and analysis for security systems and events.
- **Computer Security Incident Response Team:** ISS' team of cyber security professionals track down, investigate and mitigate threats.
- **Cyber Intelligence:** A variety of external information sources, including:
    - Subscription information services
    - Memberships in outside security organizations and groups
    - Personal relationships with outside security professionals
    - Participating in information sharing forums such as FS-ISAC
    - Relationships with the Federal Bureau of Investigation, the Department of Homeland Security and other governmental agencies
- **Security Tools:** A variety of software tools used to protect, detect, mitigate, block and analyze threats.
- **External DDoS Services:** U.S. Bancorp uses specialized protection services from internet service providers (e.g., AT&T, Verizon) for large-scale attack detection and mitigation strategies.

Business Continuity and Disaster Recovery

The mission of U.S. Bancorp's Business Continuity Program is to establish and support an on-going Business Continuity and Contingency Planning Program to evaluate the impact of significant events that may adversely affect customers, assets, or employees.

To obtain more information about the Business Continuity Program, you may engage the Enterprise Readiness Services Group through your U.S. Bancorp business line contact.

Compliance

U.S. Bancorp's Information Security Program aligns with industry-accepted information security practices, where possible, as provided by the NIST Cybersecurity Framework, the International Organization for Standardization ("ISO") and other applicable standards organizations.

In addition, to support U.S. Bancorp's Privacy Policy, U.S. Bancorp's Information Security Program supports compliance with applicable laws, regulations and contractual requirements. This includes, but is not limited to, the support of compliance with GLBA, SOX, PCI Security Standards and relevant international data protection standards.

U.S. Bancorp is subject to review by the Office of the Comptroller of Currency ("OCC"), the Federal Reserve Board ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), the Consumer Financial Protection Bureau ("CFPB"), the Securities Exchange Commission ("SEC"), the Financial Industry Regulatory Authority ("FINRA"), among others. In addition to being subject to external regulatory and assessment oversight, U.S. Bancorp also has an internal audit group which serves as a line of defense. U.S. Bancorp's TOS Risk and Compliance organization reports to the TOS Chief Risk Officer and provides oversight to the TOS compliance program.

Corporate Records Management

U.S. Bancorp ensures compliance with data privacy regulations through various compliance policies and procedures. Specific requirements for data/record retention and destruction are stipulated in policies. Retention periods range from three months to ten years depending on the classification of the record. The Corporate Retention Schedule outlines how long records must be retained to ensure compliance with legal, regulatory, and operational requirements. The Corporate Retention Schedule applies to all records that are created and/or maintained by the corporation, including both electronic and paper records.

Several options for secure destruction procedures exist including secure container program, destruction of records stored off-site, destruction of records stored on-site, destruction of plastic and media, and purging electronic records.

Any physical, electronic, and/or media records that have fulfilled the required retention period as defined by the Corporate Retention Schedule must be destroyed. According to the guidelines published by Information Security, all records classified as Internal, Confidential, and Customer Confidential must be securely destroyed.

Mobile

To stay current with the evolving technology and use of mobile devices, and to minimize risks inherent with their use, U.S. Bancorp's Information Security Program maintains requirements for secure use of mobile devices and development of mobile device applications. Mobile devices allowed on the network must adhere to documented mobile device policy requirements.

U.S. Bancorp utilizes mobile device management software that enables secure access to corporate email, calendar, contacts and intranet browsing on personal and corporate mobile devices.

Policies outline acceptable use and oversight procedures when personal or corporate mobile devices are used for storage, processing, or transmission of U.S. Bancorp information assets.

Privacy

U.S. Bancorp values the trust placed in it by its customers, and is committed to maintaining that trust by preserving the confidentiality of customer information in accordance with applicable law. U.S. Bancorp is committed to compliance with the U.S. Bank Consumer Privacy Pledge and with GLBA, the Fair Credit Reporting Act ("FCRA") and other legal requirements relating to privacy, protection and disclosure of customer information.

The U.S. Bancorp Privacy Policy establishes U.S. Bancorp's policy for the disclosure of nonpublic personal information. It discusses the types of customer information which may be disclosed and the circumstances under which it may be disclosed. For more information about privacy at U.S. Bancorp, please refer to www.usbank.com/privacy.

Software Security

To address the potential introduction of malicious software into the U.S. Bancorp environment, U.S. Bancorp's Information Security Program maintains requirements for regular patching of software and devices. ISS includes a team of information security professionals dedicated to providing an assessment services program that is aligned with the NIST Cybersecurity Framework.

Penetration Testing and Vulnerability Assessments are some of the core services performed by the Information Security Assessment Team.

Vulnerability Assessment

External network scans are run nightly from an approved scanning engine platform. Internal scans are conducted daily for workstations and over the weekend for servers. These scans cover the full network address space.

Penetration Testing

Testing against all external facing web and mobile applications is conducted annually as required, and after significant change in order to evaluate U.S. Bancorp's exposure to known security vulnerabilities. An application test targets a single application, including the program and its environment components. The operating system, hardware, databases, file systems and network accessibility associated with the application are assessed. The testers apply a variety of attacks against the application to determine whether vulnerabilities are present. Once the assessment is completed, significant findings must be corrected before the application is deployed to production.

Infrastructure testing is performed at least annually and includes PCI requirements. Additional testing is executed for new projects, ad-hoc requests and ATM reviews. Testing is conducted internally and by third parties. Retesting is performed to ensure vulnerability closure.

Remediation and Service Level Agreement

Information security vulnerabilities are remediated based on risk prioritization. Issues are classified as Very High, High, Moderate, and Low. Very High issues must be remediated within 30 days, High issues within 60 days, and Moderate issues within 90 days. Issues with a Low rating are resolved within a 1 year period.

Emergency rating is reserved as an escalation indicator applied to issues or incidents requiring immediate action. Documented SLA extensions may be approved when required. Exceptions to the established issue

SLA remediation process is based on management discretion, where applicable.

In addition, to address the potential introduction of malicious software into the U.S. Bancorp environment, U.S. Bancorp's Information Security Program maintains requirements for regular patching of software and devices.

U.S. Bancorp's security awareness program provides ongoing education for all U.S. Bancorp employees and associates and outlines preventative steps to block malicious software from entering U.S. Bancorp.