Supplemental Information

Pursuant to Education Law § 2-d and § 121.3 of the Regulations of the Commissioner of Education, the NYS Education Department ("NYSED") is required to post information to its website about its contracts with third-party contractors that will receive Student PII and/or Teacher and/or Principal APPR data ("APPR Data"), collectively referred to as PII.

Name of Contractor	Questar Assessment Inc.
	Student demographic data will be provided to the Contractor for the purpose of it performing the following tasks for NYSED: conducting field testing and operational testing, analyzing field test items and producing operational test results. The Contractor will also be gathering student test result data in scoring students' responses to multiple-choice questions and determining students' scale score and performance level results.
	Check all that apply:
	; Student PII APPR Data
	Contract Start Date: Contract End Date:
	Contractor will not utilize Subcontractors without a written contract that requires the Subcontractors to adhere to, at a minimum, materially similar data protection okpecP ;

Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting NYSED. If a correction to data is deemed necessary, NYSED will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving NYSED's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ; ; All data is hosted in the United States. Only authorized personnel have access to data, and granted only as part of their job function.

	Questar Assessment Inc.

Questar Assessment, Inc. Appendix R Supplement

1. Outline how you will implement applicable data privacy and security contract requirements over the life of the Contract.

Questar takes data security and privacy concerns very seriously and has developed policies, procedures, and practices to protect our client's data from unauthorized access. At the onset of each contract, Questar reviews all data security and privacy requirements to ensure that our existing policies, procedures, and practices meet or exceed those stipulated in the contract. If gaps are identified, Questar will develop a mitigation plan and modify our practices to be in compliance with the contract.

An important step in minimizing a breach is to learn of the potential breach as soon as possible. As such, our employees are all trained in the importance of reporting any potential breach as soon as it is discovered, } u u µ v] š] } Œ š ž š Z u ‰ o } Ç [• u v š Z Œ v (v} Œ u^ š] µ } Œ] š Ç Team.

Personnel are also made aware that staff found to have violated Questar breach notification process policy may be subject to disciplinary action, up to and including termination of employment and related civil or criminal penalties.

Materials are transported to the document destruction facility in a sealed trailer, where a combination of shredding and pulping is used for the destruction of the materials.

A Certificate of Destruction is provided for each load of material and is kept on file at Questar or can be provided to NYSED.

8. Z } Á Ç } µ Œ š ‰ Œ] À v ç µ Œ ‰ š Œ } P Œ u l ‰ Œ ‡ Á v] š Z z ^ ^

Working with the Information Security Program, Questar adopts and maintains administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws, rules and regulations, and NYSED policies.

Questar recognizes that Education Law § 2-d requires that Questar provide NYSED with a Data Privacy and Security Plan that outlines our relevant safeguards, measures, and controls, including how Questar will implement all applicable state, federal, and local data privacy and security requirements.

Please refer to DPA Exhibit 1 for Q Data Privacy and Security Plan.

4. š WŒ]Àv Ç µŒ]šÇ o] Ç

Questar recognizes that New York state law and regulation require NYSED to adopt a data privacy and security policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework.

As a current vendor, Questar is ‹µ]vš ÁŒ]šZ [• š WŒ]À µŒ]šÇ o] vÇ U other applicable policies, and we will continue to make compliance a foremost consideration as we undertake the work of the new contract.

5. Right of Review and Audit

Questar fully recognizes right to request that Questar provide NYSED with copies of its policies and related procedures that pertain to the protection of PII (in a form that does not violate confidentiality obligations and applicable laws).

Questar also recognizes that our organization may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New

o Á• Œ Pµo šŒ}v•U[• ‰}o]] • applicable to Questar, and alignment with the NIST Cybersecins

When the purpose that necessitated the receipt of PII by Questar has been completed, or authority to have access to PII has expired, Questar will ensure that all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Questar in a secure data center and/or cloud-based facilities that remain in the possession of Questar or its subcontractors is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed.

Hard copy media will be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. We recognize that only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction, and that redaction is specifically excluded as a means of data destruction.

Questar further commits to providing NYSED with a written certification of the secure deletion and/or destruction of PII held by the Questar or subcontractors to the contact and address for notifications set forth in the contract.

To the extent that Questar and/or our subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and in direct identifiers removed), we agree that neither Questar nor our subcontractors will attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition

Questar agrees, and it is our unequivocal policy, to not sell PII or use or disclose PII for a commercial or marketing purpose.

11. Encryption

We recognize the sensitive nature of testing materials, individual student information, test scores, and v o Ç • ▼U• Z Œ E z ^ [• } v À} µ š Z} v l the primacy of ensuring the security of these elements.

Á] o ‰ Z •] Ì • µ Œ Z (v • š µ] v ‰ • Œ • } v o š] ( ] o / v (} Œ / š } } Z Œ v to applicable FERPA, as well as all other laws, regulations, policies, and procedures required by the State of New York.

Questar will encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

Encryption at Rest

Questar encrypts all student data (e.g., PII) at rest, using built-in SQL Server security tools. Questar uses Microsoft Transparent Data Encryption (TDE). TDE performs real-time I/O encryption and decryption of the data and log files. AES-256 is the encryption technology used. The encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery.

The DEK is a symmetric key secured by using a certificate stored in the master database of the server or an asymmetric key protected by an EKM module. TDE protects data at rest, which is to say the data and log files.

Test forms and student responses are stored in AWS S3 volumes and are encrypted at rest using AES-256, as well as following all industry and AWS best practices, including using Customer Master Keys (CMKs). Student response metadata and scores are stored in AWS DynamoDB and are also encrypted at rest using AES-256 and following the same best practices. CMKs are protected by hardware security modules (HSMs). HSMs are validated by the FIPS 140-2 Cryptographic Module Validation Program, using a FIPS approved encryption algorithm (AES-GCM with 256-bit keys), and using the encryption context as additional authenticated data (AAD) to support authenticated encryption.

All data is stored within the continental United States. This includes all online data, back-up copies, and data for disaster recovery purposes. Only authorized users are able to access data, and access is limited to necessary data for the role of the user.

Encryption in Transit

For encryption in transit, Questar applications utilize TLS technology, over Hypertext Transfer Protocol Secure (HTTPS), ensuring that all transmissions of data occur over secure network connections. } (d > ^ µ š] o-ŽÌ certificates with SHA-256 signatures and 2048-bit keys, and the latest and most secure TLS protocols and cipher suites are supported, meeting or exceeding all of the most widely respected and stringent compliance standards. In addition, Questar systems that communicate asynchronously through AWS SQS have server-side encryption enabled, using 256-bit Advanced Encryption Standard (AES-256 GCM algorithm) to encrypt each message body.

Certain other data, such as downloaded test packages and student responses cached on the local student workstation, are additionally encrypted using AES/Rijndael with 256-bit keys using FIPS 140-2 validated libraries. Test content accessed via valid authentication information will be displayed only while the student is taking the test, and, upon completing the test, any residual, decrypted test content is automatically removed from any systems outside of the host systems.

12. Breach

Questar has a breach notification process policy that governs our actions, should a security or privacy incident occur. This process covers communications with our clients as well as data collection and forensics to identify the source and nature of the breach.

As part of our breach notification, we follow all applicable laws and contractual requirements and, as such we commit to promptly notifying NYSED of any breach of PII in the most expedient way possible and without unreasonable delay (no later than seven business days after discovery of the breach).

š]}vY µ •š Œ [• vŒ} š] (Z ‰] }Ev}]v• Ʊ µ Ž}v}PÁ]oš] P v •E ž } requirements, please refer to our response to #5 above.

13. Cooperation with Investigations

] • š‰ Œ } š] vÀ fully cooperate with NYSED (and law enforcement, where necessary) in any investigations into the breach.

Any costs incidental to the required cooperation or participation of Questar will be the sole responsibility of Questar if such breach is attributable to Questar (or our subcontractors).

14. Notification to Individuals

Should a Breach of PII occur that is attributable to Questar (or Questar subcontractors), Questar commits to promptly paying for or promptly reimbursing š Z (µ}o•š} (E z ^ [• v } š] ( ]š } š] } v parents, eligible students, teachers, and principals, in accordance with Education Law § 2d and 8 NYCRR Part 121.

15. Termination

Questar recognizes that confidentiality and data security obligations of our organization under the DPA survive any termination of the DPA, up until the point at which Questar certifies the destruction of all PII.

<u>Article III</u>

1. Parent and Eligible Student Access

As required by Education Law § 2-d, the Parents Bill of Rights for Data Privacy and Security and the Supplemental Information for the Contract is included as DPA Exhibit 2 and incorporated into this DPA.

Questar commits to signing DPA Exhibit 2, recognizing that it will be appended to this DPA.

We further understand that, pursuant to Education Law § 2-d, NYSED is required to post the Parents Bill of Rights for Data Privacy and Security and the Supplemental Information about each contract where the contractor will receive PII on its website.

2. Bill of Rights for Data Privacy and Security

Education Law § 2-d and FERPA provide Parents and Eligible Students the right to inspect and review

š •š}Œ }Œ u]vE z]'v Y D•QÀ E z ^ Q*´S êÉ Á

All Questar devices will be configured in a manner to optimize the security of the device.
An asset inventory may be generated to track company purchased hardware and software.
All Questar assets taken off-site should be kept in a secure location while not in use.
Upon termination of employment, contract or agreement, all Questar assets must be returned to Questar Assessment.

Day-

cs7.942(t)9 eaem.

The policy covers the scope and frequency of risk assessments. The results of the risk assessment are shared with internal stakeholders. Risks are enumerated, classified, and prioritized for remediation.

Additional elements include:

- Questar must v µŒ š šZ }Œ }ŒP Zl v oÇ •]• (}Œ Y µ •š Œ ... security and compliance efforts.
- Questar must re-assess the security risks to its data and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business practices and technological advancements.
- Formal organization-wide risk assessments will be conducted by Questar no less than annually or upon significant changes to the Questar environment.
- Risk assessments must account for administrative, physical, and technical risks.
- All risks will be classified and prioritized according to their importance to the organization.
- Periodically, Questar may contract with a third-party vendor to conduct an independent risk assessment and/or to validate the effectiveness of the Questar risk management process.

‰ Œ š]]v šŒ Á]šZ šZ]Œ -party firm to conduct an annual risk assessment to identify any external risks to the security, confidentiality, and integrity of Student PII that could result in the authorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information.

Supply Chain Risk Management (ID.SC): RUJDQL]DWLRQ¶V SULRULWLHV FRQVWUDLQWV tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

Agreements with vendors are structured to result in specific deliverables. Deliverables are described in appropriate concrete terms. Regular meetings are held with critical vendors to ensure SLAs and deliverables are being met.

Vendors are chosen for their relityG0ha3 (o)5(i)-8 (v)17 (erab).12 Tm[(a)6y 347.88 Tm[(sp)-12 792 rehrab-86y 347.88 Tm

Questar Project Management is consulted for scheduling considerations and to gain vendor approval by NYSED, and finance is consulted to approve budgets. Communication between all of these groups, as well as the subcontractor, continues until a final SOW is approved and signed by Questar executive leadership and the subcontractor, resulting in an executed contract.

Once the contract is executed, the vendor is trained by appropriate Questar staff (e.g., assessment specialists, psychometricians) and provided with all the background information and necessary materials to successfully complete the work. As the work progresses, periodic check-in meetings with the subcontractor are hosted by the subcontractor and attended by other Questar stakeholders as appropriate. Agenda topics for these meetings include feedback on the quality of the work and adherence to the schedules, as well as any other pertinent issues or concerns that may arise.

All subcontractors that interact with secure materials will be required to sign a non-disclosure agreement. A secure FTP site is used for exchange of secure materials, including those required by the subcontractor. Item review and development work will be carried out within our secure electronic item bank. The item bank system is accessed only through a unique username and password, with each account restricted to the material needed by a specific user.

PROTECT (PR)

Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Questar manages access to physical and logical assets and associated facilities, limiting access to authorized users, processes, and devices, and managing access consistent with the assessed risk of unauthorized access to authorized activities and transactions.

l Ç

• ‰ Œ š u ‰v o š Á } Œ l • ‰ Œ } µ µ š v] } v P v š Á } Œ l • X
Y µ • š Œ [• v š Á } K E v l o Ç u • X Œ Ç š Á } Œ l ‰ } Œ š • Œ } ‰ v
for business applications to perform as needed.

Access controls are in place for all operating systems, applications, networks, and mobile systems.
µ • Œ [• • • ‰ Œ d } À H a n d P a u t o m a t i c a l l y disable or enable functionality
based upon the user's security profile. Procedures have been established for user registration and deregistration. These procedures include:

Grant the correct level of access privilege

Control password use, change, and removal

Manage review of access rights

Secure unattended equipment, maintain a clear desk best practice

Control network service access

Control method for authentication of remote users; control configuration of ports

Control segregation of networks

Provide precise routing controls

Control sy88 e 0 Tw 5 1 Tf g e (end) 5 (ed) 10 T f t r o l s

Data is also protected while in transit. TLS with AES ciphers are used to secure data over public networks µ• Œ ‰}]vš/WX]• µ•š}• µŒ š]švŒ v•]šÁ v Yµ •š Œ[• hosting facilities.

Each customer has a dedicated instance of Nextera. Compute, networking, and storage are all dedicated per customer. The entirety of Nextera, including back-ups, are hosted within the borders of the United States. Additionally, the production environment is separated from development and testing environments. This separation includes network connectivity and access permissions.

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

l Ç } u ‰ } v }v(š Y µ •š Œ [• / v (^} Œµ uŒ šÇ W} o] Ç]• the security-related corporate policies used to document key security strategies and ensure that they are followed and enforced. These policies are in part informed by the applicable legal and regulatory requirements that our work is subject to, as well as the standard expectations and -scale state assessments clients.

Application logs are maintained in our secure database environment, which is subject to the network security requirements described above, including strong password policy, frequent changes to passwords, and the principle of least privilege, meaning that users are given the network access required to efficiently perform their job functions and no more.

Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

Questar employs designated personnel responsible for network, server, storage, and workstations. Hardware repairs are documented in tickets and handled by the IT staff responsible for the failed device type.

Questar personnel perform repairs in the field according to manufacturer field service procedures. Authorized third parties are used when field repairs are not possible. Questar personnel are within driving distance of physical infrastructure locations. Third parties are escorted during repair visits.

Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Questar keeps audit logs for AWS, Office365, and on-premise. Only authorized personnel can access the logs. Logs are reviewed for unauthorized activity which, if found, is acted upon.

Questar maintains a Removable Media policy, which policy describes acceptable use and procedures for removable media, including sourcing of media, encryption requirements, and media handling.

The network edge is protected by dedicated devices and managed by designated personnel. IDS sensors are used to monitor network traffic. Personnel respond to malicious traffic if detected.

Systems are configured to provide a specific service or host a specific application. Redundancy, availability, data backup, and disaster recovery needs are all part of the design and solution.

DETECT

Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.

Questar gathers information through a load test group when we have a new build. We base our incident thresholds on these baselines.

When there is a detected event, it is analyzed by several different people to determine the origin and to make sure our network is secure. To determine the impact of events, we have a Root Cause Analysis (RCA) process where we can bring together all the personnel and data needed.

Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

The following excerpt outlines some of the process steps detailed in the incident management policy.

> Questar IT management will establish and provide overall direction to a Questar Incident Response Team (IRT).
> Questar IRT members must create and implement an Incident Management Plan.
> Questar IRT members have pre-defined roles and responsibilities which can take priority over normal duties. Any additional Questar Assessment staff member may be called upon to assist in resolving an incident.
> The IRT will respond to any new threat to Questar information systems or data following the Incident Management Plan.
> The IRT must report the incident to:
> - Questar Executive Management
> - Any affected customers and or/partners or local, state, or federal law officials as required by applicable statutes and/or regulations.
>
> The IRT will coordinate communications with any outside organizations.
> The Incident Management Plan must be tested by the IRT no less than annually.

Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

Questar maintains a breach notification procedure that outlines incident reporting needs. This procedure is explicit about who to share information with.

Internally, upon the report of a potential breach, a representative from the IT Security team will craft a brief status message to be sent to the IT Security Committee, as well as the reporting team and executive leadership. This e-mail and all subsequent updates are considered confidential and are not permitted to be forwarded without authorization.

Externally, per the documented breach notification procedure, information is shared with external stakeholders based on the type of breach, legal obligations, and contractual obligations.

In the c z } ŒÁUµ v Œ • š Yvµ • š dEtly to promptly notify NYSED of any breach of PII in the most expedient way possible and without unreasonable delay (no later than seven business days after discovery of the b

Such notification will be sent to NYSED at the contact provided for contract related notifications, with a copy to the Chief Privacy Officer, NYS Education Department, 89 Washington Avenue, Albany, New York12234.

Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities

Alerts are triaged by a third-party security operations team. The team validates alerts and eliminates false positives. Notifications are then sent to the designated Questar team that takes action.

Notifications indicate the type of breach and the breach notification procedure describes different categories of breaches. Log information is then used to determine the scope and impact of breaches.

Appropriate forensics tools (e.g., log data, systems forensics tools) are used to collect data for analysis. Advisories from internal and external parties are sent to designated Questar IT teams.

Advisories come in several forms: automated reports, ad hoc emails from vendor partners, and trusted agencies such as CERT.

Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

In the event that the team validates that a breach occurred, one of the top priorities is containment and mitigation. The IT Security Team works with the assistance of all impacted teams to efficiently work to contain the breach and limit the scope. Questar policy includes a list of examples of containment strategies that may be considered in addition to the expertise of all involved.

Also, technical design of our assessment solutions limit exposure and prevent lateral exposure. For example, each customer assessment software system is deployed to a dedicated, independent environment.

During an incident, designated teams work to limit the exposure or loss. For example, accounts may be disabled, or systems removed from the network.

If there are newly identified vulnerabilities, these are mitigated, if possible.

Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

s incident management process focuses on immediate issue identification, impact containment, and resolution.

As part of the process, a Critical Action Plan document is maintained that documents the issue, summarizing its impact, and identifies and assigns ownership for the key actions that must be implemented to resolve the issue and return to a stable state.

This documentation and the process it represents also serve to drive process improvements from the immediate lessons from the current activities, and our incident management process mandates that relevant processes be reviewed and possibly update based on the event.

More future-facing improvements are a result of the subsequent root cause analysis that is part of our Corrective and Preventive Actions plan, which we outline in the Improvements section below.

RECOVER (RC)

Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

]v]]š]• }À Ç Œ µ •š Œ[• Z] (/v(} Œ u š] } v ^ µ Œ] š Ç K (( ] Œ l • Á] š Z

the techn7 ecpthgBT/Tyc 0 T1 Tf0a(l)-8 0 Tw 0 Ts 1eWt (l)-8 (i) Tr 11facaltoulre(u)TeW*nBT/T-1411reW*nBT/T Tw 0 Ts 1a

Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

š Z ^ šDirector assigned to NYSED communicate relevant information in a timely manner to NYSED following a documented process. Communication channels include email and telephone.

Breach communications are sent regularly to the CEO from the time an incident is discovered until the incident is mitigated and resolved.