Request for Information (RFI)

Battery Park City Authority

Authority Background

The Battery Park City Authority, d/b/a Hugh L. Carey Battery Park City Authority, ("BPCA" or the "Authority") is a New York State public benefit corporation created pursuant to the New York State Public Authorities Law.

A summary of BPCA's structure, mission, and history, as well as the Battery Park City project area, may be viewed at: http://bpca.ny.gov/. Public information regarding BPCA's finances, budget, internal controls, guidelines, and policies, including its prompt payment policy, may be viewed at: http://bpca.ny.gov/public-information/.

RFI Terms & Conditions

This Request for Information (RFI) is issued solely for planning and market research purposes. This RFI does **not** constitute a solicitation, procurement, request for proposals, or invitation to bid, and **will not result in a contract, award, or payment**. Responses will not be evaluated or scored. Furthermore, The Authority will not rank, shortlist, or otherwise evaluate respondents based on RFI submissions.

No costs incurred in responding to this RFI will be reimbursed.

The Authority reserves the right, in its sole discretion, to modify, amend, clarify, extend, suspend, or cancel this RFI, in whole or in part, and to request additional or clarifying information from one or more respondents, at any time.

If the Authority elects to pursue a future procurement, it will be conducted in accordance with applicable laws and policies and will be open to all qualified firms, regardless of RFI participation.

Overview of Request

Through this RFI, BPCA is seeking to better understand the current technology market and vendor landscape related to software that can automate certain tasks that are currently managed primarily using spreadsheets. Information received may be used to refine internal planning documents, develop future procurement strategies, or inform potential scope, schedule, and budget considerations.

The Authority is seeking to collect evaluation data from software vendors to determine market viability, vendor potential, and procurement options for the following use cases:

Use Case 1	**Capital Expenditure Tracking and Reporting and Bond Fund Drawdowns.** Tracking of expenditures by bond fund by bond issuance, including but not limited to bond fund expenditures to date and bond funds remaining, capital project payments, bond drawdown requests, bond fund expenditures by bond fund by specified project, construction in process, capital expenditure limits, bond fund budget to actual

	reporting, bond fund sustainability reporting, and contract spending to Settlement Agreements and stakeholder approvals.
Use Case 2	**PILOT and Abatement Processing.** Generating billing, recording payments, and tracking outstanding receivables for Payment in Lieu of Taxes (PILOT) and applicable abatements related to properties on land owned by BPCA based on New York City Department of Finance property tax assessments and abatements and relevant applicable tax rates.
Use Case 3	**Investment Reconciliation and Reporting.** Tracking of cash and investment activity and balances, including but not limited to investment reconciliations, investment income, fair value, investment-related cash flows, and debt service activity. *Note: BPCA currently has one custodian, two investment managers, and is limited to investments permitted under its investment guidelines.*

Vendors may respond to any or all of the use cases.

BPCA's current general ledger software is Microsoft Dynamics GP. BPCA anticipates that the solution(s) implemented for the above use cases will be used with both Microsoft Dynamics GP (for which support is scheduled to end after December 31, 2029) and its successor general ledger system, which has not yet been selected.

For all three use cases, it is anticipated that the number of users will be limited (20 or fewer).

Section 1. An RFI response should include the following:

The vendor is requested to return an RFI response to the BPCA's consultant and authorized representative, MFR Consultants, Inc. by **Friday, January 30, 2026 at 5 pm EST** to BPCAVendors@MFRConsultants.com. Other Key Dates are available in **Section 3**. The RFI process is BPCA's opportunity to ask questions to the vendor about requirements and software solution(s) and to learn more about how to procure software solution(s). General questions follow in this section. Specific questions regarding requirements to which the vendor must respond are in **Section 2** of this RFI.

RFI responses shall include a cover letter identifying the respondent's primary point of contact, including the individual's name, title, and contact information, whom BPCA may contact regarding this RFI.

General Questions (Applicable to all Use Cases)

1. Identify to which of the use cases your response applies. If multiple use cases are addressed, what , if any, are the potential benefits of using the same software across multiple use cases?
2. Details about the vendor's company strategy and software vision as well as the organization's history, size and ownership.
3. Details about recent (within the past five (5) years) examples of similar implementations, especially in relation to NYS or NYC government entities.
4. Details about vendor viability and economic standing and any vendor or government issues, including lawsuits or investigations, that have occurred either in the past ten years or are under current investigation or scrutiny in NYS or NYC.
5. Please indicate whether your company is a New-York State certified Minority-Owned Business Enterprise ("MBE"), Women-Owned Business Enterprise ("WBE"), and/or Service-Disabled Veteran-Owned Business Enterprise ("SDVOB").
6. Overview of the solution(s) offered, including features and functionality, and what makes the solution(s) superior to others in the market.
7. Details of the solution(s)' technical architecture and history (ex. COTS product, built on low-code platform, SaaS).
8. Details about ongoing support offered for the solution(s).
9. Approach to migration of historical data.

10. Overview of the implementation process and projected time necessary for implementation.
11. Details about cloud hosting capabilities and relevant security and compliance standards (ex. SOC 2, FedRAMP).
12. Details about your upgrade management approach, specifically addressing: the release history and roadmap (past two years and next two years), deployment methodology, client communication protocols, system availability during upgrades, rollback capabilities, and any costs or client responsibilities associated with version updates.
13. Details about the product cost and procurement: what is the vendor's pricing model, what are up-front implementation costs, what type of annual fees are necessary for maintenance and support, and what, if any, NYS or Federal contracting vehicles are available for procurement of the product (please include contract number where applicable).

Section 2. Specific RFI Questions for Vendor Responses

Please complete the relevant attached Appendix **for each use case for which you are responding** and return as part of your vendor response. If you are not responding to a use case, there is no need to include the related Appendix in your response

Section 3. Next Steps and Key Dates

BPCA will receive and review all vendor responses to its RFI questionnaire. The RFI is a critical tool that will assist BPCA with developing next steps related to the procurement of software focused on automating certain tasks that are currently managed primarily using spreadsheets. It will allow for the comparison of features and functionality among various vendor solutions and allow BPCA to build a business case for moving forward with procurement and implementation.

Key Date Milestone	Day/Month/Year	Time
Release of RFI	Monday January 12, 2026	-
Questions Due from Potential Vendors (to: BPCAVendors@MFRConsultants.com)	Tuesday, January 20, 2026	5:00 pm EST
Answers Provided by BPCA to Vendor Questions	Friday, January 23, 2026	-
Responses to RFI due from Vendors	Friday, January 30, 2026	5:00 pm EST

BPCA appreciates the time and expertise vendors invest in responding to this RFI. As we work to modernize our internal systems, your input helps us make informed planning decisions and identify the right solution(s) for our agency's needs.

BPCA representatives may request that vendors provide a presentation and real-time demonstration of the current production version demonstration of their solution(s) for further clarification of their response or to define their potential capability to meet the requirements. However, BPCA may move forward with a solicitation without demonstrations or presentations.

Appendix 1. Use Case #1: Capital Expenditure Tracking and Reporting and Bond Fund Drawdowns

1.1 Functional Requirements

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
1.1.1	Project Setup & Structure	Ability to define project charters, funding sources, timelines, departments, etc.	MEDIUM		
1.1.2	Project-Specific Tracking	Modules for project-specific capital planning and expenditure tracking	HIGH		
1.1.3	Project Close-Out	Ability to close-out a project and transfer totals to appropriate account to track as a capital asset and flag for depreciation	HIGH		
1.1.4	Project Close-Out	Project close out at both project and sub-project (Reach) level	HIGH		
1.1.5	Project Close-Out	Detailed information and transfers at the sub and full-project level.	HIGH		
1.1.6	Retainage	Support retainage amounts and payout upon project completion	HIGH		
1.1.7	Multi-Year Budgeting	Multi-year budgeting that supports adjustments and amendments	HIGH		
1.1.8	Funding Source Management	Ability to assign multiple fund sources to a single project (i.e., bonds, grants, general fund, etc.)	HIGH		
1.1.9	Drawdown Tracking	Ability to track bond disbursements, timing, and restrictions	HIGH		
1.1.10	Allowance Tracking	Ability to track allowances, including usage, increases, and the relationship with work orders (i.e., work orders reducing allowances).	HIGH		
1.1.11	Work Orders & Allowances	Ability to reduce work order amounts and add differences back to contract allowances.	HIGH		
1.1.12	Work Order Tracking	Tracking abilities at the work order level including against allowances and contracts.	HIGH		
1.1.13	Amendment Tracking	Tracking ability at the amendment (contract amount) level, including approved use of do-not-exceed amounts	HIGH		
1.1.14	Cost Tracking	Real-time visibility of planned, actual, and committed costs	HIGH		
1.1.15	Encumbrance Integration	Track commitments throughout the project/PO lifecycle	LOW		
1.1.16	Report Generation	Report generation by fund, project, fiscal year, funding source, and expenditure type	HIGH		
1.1.17	Historical Audit Trail	Maintenance of a traceable history for every transaction	MEDIUM		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

Appendix 1. Use Case #1: Capital Expenditure Tracking and Reporting and Bond Fund Drawdowns

1.1.18	Approval Workflows	Configurable approvals for capital budget requests, amendments, reimbursements, drawdowns, reallocations, etc. (All deliverables that must route through approval workflows)	MEDIUM		
1.1.19	Approval Workflows	Roles-based permissions built into the workflow.	HIGH		
1.1.20	Approval Workflows	Ability to automatically generate approval letters based on drawdown data and route for approvals.	MEDIUM		
1.1.21	Alerts & Notifications	Automated notifications when approaching budget thresholds, bond fund expiration, compliance deadlines, etc.	MEDIUM		

1.2 Security, Control, & Audit

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
1.2.1	Role-Based Access	Ensure role-based permissions to access and modify critical data.	HIGH		
1.2.2	Separation of Duties	Clear distinctions between those initiating, approving, posting, etc.	HIGH		
1.2.3	Audit Logs	Full audit-ready logs for drawdowns and capital transactions that include attached or linked documentation	HIGH		
1.2.4	Auditing System Integrations	Ability to export logs and reports for use with external auditing systems	MEDIUM		
1.2.5	Abide by the policies of BPCA IT Department	Abide by BPCA's Cybersecurity requirements annexed to this RFI as **Appendix 4**	MEDIUM		
1.2.6	Data Lockout	Historical Data Lockout to prevent retroactive changes once a drawdown week has been finalized.	HIGH		
1.2.7	Data Adjustments	Audit trails and approvals for adjusting entries (re: Historical Data Lockout)	HIGH		

1.3. Reporting & Analytics

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
1.3.1	Utilization Summaries	Readily available utilization summaries for bond funds, as well as real-time fund balances.	MEDIUM		
1.3.2	Project Portfolio	Configurable, user-friendly dashboard features that supports real-time data. For example, a project portfolio dashboard to display budget versus actual versus committed	MEDIUM		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

Appendix 1. Use Case #1: Capital Expenditure Tracking and Reporting and Bond Fund Drawdowns

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
1.3.3	Dashboard Integration	Ability to integrate with the future-state, comprehensive financial dashboard system.	HIGH		
1.3.4	Role-Based Reporting Metrics	Dashboards with access restrictions for specified user roles (i.e., user-based entitlements)	MEDIUM		
1.3.5	Projected Forecasts	Forecast of capital expenditures and drawdowns	MEDIUM		
1.3.6	Project Phase Views	Gantt or milestone views for capital project phases	LOW		
1.3.7	GASB Compliance	GASB-compliant capital asset tracking	MEDIUM		
1.3.8	Configurable Reporting	Dynamic reporting that can categorize data into various classes.	HIGH		
1.3.9	Periodic Reporting	Support periodic reporting, including weekly bond drawdown reports	HIGH		
1.3.10	Historical Data	Support historical drawdown reports, including items and drawdown weeks that have already been completed.	HIGH		

1.4. Integration

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
1.4.1	ERP Integrations	Considering the eventual transition to a new ERP system, the solution should have a wide array of integrations and configurations available to connect with ERP systems.	MEDIUM		
1.4.2	GP Integration	With the current financial system being GP, the solution should support bidirectional data flow integrations to import scheduled capital transactions and post financial entries back into GP	HIGH		
1.4.3	Procurement Software	Data from POs, contracts, vendor payments, etc.	MEDIUM		
1.4.4	Treasury/Bond Management	Tools containing fund balances, draw schedules, etc.	MEDIUM		
1.4.5	GIS/Asset Systems	Tag capital projects to physical assets/locations, if applicable	LOW		
1.4.6	Optionality for Integration with Procore.	There is a possibility that useful data is present in Procore, but there should not be an automatic live data pull that could impact finance's numbers. There should be an option for integration with limitations and controls.	LOW		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

Appendix 1. Use Case #1: Capital Expenditure Tracking and Reporting and Bond Fund Drawdowns

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
1.4.7	Support for 2-way Data Flows	2-way data flow support, allowing bond-related information to feed in from the general ledger, and for relevant outputs to feed back.	MEDIUM		

1.5 Implementation

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
1.5.1	Cloud-Based Deployment	Solution should ideally be cloud-hosted for scalability, security, and back-up abilities.	MEDIUM		
1.5.2	Data Migration	Data import/migration services from legacy spreadsheets and financial systems	HIGH		
1.5.3	OpenAPI or an Accessible API	OpenAPI or accessible API availability for system-to-system communication	MEDIUM		
1.5.4	Scheduled Exports/Ad Hoc Queries	Support for scheduled exports in multiple formats (Excel, CSV, PDF), as well as ad hoc data queries	HIGH		
1.5.5	Configurable Data Structure	Configurable chart of accounts and fund structure	HIGH		
1.5.6	Robust System Documentation	Robust system and workflow documentation to support onboarding and business continuity	HIGH		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

Appendix 2. Use Case #2: PILOT and Abatement Processing

2.1 Functional Requirements

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
2.1.1	Agreement Management	Track PILOT/abatement agreements by parcel, property, or owner	HIGH		
2.1.2	Agreement Management	Ability to store agreement terms, schedules, conditions, and effective periods	MEDIUM		
2.1.3	Billing Engine	Generate PILOT/Abatement invoices or billing notices based on fixed amounts or agreed-upon schedules	HIGH		
2.1.4	Billing Flexibility	Ability to add additional fees to PILOT billing, including base rent and CFM	HIGH		
2.1.5	Cash Receipts	Support payment receipt after billing	HIGH		
2.1.6	Payment Application	Apply payments to specific billing periods or obligations	HIGH		
2.1.7	Payment Support	Support partial payments, prepayments, and write-offs	MEDIUM		
2.1.8	Schedule Tracking	Support custom payment frequencies (monthly, quarterly, annual, etc.)	MEDIUM		
2.1.9	Due Dates	Auto-calculate due dates based on agreement terms	MEDIUM		
2.1.10	Exemption & Reduction Rules	Apply abatements by property class, use, location, or Commercial/Residential distinction	MEDIUM		
2.1.11	Automated Reductions	Automate the application of yearly reductions on applicable properties	HIGH		
2.1.12	Automate Site Information Entry	Automated application of site information and internal/external labels to uploaded/imported assessment data, including commercial/residential distinction	HIGH		
2.1.13	Amendments with Logging	Allow amendments to agreements with audit logs and version control	HIGH		
2.1.14	Performance-Based Compliance	Track conditions tied to KPIs, if applicable	LOW		
2.1.15	Notifications & Alerts	Notify internal staff and external stakeholders of upcoming obligations, payments, or expiring agreements	MEDIUM		
2.1.16	Lien/Collection Integration	Flag non-payment and initiate escalation procedures (if applicable)	LOW		
2.1.17	Audit Support	Maintain full transaction and decision trail for audits and legal reviews	HIGH		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

Appendix 2. Use Case #2: PILOT and Abatement Processing

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
2.1.18	Adjustments	Support workflows for revisiting or adjusting abatements due to compliance or renegotiation	MEDIUM		
2.1.19	Bulk Uploads	Support bulk uploads of assessment information	MEDIUM		
2.1.20	Tax Rates	Ability to select given period and have applicable rates automatically applied to the calculations	HIGH		
2.1.21	Monthly Reconciliation	Support monthly reconciliation of billed amounts versus revenue received	HIGH		
2.1.22	Automated Calculations	Automated calculations to derive necessary figures (i.e., billable amounts)	HIGH		

2.2 Security, Control, & Audit

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
2.2.1	Role-Based Access	Role-based access to restrict who can view, edit, and approve PILOT & Abatement records	HIGH		
2.2.2	Separated Access	Separate access for agreement negotiation, payment processing, legal or policy review, etc.	LOW		
2.2.3	External Access	Optionality for read-only or time-limited external access (i.e., auditors, public users)	MEDIUM		
2.2.4	Complete Audit Trails	Maintain complete audit trails of agreement changes, payment history, billing adjustments, compliance determinations, etc.	HIGH		
2.2.5	Internal Controls	Support internal control workflows (i.e., two-step review for abatement approval or extension)	HIGH		
2.2.6	Approval Workflows	Configurable, role-based approval workflows built-into the system	HIGH		

2.3. Reporting & Analytics

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
2.3.1	Agreement Inventory Report	Summary of active, expired, and upcoming PILOT/abatement agreements	MEDIUM		
2.3.2	Billing & Collections Report	Amounts billed, paid, outstanding, and delinquent per entity/property	HIGH		
2.3.3	Revenue Impact Report	Estimated foregone tax revenue from abatements; PILOT payments versus fill assessment	MEDIUM		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

Appendix 2. Use Case #2: PILOT and Abatement Processing

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
2.3.4	Public Transparency Report	Exportable summary showing PILOT recipients, amounts, and term lengths (as required by law)	HIGH		
2.3.5	Adjustments Report	Track frequency, outcome, and financial impact of changes	LOW		
2.3.6	Summary Report	Exportable, configurable summary report to showcase necessary information	HIGH		
2.3.7	Detail Report	Exportable, configurable detail report displaying data and calculations in various groupings	HIGH		
2.3.8	Base Rent & CFM	Ability to report on Base Rents and CFM	HIGH		
2.3.9	Building Reports	Ability to generate various reports by building	HIGH		
2.3.10	Organizational Reports	Flexibility to configure & generate current organizational reporting for various periods (i.e., Monthly, Quarterly, etc.), including: • Cash Receipts • Assessment Billings • Billed vs Received • Budget to Actual This reporting should include supplementary reports and calculations necessary to derive reported figures, as applicable.	HIGH		
2.3.11	Compliance Dashboard	Visual status of agreement conditions and performance triggers	LOW		
2.3.12	Export Formats	Ability to export in PDF, Excel, and open data formats (CSV or JSON) for cross-departmental use	HIGH		

2.4. Integration

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
2.4.1	Tax Assessment System	Sync assessed values, parcel data, and taxable entities	HIGH		
2.4.2	ERP Integrations	Considering the eventual transition to a new ERP system, the solution should have a wide array of integrations and configurations available to connect with ERP systems.	HIGH		
2.4.3	GP Integration	With the current financial system being GP, the solution should support integrations to post revenues and abatement credits into GP	MEDIUM		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

Appendix 2. Use Case #2: PILOT and Abatement Processing

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
2.4.4	Document Management Integrations	If the system cannot do this, support integrations to store signed agreements, compliance reports, correspondence, and legal notices	MEDIUM		
2.4.5	Collections/Enforcement Systems	Optionality to integrate with collection tracking modules (i.e., Condo Deficiency System)	HIGH		

2.5 Implementation

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
2.5.1	Cloud-Based Deployment	Solution should ideally be cloud-hosted for scalability, security, and back-up abilities.	MEDIUM		
2.5.2	Configurable Data Structures	Configurable data structures for agreement types, billing formulas, and compliance rules	HIGH		
2.5.3	Ad Hoc Reporting/Query	Ad hoc reporting and query builder to filter by site, lot, term, payment status, etc.	HIGH		
2.5.4	Bulk Import Capability	Bulk import capability for legacy agreement data and historical payments	HIGH		
2.5.5	Batch Generation	Batch generation of billing notices and compliance reminders	MEDIUM		
2.5.6	Role-Based Dashboards	Role-based dashboards tailored to finance, legal, and program managers	HIGH		
2.5.7	API Support	Support for APIs or scheduled data exchange (i.e., sync to ERP nightly)	HIGH		
2.5.8	Scalable for Future Programs	Scalable to add new PILOT or incentive programs in the future	HIGH		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

Appendix 3. Use Case #3: Investment Reconciliation and Reporting

3.1 Functional Requirements

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
3.1.1	Portfolio Management	Tag investments by fund, project, type, advisor, and custodian	MEDIUM		
3.1.2	Trade Entry	Support manual or batch trade entry, especially for trades executed by advisors	HIGH		
3.1.3	Retroactive Approvals	Record execution date versus approval date, requiring justification and maintaining audit trails	MEDIUM		
3.1.4	Approval Workflows	Custom approval workflows for trade approvals and reconciliation sign-off	HIGH		
3.1.5	Interest Tracking	Calculate and track interest income and receivables across all securities	HIGH		
3.1.6	Reconciliation Against Records	Match positions, income, and transactions against custodial (or advisor) records, allowing for exceptions	HIGH		
3.1.7	Automated Reconciliations	Automated reconciliations that compare statements of activities against executed investment letters and reports	HIGH		
3.1.8	Maintaining Values	Maintain book versus market valuations, supporting pricing feeds and manual entries	HIGH		
3.1.9	GASB Footnote Generation	Support footnotes for GASB 31, 40, and 72, including credit risk, maturity buckets, valuation levels (see requirements D.16, D.17, and D.18)	HIGH		
3.1.10	Policy Compliance	Rule-based monitoring for maturity limits, credit ratings, issuer/sector exposure	LOW		
3.1.11	Exception Handling	Alert and report exceptions, including policy violations, unmatched transactions, delayed approvals, etc.	MEDIUM		
3.1.12	Audit Trails	Log all transactions, changes, and approvals with user/timestamp metadata	HIGH		

3.2 Security, Control, & Audit

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
3.2.1	Role-Based Access	Role-based access control to restrict visibility and action by user role (i.e., trade entry, approver, auditor)	HIGH		
3.2.2	External Parties	Read-only access for auditors and external reviewers	LOW		
3.2.3	Data Restriction	Ability to restrict data by investment type, fund, or advisor based on role	HIGH		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

Appendix 3. Use Case #3: Investment Reconciliation and Reporting

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
3.2.4	Separation of Duties	Enforce separation of duties between execution, approval, and reconciliation	HIGH		
3.2.5	Audit Trail	Full audit trail for all activity with timestamped logs, including trade entry, approvals, changes, exceptions, etc.	HIGH		
3.2.6	Version Control	Version control for all records with timestamped approval logs	HIGH		
3.2.7	Approval Workflow	Retroactive approval workflow with required rationale and timestamp logging	LOW		
3.2.8	Confirmation Approval	Optionality to: • Automatically generate trade letters, based on confirmations, and route for approvals • Define a non-letter-based workflow for wrap around trade approvals (i.e., eliminate repurposing information into letters)	HIGH		
3.2.9	Trade Aggregation	Optionality in the aggregation period for trade approvals (i.e., currently aggregated per week, but could be more rapid)	HIGH		

3.3. Reporting & Analytics

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
3.3.1	Portfolio Summary Reports	Portfolio summary reporting, including book versus market value, duration, yield, income earned, etc.	HIGH		
3.3.2	Accrued Interest & Income Reports	Track expected and received interest, including calculating and reconciling interest income per investment/fund	HIGH		
3.3.3	Reconciliation Reports	Matched/unmatched positions and transaction summaries	MEDIUM		
3.3.4	Policy Compliance Reports	Highlight exposure, violations, limits exceeded	MEDIUM		
3.3.5	Advisor Oversight Reports	Group trades and performance by investment advisor	HIGH		
3.3.6	Reporting Format	Ability to export/run monthly reports directly in Excel	HIGH		
3.3.7	Gain/Loss	Reporting on realized gain/loss at each sale or maturity.	HIGH		
3.3.8	Account Tracking	Tracking abilities to ensure securities are in current accounts	HIGH		
3.3.9	Portfolio Tracking	Tracking abilities at the portfolio level to maintain cost basis over time	HIGH		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

Appendix 3. Use Case #3: Investment Reconciliation and Reporting

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
3.3.10	Maturity Tracking	Ability to track securities over multiple years (i.e., those purchased years ago that have not matured.)	HIGH		
3.3.11	Tracking Identifiers	Additional levels of identifiers (i.e., Those with the same CUSIP use portfolio numbers as the first level of identification)	HIGH		
3.3.12	Fair Value Analysis	Ability to report at both cost basis and fair value basis	HIGH		
3.3.13	Fair Value Schedule	Ability to pull values from statement to generate fair value adjustment numbers, update schedules, and book entries	HIGH		
3.3.14	Trade Register	Register showing trade details, advisor, execution versus approval status, etc.	HIGH		
3.3.15	Maturity Ladder	Visualize maturing investments by time bucket	HIGH		
3.3.16	GASB Footnote Reports	GASB 31 footnote report for book versus fair value	MEDIUM		
3.3.17	GASB Footnote Reports	GASB 40 footnote report for credit risk, interest rate risk, and concentration of credit risk	MEDIUM		
3.3.18	GASB Footnote Reports	GASB 72 footnote report for fair value hierarchy at levels 1, 2, and 3	MEDIUM		
3.3.19	Export Options & Queries	Optionality to export reports in Excel, Word, PDF, etc. Allow for custom, ad hoc queries	HIGH		
3.3.20	Interactive Dashboards	Interactive dashboards by user role (investment accountant, controller, etc.)	MEDIUM		

3.4. Integration

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
3.4.1	Custodial Integration	Accept daily/monthly data from custodian in formats including, SWIFT, SFTP, Excel/CSV, or API through Nexen	HIGH		
3.4.2	Advisor Trade Uploads/Integration	Accept standardized templates from investment advisors for trade reconciliation through upload or integration	HIGH		
3.4.3	ERP Integrations	Support integrations with a variety of ERP systems considering the BPCA will be transitioning in the near future. This should support journal entry exports for investments and accruals	HIGH		
3.4.4	GP GL Integration	The system should integrate with GP (the current financial system) to support data exports/imports	MEDIUM		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

Appendix 3. Use Case #3: Investment Reconciliation and Reporting

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
3.4.5	Document Management Integration	If document workflows are not contained within the system, support integrations with document management systems to attach broker confirmations, policy documents, and audit evidence	LOW		
3.4.6	Pricing Feeds Integration	Ability to import pricing data from applicable systems, including custodian/advisor systems or manual uploads (i.e., where treasury data is available)	MEDIUM		
3.4.7	Fair Value Integration	Ability to directly import Fair Value data	HIGH		

3.5 Implementation

ID	Requirement	Details	Priority	Ability to Deliver*	Comments
3.5.1	Cloud-Based Deployment	Preference for cloud-based deployment that supports SOC2 or equivalent compliance	MEDIUM		
3.5.2	User-Friendly Configuration	Allow for configurations including user-defined fields, tags, and policy rules	HIGH		
3.5.3	Batch Uploads	Batch upload capabilities for trades, prices, and custodial records	HIGH		
3.5.4	Scheduled Imports/Generation	Scheduled imports and report generation	MEDIUM		
3.5.5	Reporting & Queries	Ad hoc reporting/query builder, with drag-and-drop or SQL-like GUI functionality	HIGH		
3.5.6	Cross-Reporting	Multi-entity or multi-fund support with cross-reporting capabilities	HIGH		
3.5.7	Audit Logs	Exportable audit logs for review or archival	HIGH		
3.5.8	Scalable Solution	Scalable to accommodate growing number of advisors, funds, or assets	HIGH		
3.5.9	IT Dependency	Minimal IT dependency for regular operations and maintenance	HIGH		

* Please indicate: **YES, YES (with Customization) – please describe in Comments, or NO**

BPCA CYBERSECURITY REQUIREMENTS

1. PURPOSE:

To establish Cyber Security requirements and guidelines that can be used consistently to ensure a secure network for the Battery Park City Authority ("BPCA" or the "Authority").

2. II. SCOPE:

This procedure applies to all BPCA staff and affiliates (e.g., contractors, vendors, solution providers), which have access to or manage BPCA information and systems. This policy encompasses all systems (in the cloud, offsite or on-premises), automated and manual, for which the Battery Park City Authority has administrative responsibility, including systems managed or hosted by third parties on behalf of the Authority and addresses all information, regardless of the form or format, which is created or used in support of business and operational activities of the Authority.

3. Cloud Requirements, contractor shall:

a. Cloud services provider proposed for housing BPCA data offsite shall be compliant with the following standards: ISO27001, ISO27017, ISO27018, SOC2 Type 2 and FedRAMP.
b. Ensure that BPCA data and processing is isolated from other customers.
c. Ensure that BPCA data remain within the continental United States at all times.

4. General Requirements, contractor shall:

a. PCI DSS (Payment Card Industry Data Security Standards) compliance shall be required when accepting or processing payment cards or handling Personally Identifiable Information.
b. ICS/SCADA environments, including onboard or vehicle systems, shall be designed in accordance to NIST SP 800-82 R2.
c. Securely destroy BPCA data in all formats (e.g., Server, Disk, CD/DVD, backup tape, and paper) when requested by the Authority. Data shall be permanently deleted and be unrecoverable. Certificates of destruction must be retained by Vendor and made available to BPCA upon request.
d. All contractors with access to BPCA data must sign and submit a non-disclosure agreement (NDA) which NDA shall specify that in no event shall any BPCA data be disclosed to any entity not covered by the NDA.

5. Operating Systems, contractor shall:

a. Use only commercially supported Operating Systems and maintain timely security patching.
b. Configure Operating Systems based on the CIS Hardening Standard, (https://www.cisecurity.org/cisbenchmarks) with non-essential services disabled. Exceptions to the Hardening standard must be documented and approved through the Change Control process or BPCA's IT department.
c. Configure the Operating System with BPCA specific standards for local and network password management (Password Aging, Password Expiration, Password Length, Multifactor, etc.).
d. Use volume encryption for Operating System and all volumes storing data.
e. Ensure that Operating System protection tools are installed and centrally managed to mitigate exploits, malware, malicious code, or viruses.
f. Ensure that Clear-text and weak cipher protocols are disabled and not used for data transfer
g. Ensure that Network Interface Cards are not multi-homed or used for routing.
h. Ensure that Inbound internet sourced traffic to systems is terminated at a DMZ.
i. Ensure that Internet-bound traffic from system utilizes a proxy or other form of security inspection.

j. Ensure that Split tunneling is not enabled while connected to the BPCA network (access to non-BPCA internet while connected to BPCA resources).
k. Ensure that Operating System is registered with appropriate records in IP Address Management, DNS, and with BPCA IT.

6. **Authentication, contractor shall:**
   a. Develop a plan for identity management consisting of role-based user accounts which isolate access to BPCA data. All account activities, to include role changes, must be logged.
   b. Ensure that all credentials are not passed over the network in clear-text or with weak encryption ciphers.
   c. Use secure, dedicated, and privileged-access workstation (PAW) to administer BPCA Systems.
   d. Use Multifactor Authentication for administrative users on cloud/internet-facing BPCA System components.
   e. Integrate application authentication into Identity Management Solution (IDMS) via SAML 2.0.
   f. Ensure that users utilize Multifactor Authentication to access the system(s) and application(s) via the Internet.
   g. Ensure accounts not accessed within 90 days are either automatically disabled or have their passwords expired.
   h. Perform annual role reviews of active accounts (applicable to non-BPCA managed environments).

7. **Encryption, contractor shall:**
   a. Ensure that all encryption methods for data-in-motion and data-at-rest meet or exceed FIPS-140/NIST standards.
   b. Ensure that data transfers between hosts are encrypted.
   c. Ensure that OS/data volumes in the cloud are encrypted.
   d. Ensure that data files that contain PII are encrypted.
   e. Ensure that PII data residing in databases are encrypted.
   f. Ensure data backups are encrypted.
   g. Ensure that encryption key management system is on a separate platform from the data and its application (keys are not stored with data).
   h. Provide exclusive ownership of encryption keys to BPCA.

8. **Networking, contractor shall:**
   a. Ensure that Intrusion Prevention Systems are implemented on networks with connectivity to the Internet and networks with sensitivity zones and/or trust boundaries.
   b. Ensure that public cellular-based solutions employ a private cellular cloud meeting segregation requirements outlined in this document.
   c. Ensure that systems are deployed in a multi-tier firewall segmented network architecture
      - User Workstations
      - Operational application/system servers
      - Backup and Storage
      - Development
      - QA and Testing
      - Programmable Logic Controllers
      - Sensors
      - Wireless Systems

- Internet of Things (IOT)

d. Ensure that listening ports/services are protected by firewalls and filters to inspect traffic between segments and hosts.
e. Ensure that management of systems are restricted through firewall or access control lists over secure protocols and that they are managed over a secure network or VPN.
f. Perform annual firewall rule audits (applicable to non-BPCA managed environments).
g. Disable unused functions on network devices.
h. Implement a tiered firewalled architecture that is restricted to communications where all traffic is monitored, alarmed, and filtered.
i. Implement appropriate security controls to ensure the integrity and confidentiality of data flowing across the network.

9. Control System End Devices, contractor shall:

a. Provide physical and cyber security features including, but not limited to, authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.
b. Clearly identify the physical and cyber security features and provide the methodologies for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.
c. Verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.
d. Remove or disable all software components that are not required for the operation and maintenance of the device.
e. Provide, within a pre-negotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

10. Vulnerability Management, contractor shall:

a. Ensure that all system components (Hardware, Software, Hypervisor, Operating System, Database, Network/Firewall Equipment, etc.) are managed within a vulnerability management and patching program. Documentation and reporting on program activities and gaps must be made available to BPCA upon request.
b. Ensure that third-party security assessments are conducted on an annual basis for the system and provided to the Authority.
c. Ensure that periodic penetration tests are performed to assess system configuration and security vulnerabilities for remediation.
d. Submit biannual security reports to BPCA detailing vulnerability management, penetration tests, security incidents, and enhancements and changes to the infrastructure.
e. Keep all system components updated to vendor supported releases and maintain current security updates. To the extent possible, critical patches should be installed within one week of patch release. Deviations must be documented and a "plan to cure" developed to bring the patch level current.
f. Allow BPCA to conduct an independent Penetration Test upon request.

11. Incident Management, contractor shall:

a. Submit and document an Incident Management Plan to guide the response and recovery process in the event of a security breach.
b. Ensure that all security incidents are promptly reported to the Authority. Any incident involving compromised Personally Identifiable Information (PII), must be reported within 1 hour of detection.
c. Fully cooperate through technical assistance and logs to investigate security incidents when required.

12. Mobile, contractor shall:

a. Deploy a centralized mobile device management solution to manage all mobile devices permitted to store, transmit or process BPCA data.
b. Ensure the use of encryption for devices permitted to store, transmit or process BPCA data.
c. Ensure that password policies, applicable to mobile devices are documented and enforced.

13. Application Security, contractor shall:

a. Ensure that any software delivered to BPCA adheres to industry standards and best practices for architectural standardization, secure coding standards, and security testing procedures.
b. Employ threat modeling techniques in the design and assessment phases of the Software Development Life Cycle (SDLC) for systems delivered to BPCA, and incorporate realistic security scenarios during application security assessment.
c. Perform static analysis scans as part of security-focused reviews and validation of the use of secure coding standards.
d. Perform dynamic scans as part of applications testing, production deployment, regular health checks, change management requests and audits.
e. Conduct overall application and systems cybersecurity assessment, which may include penetration testing, evaluating external infrastructure, perimeter assessment, web application testing, internal network assessments, wireless security testing and red teaming.
f. Have a notification and alert process for vulnerabilities, as well as a documented response plan for addressing newly identified vulnerabilities. Remediation may include patches, updates, security fixes, component replacements, or other steps as dictated by the situation.
g. Ensure that any open-source, 3rd-party, commercial components used as part of any deliverables have been validated through security assessments and remain as such during their operational use.
h. Ensure that application APIs have been validated through security assessments and security measures are in place to protect both data and application. Such measures may include gateways, secure protocol, authentication, and keys.
i. Use, at minimum, industry standard security logging standard for the Applications, and ensure that logging profiles are available and configurable to log events at various levels for various purposes (debugging, verbose, illegal requests, failed access, etc.)

14. NYS Policy Compliance, contractor shall:

a. Comply with applicable New York State Policies, Standards and Procedures as listed at: https://its.ny.gov/eiso/policies/security
b. Comply with Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules.
c. Comply with Federal Risk and Authorization Management Program (FedRAMP) if cloud computing is utilized (http://www.gsa.gov/portal/category/102371).
d. Comply with all applicable NYS laws and regulations related to privacy protections.

APPENDIX 4: Cybersecurity Requirements

15. **Privacy and Security Plan, contractor shall:**
    a. Without written authorization from the Authority, shall not divulge to third parties any confidential information obtained by the Contractor or its agents, distributors, resellers, subcontractors, officers or employees in the course of performing contract work, including, but not limited to, security procedures, business operations information or commercial proprietary information.
    b. Develop a security and privacy plan in accordance with attachment 1-ITSEC. The Contractor will also be expected to complete the System Security Plan (SSP) based on NIST 800-53 security and privacy controls and complete the section for each control indicating how the control is met.

APPENDIX 4: Cybersecurity Requirements

TERMS & ABBREVIATIONS	
CIS	Center for Internet Security

FedRAMP	The Federal Risk and Authorization Management Program. Governmentwide program that provides a standardized approach to security.
Government Compliant	Cloud services that are compliant for hosting U.S. Federal, State and local agencies and are isolated from commercial, public and other cloud services. (e.g., AWS GovCloud; Azure Government).
ISO 271001	Specification for information security management system (ISMS). ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management program.
ISO 271017	Provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards.
ISO 271018	Code of practice that focuses on protection of personal data in the cloud. This provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII).
SIEM	Security information and event management
SOC 2 Type II	Service Organization Controls. SOC 2 concerns the internal controls in place at the third-party service organization. Type II reports, concern policies and procedures over a period of time – systems must be evaluated for a minimum of six months.
API	Application Programming Interface
BPCA Data	Any and all data maintained by the Authority, including, but not limited to, data related to its finances, operations, engineering, taxes, employees, customers, suppliers and the business.

1-ITSEC - SECURITY AND PRIVACY REQUIREMENTS

OVERVIEW

The Contractor must comply fully with all current security procedures of BPCA, as well as with all applicable State and Federal requirements, in performance of this contract.

The Contractor must not, without written authorization from BPCA, divulge to third parties any confidential information obtained by the Contractor or its agents, distributors, resellers, subcontractors, officers or employees in the course of performing contract work, including, but not limited to, security procedures, business operations information or commercial proprietary information in the possession of BPCA.

To ensure confidentiality, the Contractor must take appropriate steps as to personnel, agents and subcontractor education in specific security requirements as applied to this contract, explaining its responsibilities in maintaining security, and reviewing all policies, processes and procedures that will be used for this project.

All activity covered by this RFP must be fully secured and protected by satisfactory security arrangements approved by BPCA. BPCA and the Contractor will establish a joint security management team to accomplish these objectives. The Contractor must treat all information obtained through its performance under the contract as confidential information and will not use any information so obtained in any manner except as necessary for the proper discharge of its obligations and securing of its rights, or as otherwise provided. State or Federal officials, or representatives of these parties as authorized by State or Federal law or regulations, will have access to all confidential information in accordance with the requirements of State and Federal laws and regulations. BPCA will have absolute authority to determine if, and when, any other party is allowed to access application information. Confidentiality is the concept that data only will be viewable by those who are explicitly permitted to view it.

GENERAL SECURITY REQUIREMENTS

SECURITY AND PRIVACY PLAN

The Contractor shall develop follow a Security and Privacy Plan approved by BPCA for all projects and all major system enhancements to address potential security issues and the steps that the Contractor has taken to ensure these issues will not compromise the operation of the program. The plan must be an overarching plan for all levels of security, including but not limited to:

1. Data Security;
2. Network Security; and
3. Application Security
4. Threat, Vulnerability and Risk Assessment

All provisions of the Security and Privacy Plan must be compliant with:

1. All policies and standards defined in the New York State ITS security policies and standards (http://its.ny.gov/eiso/policies/security);
2. Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules;

3. Federal Risk and Authorization Management Program (FedRAMP) if cloud computing is utilized (http://www.gsa.gov/portal/category/102371);
4. All applicable NYS laws and regulations related to privacy protections.

The Security and Privacy Plan must include:

1. A description of all security tools, hardware and software the Contractor is using and how they integrate to form a comprehensive security architecture; and
2. A system overview of processes, data transfer methodology, key management, encryption, vulnerability/patch management, system/application administration, and user access.
3. Data flow diagrams, data dictionary, application architecture, and network diagram of the proposed solution, describing system interfaces, file and data types, protocols, services, and document encryption process.
4. The approach to monitoring attempted security violations and the actions that will be taken when attempts are made at violating security.

The Contractor must:

1. Deliver an initial Security and privacy Plan during the first thirty (30) Calendar days of the project for BPCA review and approval;
2. Revise the Security and Privacy Plan annually and submit for BPCA review and approval; Submit an updated Security and Privacy Plan to BPCA for review and approval thirty (30) business days prior to the start of Operations.

Proposal Requirements

Describe in your proposal how you will support the general security requirements described above.

A. DATA SECURITY

Data Security is the concept that data only will be viewable by those who are explicitly permitted to view or receive it. The security model being developed to support the program is one that is based upon security access roles and organizational affiliation. A role base access control method is one that groups resources (such as business activities, business functions, screens, etc.) into roles. Employees are then assigned roles based on their need-to-know information or their need to accomplish a particular business function. A user's organizational affiliation will also determine what data is available to them.

The Contractor shall:

1. Support a role-based security system that has the flexibility to easily add or delete roles;
2. Submit a solution that will make it easy for Security Administrators to add or remove individuals from established roles;
3. Submit a solution that is able to establish different roles for the metadata database;
4. Submit a solution that will keep a record of activities performed by the users;
5. Submit a solution to track user logon and logoffs into the data warehouse system by user identifiers so that a history of valid and non- valid logon requests by user can be available for investigative purposes.
6. Submit a solution that prevents unauthorized access and safeguard the confidentiality of person/consumer data in compliance with State and Federal law, including the Health Insurance Portability and Accountability Act (HIPAA), the New York State Personal Privacy Protection Law, and the data breach provisions of the New York State Technology Law.

Proposal Requirements
Describe in your proposal how you will support the data security requirements described above.

B. NETWORK SECURITY

The Contractor shall:

1. Provide a network infrastructure solution that must be self-contained and in its own security perimeter. In securing the perimeter of the Contractor's network, the use of International Computer Security Association (ICSA) compliant firewalls is required.
2. NOT connect to the State's internal computer network without the prior, written consent of the State, which the State will reasonably provide if necessary or appropriate for the Contractor to provide support. As a condition of connecting to the State's computer network, the Contractor must secure its own connected systems in a manner consistent with the State's then-current security policies, which the State will provide to the Contractor on request;
3. Provide Internet security functionality to include the use of firewalls, intrusion detection, https, encrypted network/secure socket layer, and security provisioning protocols such as secure sockets layer, and Internet protocol security (IPSEC);
4. Implement mechanisms to safeguard data integrity and confidentiality of data passing over public networks;
5. Put in place a firewall between its private network and the connection to the State's network;
6. Keep any information passing through its network confidential;
7. Ensure that measures are in place to mitigate any new network security risks created by connecting the network to a third-party network
8. Submit and document the design for all communication paths between networks of different security zones through a DMZ
9. Submit and document firewall and monitoring rules for all security zones, and alarm for unexpected traffic
10. Establish responsibilities and procedures for remote use, as defined in the New York State ITS security policies and standards (http://its.ny.gov/eiso/policies/security);
11. The Contractor's Network Architecture and all proposed network hardware and software must be compliant with:
    - All policies and standards defined in the New York State ITS security policies and standards (http://its.ny.gov/eiso/policies/security);

Proposal Requirements
Describe in your proposal how you will support the network security requirements described above.

C. APPLICATION SECURITY

The Contractor's solution shall allow for the following:

1. Applying a consistent security policy across all applications;
2. Ensuring that applications are protected;
3. Providing an easy and consistent mechanism for configuring operational rules and security policies;
4. Providing a structure where applications can be developed without needing to understand the specifics of security implementation; and
5. Restricting access based upon the user's role.

Proposal Requirements
Describe in your proposal how you will support the application security requirements described above.

C. THREAT, VULNERABILITY AND RISK ASSESSMENT

The Contractor shall prepare and submit for approval a Threat, Vulnerability, Risk Assessment (TVRA) that identifies all potential system vulnerabilities; associated risks (including exploit likelihood and consequences); countermeasures applied; and resulting mitigated risks across all system levels

1. Security measures shall include, but are not limited to, the following, as appropriate:
    a. Restricting physical access to communication, control system components, and onboard data (stored, live) to all but authorized personnel
    b. Restricting wired or wireless access to all systems on-board, except for authorized personnel utilizing a centralized system, i.e., cloud-based or data center, such as Identity and Access Management IAM/Active Directory
    c. Use of centralized system (cloud-based/data center) for device and/or user authentication
    d. Use of centralized system (cloud-based/data center) to administer and manage encryption
    e. Centralized system (cloud-based/data center) to administer and manage antivirus, intrusion detection/prevention, Access Control Lists (ACL), firewall policies and logs.
    f. Proper isolation of security critical system functions from other functions end-to-end (client-to-server, wired/wireless, cloud-based/data center)
    g. Application of secure coding practices
    h. Use of secure operating systems
    i. Operating System version shall have a useful life of five years at the time of final acceptance by BPCA
    j. All systems/software shall be upgradeable and compatible with the latest Operating System at the time of final acceptance by BPCA

* * *

Exhibit B

CYBERSECURITY TERMS AND CONDITIONS

A. Definitions.

1. Authority: shall mean the Battery Park City Authority ("BPCA") and its subsidiaries and affiliates.

2. Authority Data: shall mean the following regardless of whether it is contained in existing or newly created in the future physical or electronic media at rest or in motion, any and all

    a. Personal Information as such term is defined herein;
    b. all other data, information and documentation of the Authority including current and revised technology assets and systems, procedures and methodologies for designing implementing or maintaining in general and specifically, with information technology and physical and electronic security;
    c. the Authority's owned, licensed, or subscribed inventions, ideas and designs, design documents, equipment technology and software;
    d. reports and studies whether prepared by Authority, the Contractor or a third-party and whether in development or completed; and
    e. data, information, documentation and material prepared by or for the Contractor, any subcontractor, or by their respective consultants, agents, officers or employees in connection with performance of the Work, whether prior or subsequent to execution of this Contract or Agreement, and
    f. the results of the Work.

3. Personal Information or Personal Identifiable Information: shall mean

    a. any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means;

    b. information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, code, symbol, mark or other identifier) or (ii) by which the Authority or other agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors; and

    c. information permitting the physical or online contacting of a specific individual shall be deemed Personally Identifiable Information.

4. Contractor: as used in this Article shall mean the vendor, contractor, individual or organization that enters into the Contract or Agreement to perform the Work pursuant to the Contract Documents.

5. Work: as used in this Article shall mean as all the required obligations of the Contractor under the Contract or Agreement including but not limited to, the performance of any labor or services, the supplying of any goods, materials or personnel, the furnishing of any equipment, supplies or any other resources or requirements or deliverables necessary for the performance of the work and/or required by the Contract Documents including any scope of work and any modifications to the Contract or Agreement, if any.

B. Compliance with Applicable Laws, and Authority Security Policies and Procedures.

1. The Contractor, including its subcontractors, agents, officers, employees, and all other persons performing under this Contract or Agreement on behalf of the Contractor, shall comply with the applicable standards and

policies set forth in the New York State Office of Information Technology Services Security Policies, which, are located at https://its.ny.gov/eiso/policies/security, in connection with the work, products, services and/or systems that the Contractor is providing to the Authority.

2. The Contractor shall deploy a system security plan (SSP) for ensuring the security of the Authority's systems and data. The SSP and associated technical, organizational and security measures shall align with the information security management system (ISMS) family of standards as published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), also known as the ISO/IEC 27000 series, the NIST cybersecurity framework, or the CIS Top 20 security framework, and SAE International applicable standards, as each may be modified or replaced from time to time.

3. The Contractor shall implement and maintain security measures that meet or exceed the BPCA Cybersecurity Requirements annexed hereto and incorporated herein by reference ("Baseline Cybersecurity Requirements"). At a minimum, the Contractor shall comply with the Baseline Cybersecurity Requirements.

C. Data Privacy and Information Security.

The Contractor's existing methods and procedures shall be in compliance with these terms and conditions and the Baseline Cybersecurity Requirements. Should the Authority require the Contractor to make changes to its cybersecurity compliance during the term of the Contract or Agreement, the Contractor shall work with the Authority to agree on the changes to the cybersecurity compliance.

1. The Contractor shall provide the Authority, upon request, with information regarding the Contractor's compliance and implementation of the Baseline Cybersecurity Requirements.

D. Protection of Data; Notice.

1. The Contractor shall appoint a team of dedicated personnel to work with the Authority during any Security Incident Response (the "Cyber Incident Response Team"). The Cyber Incident Response Team shall be maintained by the Contractor for the duration of the Contract or Agreement. The Contractor shall within twenty-four hours (24) hours of the Authority's Notice of Award (or execution of the Contract or Agreement if no Notice of Award has been issued) provide, in writing, a list of the individuals on the Cyber Incident Response Team. Such list shall include the name of each team member together with a phone number and email address for each such member. In the event of any changes to team members or team member information, the Contractor shall provide such new information to the Authority, to the attention of the Project Manager, in writing.

2. The Vendor shall comply with the New York Stop Hacks and Improve Electronic Data Security Act (also known as the SHIELD Act) in the performance of the Work, as applicable, which, among other things, imposes on entities identified in the SHIELD Act:

    a. particular data breach notification requirements; and
    b. data security safeguards.

3. Unless otherwise provided by law or as further detailed in the Contract or Agreement, in the event of an any act, error or omission, negligence, misconduct, or breach that compromises or is suspected to compromise the security, confidentiality, or integrity of Authority Data or the physical, technical, administrative, or organizational safeguards put in place by the Vendor that relate to the protection of the security, confidentiality, or integrity of Authority Data, the Contractor shall, as applicable:

    a. promptly notify (i) the Project Manager and (2) the Authority by email to [EMAIL], as well as verbally by phone at [PHONE] as soon as practicable but no later than twenty-four (24) hours after initially becoming aware of such occurrence;

b. perform or take any other actions required to comply with applicable law as a result of the occurrence;

c. cooperate with the Authority in investigating the occurrence, including making available all relevant records, files, data reporting, and other materials reasonably required to comply with applicable law, in referring the occurrence to appropriate law enforcement agencies, and in issuing appropriate press releases and responding to the media;

d. in the case of Personally Identifiable Information (PII), (i) notify the Authority, to the attention of: (1) the Project Manager, within twenty-four (24) hours of a confirmed breach and (2) by email to [EMAIL], as well as verbally by phone at [PHONE]; and (ii) at the Authority's sole election, notify the affected individuals who comprise the PII as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within seventy-two (72) hours of the Authority providing written notification to the Contractor requiring the Contractor to notify the affected individuals; and

e. provide to the Authority a detailed corrective action plan as soon as possible, but no later than within ten (10) calendar days of the occurrence, describing the measures the Contractor will undertake and the implementation schedule for such measures, to both resolve the breach and prevent a future occurrence. If the Contractor is unable complete the corrective action within the required timeframe, in addition to the remedies provided herein, the Authority may contract with a third party to provide the required product, service or system until (i) corrective actions have been taken, (ii) the Authority is able to procure from the Contractor the product, service or system in a manner acceptable to the Authority, and/or (iii) until the Authority has completed a new procurement for a replacement product, service or system (the "Mitigation Efforts"). In such case, the Contractor shall reimburse the Authority for the reasonable costs related to the Mitigation Efforts following notice and demand for payment by the Authority.

f. The Contractor shall be responsible for recreating lost Authority Data, if any, in the manner and on the schedule set by the Authority without charge to the Authority.

E. Supply Chain Risk.

1. Upon commencement of the term of the Contract or Agreement, the Contractor shall establish, document, and implement risk management practices for supply chain delivery of work, products, services and systems provided under this Contract or Agreement, if any. The Contractor shall provide documentation on its: chain-of-custody practices, information protection practices, and integrity management program for components provided by sub-suppliers within fourteen days (14) of issuance of Notice of Award or, in the event there is not a Notice of Award issued, within fourteen (14) days of execution of the Contract or Agreement. The Authority may, in is sole discretion and upon the request of the Contractor, extend such time period upon good cause shown.

2. The Contractor shall identify the countries where the development, production and maintenance for the work, products, services and systems provided under this Contract or Agreement is performed ("List of Supplier Countries"). The Contractor shall notify the Authority of changes to the List of Supplier Countries promptly but no less than seven (7) days after the Contractor knows or has reason to know that the list has changed.

F. Prohibition Against Offshore Work

1. If the Contractor is providing consulting and/or professional services including, but not limited to, software development or maintenance, for BPCA Systems, the Contractor

shall not perform any Work outside the United States or utilize any third party to perform (including its own employees) to provide any Work outside the United States.

2. Notwithstanding the foregoing, the Contractor may request that it be permitted to perform Work outside the United States, which determination shall be in the sole discretion of the Authority. In the event the Authority grants such request, the Contractor shall:
    a. In no event transmit, transfer, or otherwise store Authority Data outside of the United States.
    b. Access Authority Data only through virtual desktops provided by BPCA. Access through other paths is strictly prohibited.
3. Enforce compliance with the BPCA IT Security requirements on the devices connecting to the BPCA virtual desktops including:
    a. Not transfer Authority Data between virtual desktop and Contractor's device
    b. Not print Authority Data on non-BPCA managed printers.

G. Cybersecurity Insurance.

The Contractor shall, at its own expense, procure and maintain in full force and effect during the term of this Contract or Agreement, a cybersecurity-related policy of insurance, as set forth by the Authority's schedule of insurance requirements; such policy shall have the minimum coverage set forth therein.

H. Patching Governance.

1. After Notice of Award but prior to the performance or delivery of any work, products, services and systems to the Authority or any connection of electronic devices, assets or equipment to the Authority's electronic equipment, the Contractor shall provide documentation regarding its patch management and vulnerability management/mitigation programs and update process (including third-party hardware, software, and firmware) for work, products, services, systems and any electronic device, asset, or equipment required to be connected to the assets of the Authority during the provision of products and services under this Contract or Agreement. This documentation shall be provided to the Authority, to the attention of the (1) Project Manager, and (2) the Authority by email to [EMAIL], and shall include information regarding:

    (a) the resources and technical capabilities to sustain this program and process such as the Contractor's method or recommendation for how the integrity of a patch is validated by the Authority and

    (b) the Contractor's approach and capability to remediate newly reported zero-day vulnerabilities.

2. Unless otherwise approved by the Authority in writing, current or supported versions of the Contractor's work, products, services and systems ("Items") shall not require the use of out-of-date, unsupported, or end-of-life version of third-party components.

3. The Contractor shall verify and provide documentation to the Authority to the attention of the Project Manager that procured Items (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to the Authority.

I. Updates.

The Contractor shall provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses every thirty (30) calendar days, and within every fourteen (14) calendar days to the Authority, to the attention of the Project Manager, if an update is required to remediate critical vulnerabilities. If updates cannot be made available by the Contractor within these time periods, the Contractor shall provide mitigations and/or workarounds every forty-five (45) calendar days.

J. Cooperation with Authority Cybersecurity Reviews.

1. The Contractor acknowledges that the Authority has a significant interest in protecting and securing Authority Data and that maintaining cybersecurity is an essential element of the Work. The Contractor shall cooperate with the Authority's compliance and cybersecurity reviews during the term of the Contract or Agreement and shall provide (1) information; (2) responses to inquiries and questionnaires in written form, when requested, and (3) supporting documentation to facilitate the Authority's review(s). Such reviews will be coordinated by the Authority's Project Manager.

2. The Contractor shall submit to the Authority, to the attention of the Project Manager, the following: a SOC Type 2 Report within seven (7) days of Notice of Award or, if no Notice of Award is issued by the Authority, within seven (7) days of execution of the Contract or Agreement. When the Contractor's SOC Type 2 Report has expired, the Contractor shall submit an updated SOC Type 2 Report or, if a new report is not immediately available, a bridge letter from the Contractor's senior management, within seven (7) days after expiration of the preceding report. The obligations set forth herein shall be ongoing throughout the term of the Contract or Agreement.

K. Destruction of Authority Data.

1. All Authority Data including, but not limited to, all copies and reproductions thereof and all documents and materials derived from such Authority Data including any data in electronic form (i.e. cloud hosted Authority Data, etc.) provided to, prepared by or for the Contractor or any of its employees, subcontractors, agents and representatives (collectively, the "Contractor Personnel") shall, irrespective of whether such is in writing or stored electronically, be returned to the Authority or irrevocably destroyed by the Contractor and the Contractor Personnel, at the Authority's election, promptly upon the earlier of: (i) the termination or expiration of the Contract or Agreement; or (ii) the Authority's request.

2. The Contractor shall, and shall cause its Contractor Personnel to, irrevocably destroy the Authority Data by: (i) shredding physical documents; (ii) wiping clean the device memory on all equipment, machines, databases, servers, cloud storage or other electronic media on which the Authority Data is located; and (iii) sanitize storage media, as well as temporary files and backup files on which the Authority Data is stored. The Authority may request certification that destruction has been irrevocably completed for all primary, backup and any other applicable systems or mediums from the Contractor which shall be promptly provided by the Contractor for itself and for the Contractor Personnel; but in no event, not later than fourteen (14) days following the Authority's request.

L. Subcontractor Compliance.

1. The Contractor shall flow down these Cybersecurity Terms and Conditions to its subcontractors, agents and representatives who perform any Work pursuant to the Contract or Agreement.

2. The Contractor shall ensure that each of its subcontractors, agents and representatives comply with these Cybersecurity Terms and Conditions.

M. Cybersecurity Training.

The Contractor shall ensure that any individual or individuals who have access to Authority Data under this Contract or Agreement shall undergo cybersecurity awareness training from a reputable training source. Such training shall be at the Contractor's cost and the Authority shall not be required to pay any costs related to such training. The Contractor shall maintain training records during the term of the Contract or Agreement and shall make such documents available to the Authority for inspection upon request of the Authority.

N. Conflict.

If there is a conflict between these Cybersecurity Terms and Conditions and the Contract Terms and Conditions, the most stringent provision shall apply.

* * *