DPA EXHIBIT 2 - Education Law § 2-d Bill of Rights for Data Privacy and Security and Supplemental Information for Contracts that Utilize Personally Identifiable Information

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A Student's Personally Identifiable Information (Student PII) cannot be sold or released for any Commercial or Marketing purpose. Student PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR § 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Regulations of the Commissioner of Education at 8 NYCRR Part 121, FERPA at 12 U.S.C. § 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. §§ 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. § 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. § 1400 et seq. (34 CFR Part 300); protect the confidentiality of Student PII.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when Student PII is stored or transferred.

5. A complete list of all student data elements collected by New York State Education Department ("NYSED")is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of Student PII addressed. (i) Complaints should be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of Student PII occurs.

8. NYSED workers that handle Student PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. NYSED contracts with vendors that receive Student PII will address statutory and regulatory data privacy and security requirements.

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.
Description of the purpose(s) for which Contractor will receive/access PII	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.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date: Contract End Date:
Subcontractor Written Agreement Requirement	Contractor will not utilize Subcontractors without a written contract that requires the Subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☐ Contractor will not utilize Subcontractors. ☒ Contractor will utilize Subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to NYSED, or a successor contractor at NYSED's option and written discretion, in a format agreed to by the parties**.** • Securely delete and destroy data.

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) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☒ Using Contractor owned and hosted solution. ☐ Other: Please describe how data privacy and security risks will be mitigated in a manner that does not compromise the security of the data: All data is hosted in the United States. Only authorized personnel have access to data, and granted only as part of their job function. NYSED data is encrypted using a key generated, and maintained, by Questar. The hosting provider is unable to access the data without the key. The key can only be accessed by authorized Questar personnel.
Encryption	Data will be encrypted while in motion and at rest.

Contractor's Name	Questar Assessment Inc.
Signature	
Printed Name	
Title	
Date	

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.

Questar fully commits to the protection of student data and PII, including complying with state and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

An integral component of Questar's plan for ensuring that we meet all RFP requirements related to security of data and protection of PII is our Information Security Program. This plan is the blueprint for the organization's security processes, policies, technologies, and organizational structures, and is based around data security and privacy best practices, including the NIST Cyber Security Framework.

The Questar Information Security Program is overseen by Questar's Executive Security Council, which is headed by Questar's Chief Information Security Officer, Brendan Kealey, and also includes Questar's Chief Financial Officer, Vice President of Operations, Vice President of Human Resources, and Director of IT Enterprise Services.

This cross-functional team possesses the skills and seniority level to ensure that Questar security and privacy practices are evaluated from multiple perspectives and that all functions (technology, operations, finance, etc.) have an active voice in making security policy and risk management decisions.

A key component of the Information Security Program is 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 are work is subject to.

Questar's core security and privacy policies include Asset Management, Audit Policy, Breach Management and Notification, Building Security, Code of Conduct, Data Retention and Destruction, Incident Management, Malicious Software, Media use and Destruction, and Removable Media Policy.

The Executive Security Council meets quarterly to review concerns that may have arisen during the quarter to: analyze and manage potential new security risks, review and update security policies as necessary, identify areas that should be addressed during annual security training, and more.

As part of Questar's risk management process, Questar contracts with a third-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.

2. Specify the administrative, operational, and technical safeguards and practices that you have in place to protect PII.

Access to personally identifiable information is controlled via a combination of measures. First, the infrastructure used to house PII data is secured using industry best practices to ensure systems are sufficiently hardened and protected from known vulnerabilities and external threats. Second, our applications are designed to prevent unauthorized access to PII using role-based access control. Third, access to PII data within the Questar organization is granted on a 'need to know' basis to explicitly control who has the ability to access to sensitive data.

The above measures and their implementations are evaluated on a regular basis to ensure that system protections are kept current and that the list of authorized users is accurate.

Encryption of data is an example of a core technical safeguard. Questar encrypts all student data (e.g., PII) at rest and in transit using industry best-practices. Data is encrypted at rest using built-in SQL Server security tools. (Microsoft Transparent Data Encryption). 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.

An example of an operational safeguard that we have in place is the use of employee termination checklists to ensure account access termination is performed. This safeguard applies not only to employees who have left the organization, but also to those who may have changed job functions within Questar and therefore may have different access to certain accounts.

The Nextera test platform that Questar will develop to administer and deliver NYSED's assessment will be delivered from a state-of-the-art cloud environment that itself is protected by a litany of safeguards and practices, including regular threat and vulnerability reviews, and ongoing assessment and mitigation of potential vulnerabilities.

3. Address the training received by your employees and any Subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.

Annually, all Questar employees and subcontractors are required to participate in and successfully pass Security Awareness and Personally Identifiable Information security trainings.

The Security Awareness course covers key security best practices end users must follow so they can prevent, detect, and respond to information security threats. It is designed to cover all of today's critical security topics, such as password management, identity theft, malware, social engineering, phishing, spear phishing, physical security, business email compromise, Internet of Things (IoT), travel safety, mobile data, privacy, and acceptable use.

The course was developed by Inspired eLearning, a leader in security training with a focus on training that achieves more effective and measurable changes in organizations, with content created by instructional design professionals and backed by cybersecurity experts.

All Questar employees are required to re-certify their mastery of Security Awareness annually.

The Personally Identifiable Information course is designed to ensure that Questar staff are fully prepared to meet the high-standard of PII-protection that our customers expect, as well as mandated by state and federal law.

This mandatory course covers what constitutes PII, where it is typically found, appropriate and limited circumstances for accessing PII, how employees should (and should not) handle PII, and required steps in the unlikely event of unauthorized disclosure of PII.

Both of these mandatory security training courses are delivered online through an interactive design that engages employees in learning and concludes with a required test that must be passed to successfully complete the course.

In the course of training, employees must also access, read, and assert compliance with Questar's official IT Security Policies, including Data Retention and Destruction Policy, Security Awareness and Training Policy, Media Use and Destruction Policy, and Removable Media Policy.

In addition to these trainings, internal technology infrastructure employees are trained in data retention, disaster recovery, and business continuity workflows. They also participate regularly in quality improvement conference sessions. Questar employees stay current on strategies for protecting data, materials, and the interests of students and state departments of education.

4. Outline contracting processes that ensure that your employees and any Subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.

Questar's contracting processes ensure that all employees and subcontractors are bound by written agreement to the requirements of the Contract. This is implemented internally through our employment agreement and externally through contractual language with our subcontractors.

Regarding Questar employees and contractors, all must pass a background check as a condition of employment, and then must sign confidentiality and non-disclosure agreements as a condition of employment.

Employees also must review and sign Questar's Code of Conduct, which lays out in detail expectations for employees regarding the safe and secure handling of the sensitive data and information to which our organization is entrusted.

We keep a copy of each signed agreement on file and will provide copies to NYSED, if requested.

In addition, Questar ensures that committee meeting participants (e.g., item reviews and standard setting) also sign confidentiality and non-disclosure agreements, while also being training in the importance of security and requirements for the safe handling of secure materials.

5. Specify how you will manage any data privacy and security incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the NYSED.

Should a security or privacy incident occur, Questar has a breach notification process that governs our actions. This process covers both communications with our clients as well as data collection and forensics to identify the source and nature of the breach. In the event of a security incident, Questar will inform NYSED and work in partnership to resolve the incident.

Our process is designed to contain, investigate, and remediate a security breach. Because any potential security breach will be unique, our process is designed to guide staff involved in discovering, containing, remediating or providing notice regarding the breach.

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, with communication directed to both the employee's manager and the Information Security 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.

Upon the report of a potential breach, a representative from the IT Security Department will craft a brief status message to be sent to the IT Security Committee as well as the reporting team. This email and all subsequent updates are considered confidential and are NOT permitted to be forwarded without authorization.

Depending upon what is discovered during the investigation and recovery process, additional stakeholders may be notified of the breach.

A representative from the IT Security team will work with the reporting team along with additional resources in order to verify that a breach is occurring (or has occurred).

There are times where it appears that a breach is occurring (or has occurred), but upon gathering additional data elements the situation shows to be normal or failed traffic. In that event, the report will be designated as a false positive. The IT Security team representative will send a notification to the IT Security Committee informing them that the security breach is a false positive.

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

Another stage of the procedure is breach investigation, which aims to gather critical information about the nature of the breach that may serve to help with containment, if not yet achieved, as well as informing notification steps and remediation.

Our policy provides guidelines for a standard investigation, though, again, the work will be driven by the expertise of the individuals involved. As appropriate, we broaden to involve experts from in-scope subcontractors, such as our data center vendor.

Notification is another stage of the breach policy. It is informed by a number of factors, including the nature of breach, based on our initial investigation, as well as the legal and contractual variables that may be in scope.

Questar fully commits to comply with all notification requirements to which we will be subject in the new contract, including the duty 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 breach).

As required by the RFP, the program manager will immediately notify the Director of State Assessment, or his/her designee, via telephone and in writing of the issue and Questar's proposed solution. Questar will also include the issue and NYSED approved solution on any subsequent report(s).

Questar will also abide by additional requirements to which we are subject, which may include providing notifications in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified mail, and must to the extent available, include a description of the breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Questar's investigation; and the name of a point of contact.

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 York, 12234.

Questar also recognizes that violations of the requirement to notify NYSED will be subject to a civil penalty pursuant to Education Law § 2-d. The Breach of certain PII protected by Education Law § 2-d may subject Questar to additional penalties.

At the conclusion of the investigation phase, action items may remain open, or could be added as steps required to remediate the root cause entirely, as well as to prevent any future re-occurrence of the threat. As the process goes into the post breach remediation phase, the IT Security Committee will assist the IT Security team and impacted teams on prioritizing remaining action items.

6. Describe how data will be transitioned to NYSED when no longer needed by you to meet your contractual obligations, if applicable.

Upon termination of the agreement between Questar and NYSED, Questar acknowledges and agrees that we are responsible for ensuring that all student data shared by Questar must be returned to NYSED or otherwise destroyed.

The presumed method of transfer of electronic data would be via the secure FTP that we currently have in place for secure transfer with NYSED.

Questar will maintain such a site for the new contract (as is our standard practice and in effect for the current contract). Access to the site will be limited to appropriate Questar personnel and NYSED, unless further sharing with other parties is authorized in writing by NYSED.

In regard to the transfer of any secure test materials that Questar stores for NYSED, we would work with the existing process of using lockboxes.

That stated, would certainly defer to NYSED on preferred methods for secure transfer.

7. Describe your secure destruction practices and how certification will be provided to the NYSED.

Questar maintains a Data Retention and Destruction policy and a Media Use and Destruction policy that together mandate how our organization securely disposes of data and media according to established standards. Questar will supply an attestation that electronic data was destroyed according to policy, should NYSED require.

In regard to the secure destruction of paper-based NYSED materials, which may include secure data and student PII, Questar works with well-established document destruction firms. Before materials leave Questar, Operations staff inventory the materials (i.e., material type, SKU number, quantity remaining) and provide a comprehensive list of those materials to our Program Management team. The Program Management team reviews the list and conducts a spot inspection of materials before requesting permission from NYSED to destroy the materials.

Materials are transported to the vendor's 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. Outline how your data privacy and security program/practices align with NYSED's applicable policies.

Questar's data privacy and security practices are part of our Information Security Program, which is the blueprint for the organization's security processes, policies, technologies, and organizational structures.

The program is based around data security and privacy best practices, including the NIST Cyber Security Framework, and it is also informed by the needs and requirements of the large-scale state assessment clients that we have supported for decades, as well as the state and federal laws that our clients and we are subject to, including the Family Educational Rights and Privacy Act (FERPA).

In the text that follows, we offer details regarding our alignment with the applicable NYSED policies outlined in Article II and III or this document.

Article II

1. Compliance with Law.

Questar recognizes the sensitive nature of testing materials, individual student information, test scores, and statistical analyses because we work with confidential student data and secure testing materials every day.

We understand that student privacy laws prohibit access to individual student results or easily traceable student information by anyone or any organization other than the student, the student's parent or guardian, or the school, district, state [as defined by the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C.§1232g. and 1232h.; 34 CFR Part 99)].

Our organization goes to great lengths to protect the privacy and security of student data, and we have an excellent record of protecting student data. Questar reviews all data security and privacy requirements at the onset of each contract 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.

We have extensive experience partnering with NYSED to ensure the security of student data and PII, including as stipulated in the New York and federal laws and regulations in Article II of Appendix R.

2. Authorized Use.

Questar fully recognizes that the organization has no property or licensing rights or claims of ownership to PII, and that Questar must under no circumstances use PII for any purpose other than to provide the relevant contract services.

3. Contractor's Data Privacy and Security Plan.

Questar maintains an Information Security Program that serves as the blueprint for the organization's security processes, policies, technologies, and organizational structures. This program built is on industry data security and privacy best practices, including the NIST Cyber Security Framework.

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 Questar's Data Privacy and Security Plan.

4. NYSED's Data Privacy and Security Policy

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 closely acquainted with NYSED's Data Privacy and Security Policy, and 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 NYSED's 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 Questar's 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 York State laws and regulations, NYSED's policies applicable to Questar, and alignment with the NIST Cybersecurity Framework performed by an independent third party (at Questar's expense), and provide the audit report to NYSED.

We also recognize that Questar has the option, in lieu of performing an audit, of providing NYSED with an industry standard independent audit report on Questar's privacy and security practices that is no more than twelve months old.

6. Contractor's Employees and Subcontractors

Questar shall only disclose PII to our employees and subcontractors who need to know the PII in order to provide the relevant contracted services and the disclosure of PII shall be limited to the extent necessary to provide such services. Questar will ensure that all such employees and subcontractors comply with the terms of this DPA.

Questar will, as required, ensure that each subcontractor performing contracted services where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

Questar commits to examine the data privacy and security measures of its subcontractors prior to utilizing the subcontractor. If at any point the subcontractor fails to materially comply with the requirements of this DPA, Questar will: notify NYSED and promptly remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Questar will follow the data breach reporting requirements.

Questar takes full responsibility for the acts and omissions of its employees and Subcontractors.

Other than Questar's employees and subcontractors, Questar will not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena.

Questar will make a reasonable effort to notify NYSED of the court order or subpoena in advance of compliance, but in any case, will provide notice to NYSED no later than the time the PII is disclosed, unless such disclosure to NYSED is expressly prohibited by the statute, court order, or subpoena.

7. Training

Questar will ensure that all its employees and Questar subcontractors who have access to PII will have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

Upon initial hire and then annually, all Questar employees and subcontractors are required to participate in and successfully pass Security Awareness and Personally Identifiable Information security trainings.

The Security Awareness course covers key security best practices end users must follow so they can prevent, detect, and respond to information security threats. It is designed to cover all of today's critical security topics, such as password management, identity theft, malware, social engineering, phishing, spear phishing, physical security, business email compromise, Internet of Things (IoT), travel safety, mobile data, privacy, and acceptable use.

The Personally Identifiable Information course is designed to ensure that Questar staff are fully prepared to meet the high-standard of PII-protection that our customers expect, as well as mandated by state and federal law.

This mandatory course covers what constitutes PII, where it is typically found, appropriate and limited circumstances for accessing PII, how employees should (and should not) handle PII, and required steps in the unlikely event of unauthorized disclosure of PII.

8. Termination

Questar recognizes that this DPA will continue and will not terminate for as long as Questar or our subcontractors retain PII or retain access to PII.

9. Data Return and Destruction of Data

Questar recognizes that our organization is prohibited from retaining PII or continued access to PII or any copy, summary, or extract of PII, on any storage medium (including, without limitation, insecure data centers and/or cloud-based facilities) whatsoever beyond the term of the contract unless such retention is either expressly authorized for a prescribed period by the contract, expressly requested in writing by NYSED for purposes of facilitating the transfer of PII to NYSED, or expressly required by law. As applicable, upon expiration or termination of the contract, Questar shall transfer PII, in a format agreed to by the parties to NYSED.

When the purpose that necessitated the receipt of PII by Questar has been completed, or Questar's 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 statistical analyses, and share NYSED's conviction about the absolute primacy of ensuring the security of these elements.

We will emphasize secure handling of students' Personally Identifiable Information (PII) and adherence 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. Questar's implementation of TLS utilizes SHA-2 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).

For additional detail on Questar's breach notification process, including how it aligns to NYSED requirements, please refer to our response to #5 above.

13. Cooperation with Investigations

Questar's stated policy is to proactively and 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 NYSED the full cost of NYSED's notification to 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.

Article III

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 their child's or the Eligible Student's Student Data stored or maintained by NYSED.

To the extent Student Data is held by Questar pursuant to the contract, Questar will respond within thirty calendar days to NYSED's requests for access to student data necessary for NYSED to facilitate such review by a parent or eligible student, and facilitate corrections, as necessary.

Should a parent or eligible student contact Questar directly to review any of the student data held by Questar pursuant to the contract, Questar commits to referring the parent or eligible student to NYSED and notify NYSED.

9. Outline how your data privacy and security program/practices materially align with the NIST CSF v1.1 using the Framework chart below.

[This field blank]

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

IDENTITY (ID)

Asset Management (ID.AM): *The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.*

Questar actively manages the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes, as part of which all such components are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

The Questar Assessment Asset Management policy applies to all individuals who are responsible for the use, purchase, implementation, and/or maintenance of Questar's computer hardware or software.

Physical and logical devices are inventoried through automated processes. Asset records are stored in a common location. Devices include physical and virtual servers, network devices, storage devices, and workstations. Purchased applications are also inventoried and tracked. Data flows and application diagrams are kept for critical applications.

Software utilized within the Questar environment will be standardized where possible. By standardizing the software utilized in the corporate environment the Service Desk in conjunction with the IT Security department will be able to maintain the highest security levels possible.

Questar devices that are detected on the corporate network using a version of software that is in violation to the compliance section of the policy will have its ability to access corporate resources removed until the device can be brought up to the standardization levels set forth by the IT enterprise team.

Additional guidelines of Questar's asset management policy include:

- Hardware and software used to conduct business on behalf of Questar Assessment will be provided by the company.
- Use of personally-owned computing hardware or software on Questar networks is not permitted.
- If additional hardware or software must be purchased, approval must be attained by the department manager/supervisor and Director of IT or designated approvers for those roles.
- Software used by Questar employees, contractors and/or other approved third-parties working on behalf of Questar, must be properly licensed.
- Maintenance, upgrades, or modifications to company devices should be performed by Questar Service Desk personnel.

- 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-to-day responsibility for asset management at Questar is the responsibility of the IT Enterprise Services team.

Business Environment (ID.BE): *The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles,* responsibilities, and risk management decisions.

Questar is a K–12 assessment provider that is single-mindedly focused on bridging the gap between accountability and learning.

To achieve this goal, we research, design, and manage innovative assessment programs for state and local education agencies; develop technologies to make assessments more efficient and effective; and pride ourselves on providing a high-touch experience to gain and keep the utmost level of trust.

Questar's vision is for a world in which all educators use meaningful assessment to directly improve instruction and fully prepare students for college or career.

Driven by this mission and pursuing these goals, we partner with states like New York in the critical work of assessing students for federal accountability purposes, among others. Stakeholders include state administrators, educators, parents, and students.

Our business environment thus involves vital work that demands—given the work involves student data and PII—the highest standards of cybersecurity, which in turn directly informs Questar cybersecurity roles, responsibilities, and risk management decisions.

Governance (ID.GV): *The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.*

The policies, procedures, and processes critical to managing and monitoring Questar's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk, which is owned by our Executive Security Council.

Questar Executive Security Council owns the organizational Information Security Program, which is the blueprint for the organization's security processes, policies, technologies, and organizational structures, and is based around data security and privacy best practices, including the NIST Cyber Security Framework.

This cross-functional team possesses the skills and seniority level to ensure that Questar security practices are evaluated from multiple perspectives and that all functions (technology, operations, finance, etc.) have an active voice in making security policy and risk management decisions.

The Executive Security Council meets quarterly to review concerns that may have arisen during the quarter, to analyze and manage potential new security risks, to review and update security policies as necessary, to identify areas that should be addressed during annual security training, and more.

The group also stays apprised of many state and federal laws and regulations to which our work is subject, including:

• New York Education Law § 2-d

• Family Educational Rights and Privacy Act

• Children's Online Privacy Protection Rule

Part of Questar's Information Security Program involves ensuring that all related security requirements are understood by staff, which we detail in the training that is required of staff. In addition, Questar's cybersecurity policies are posted on our intranet site. Policies are communicated during the on-boarding process and as needed to communicate updates. A corporate document library is also used to store procedures and diagrams.

Employees also must review and sign Questar's Code of Conduct upon being hired, and also review and attest to on an annual basis, which enumerates the most critical aspects of employee responsibilities in regard to security and privacy.

In keeping with the seriousness with which Questar views our responsibility for maintaining the security of client and stakeholder data, Questar policies and Code of Conduct make clear that personnel found to have violated Questar policies may be subject to disciplinary action, up to and including termination of employment and related civil or criminal penalties.

The Executive Security Council meets regularly to manage security governance issues. The group is comprised of leaders from across the organization.

Risk Assessment (ID.RA): *The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.*

Questar maintains a Security Audit policy that requires annual risk assessment. Systems are scanned regularly for technical vulnerabilities. The issues discovered are prioritized and then remediated. Organizational security assessments are performed annually.

Internal and external threats to systems and services in the public cloud are identified and documented by the cloud platform vendor. Threats to systems and services in our private cloud are identified and documented by our third-party Security Operations Center (SOC).

We receive cyber threat intelligence from a variety of sources, including, but not limited to:

- Vendor Technical Security Notifications
- Regular meetings with our third-party Security Operations Center (SOC)
- CERT vulnerability announcements

Risk Management Strategy (ID.RM): *The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.*

Questar maintains a Risk Management Policy to ensure Questar conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of data held by Questar Assessment.

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 conduct an accurate and thorough risk analysis to serve as the basis for Questar's 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.

Questar's current practice is to contract with a third-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): *The organization's priorities, constraints, risk 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 reliability and ability to meet the security and regulatory compliance needs of Questar and our customers.

A key vendor used to host Nextera is AWS. AWS provides public information about the state of their compliance. That documentation can be found here https://aws.amazon.com/compliance/programs/

In many cases, Questar contracts with subcontractors to conduct specialized components of the contract, as we do on behalf of our contract with NYSED. When a subcontractor is being considered to complete work for a Questar project, corporate capabilities are requested for new subcontractor or reviewed for existing vendors.

If there is agreement with our client that the vendor is qualified and a good fit, then the vendor is contacted to determine availability. If the vendor is capable and available, the vendor and a representative from the department for which the vendor will work (e.g., Assessment Development Manager), work together to complete required paperwork (Master Services Agreement, NDA, tax forms, etc.) and complete a Statement of Work (SOW) that takes into account contract requirements and project schedules.

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.

A key component of Questar's security strategy is our methodology for controlling internal user access to systems and data, which we achieve with a strong password policy, limitations on user access, multi-factor authentication, frequent audits, and the use of redundant security strategies (defense-in-depth).

All Questar electronic systems, applications, and data environments require user accounts to access. Accounts are only issued to Questar employees, contractors, and temporary staff after they have been subject to background checks, completed training, and signed non-disclosure agreements.

Access is provisioned through a central Service Desk function. The Service Desk manages the lifecycle of identities within Questar. Access requests are documented in a ticketing system, along with approval from the user's supervisor. Only sufficient access for an employee's job function is granted. Physical, logical, and remote access are all managed in this same manner.

User accounts are issued by a centralized team. Questar's network and systems require usernames and passwords for access, with passwords subject to frequent change, and multi-factor authentication. Password fields mask user input, and all logins are via SSL, with password transmissions occurring in SSL and encrypted with at least 256-bit encryption.

The access that we assign to users is governed by the concept of least privilege; users are given the access required to efficiently perform their job functions and no more. Only the appropriate employees have access to the directories or systems in which sensitive information resides (answer keys, score conversion tables, student demographics).

Questar's network is segmented to separate employee networks from production and edge networks. Network access is managed through Questar's network team. Only necessary network ports are opened for business applications to perform as needed.

Access controls are in place for all operating systems, applications, networks, and mobile systems. Systems check each user's access privileges at log in, and automatically 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 system utilities
- Secure communications over mobile computing devices

Systems automatically log users out after periods of inactivity and Questar workstations and laptops are locked when left unattended. Upon the user's return, they are prompted to enter their user ID and password.

All user activities are tracked. Questar's online systems maintain event logs on date, time, user ID, device, device configuration, and IP address in an audit log. The log information can be analyzed using an SQL interface and can be provided upon request.

Our internal security processes include frequent auditing of user account, with a variety of audit strategies in place to identify potential risks or violations of Questar user security policies.

Employee termination checklists ensure account termination is performed. This applies not only to employees who have left the organization, but also to those who may have changed job functions within Questar and therefore may have different access to certain accounts.

In addition to these systems and strategies for controlling internal electronic access to Questar systems and data, the physical components of Questar's internal network (e.g., servers, switches, and firewall) are located in a secure data center, with access limited and user access tracked.

All of these approaches and tools are part of Questar's overarching defense-in-depth strategy, which uses coordinated layers and mechanisms to ensure the security of client data.

Awareness and Training (PR.AT): *The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.*

Employees receive security training when joining Questar and then annually thereafter. Questar employs designated people responsible for physical security and cybersecurity. Additionally, users understand when and if their role requires privileged access.

Questar maintains a documented Awareness and Training policy, and employees and contractors are required to participate in and successfully pass two separate trainings in support of the policy: Security Awareness and Personally Identifiable Information security trainings.

The Security Awareness course covers key security best practices end users should follow so they can prevent, detect, and respond to information security threats. It is designed to cover all of today's critical security topics, such as password management, identity theft, malware, social engineering, phishing, spear phishing, physical security, business email compromise, Internet of Things (IoT), travel safety, mobile data, privacy, and acceptable use.

The course was developed by Inspired eLearning, a leader in security training with a focus on training that achieves more effective and measurable changes in organizations, with content created by instructional design professionals and backed by cybersecurity experts.

All Questar employees are required to re-certify their mastery of Security Awareness annually.

The Personally Identifiable Information course is designed to ensure that Questar staff are fully prepared to meet the high-standard of PII-protection that our customers expect, as well as mandated by state and federal law.

This mandatory course covers what constitutes PII, where it is typically found, appropriate and limited circumstances for accessing PII, how employees should (and should not) handle PII, and required steps in the unlikely event of unauthorized disclosure of PII.

Both of these mandatory security training courses are delivered online through an interactive design that engages employees in learning and concludes with a required test that must be passed to successfully complete the course.

In the course of training, employees must also access, read, and assert compliance with Questar's official IT Security Policies, including Data Retention and Destruction Policy, Security Awareness and Training Policy, Media Use and Destruction Policy, and Removable Media Policy.

In addition to these trainings, internal technology infrastructure employees are trained in data retention, disaster recovery, and business continuity workflows. They also participate regularly in quality improvement conference sessions. Questar employees stay current on strategies for protecting data, materials, and the interests of students and state departments of education.

Data Security (PR.DS): *Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.*

Data is protected while at rest using native encryption technologies such as Microsoft SQL's TDE and AWS S3-Managed encryption keys. AES-256 encryption is used in both solutions. Storage solutions are monitored to ensure they are available and have adequate capacity and performance.

Data is also protected while in transit. TLS with AES ciphers are used to secure data over public networks between applications and user end points. IPSEC is used to secure data in transit between Questar's 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.*

A key component of Questar's Information Security Program is 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 requirements of Questar's large-scale state assessments clients.

Questar's core security policies include Appendix R Data Privacy Forms section of our proposal, and include Asset Management, Audit Policy, Breach Management and Notification, Building Security, Code of Conduct, Data Retention and Destruction, Incident Management, Malicious Software, Media use and Destruction, and Removable Media Policy.

Policies are shared with employees when they join Questar. Access deprovisioning occurs within two business days of termination, but can be done immediately if requested.

Nextera environments are built using Infrastructure as Code techniques. Questar's implementation uses a source code repository along with software development practices to build and make changes to Nextera environments.

Changes are required to be documented in Request for Change (RFC) tickets, which capture details of the change, risk, impact, and purpose. RFCs are approved by the Production Control Board in accordance to their risk and impact.

Questar has documented business continuity and disaster recovery plans covering all aspects of the business, including IT.

Questar has comprehensive capabilities and practices in place for tracking, logging, and auditing user activity within the online environments we maintain, given the important part such practices play in a successful security program.

Questar software applications—both our internal environments and those made available to customers—are housed on secure enterprise-grade SQL database servers that are only accessible via encrypted HTTPS protocol, with access to the systems is controlled by Questar's comprehensive identity management.

All users are required to log in for access. All logins are via SSL, with password transmissions occurring in SSL and encrypted with at least 256-bit encryption. Subsequently, all user activities are tracked, with systems maintaining event logs on date, time, user ID, device, device configuration, and IP address in an audit log.

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.*

Questar strives to continuously improve its security posture. Whenever there is an event that requires an RCA, we have follow-ups to determine how to make improvements. We have detection testing and communication chains for those events. Additionally, we are always exploring new security software and updates to the way we monitor the network.

The hosted AWS data center in which we deploy NYSED's assessment system is also monitored using global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

The Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities are performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

We also work with a number of AWS tools as part of our strategy for protecting client production instances, in AWS CloudTrail, which is a service that enables governance, compliance, operational auditing, and risk auditing of AWS accounts.

With CloudTrail, Questar can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of the New York Nextera account activity on AWS, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

Detection Processes (DE.DP): *Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.*

Questar's server room has access restriction, security cameras, and regular walkthroughs to detect any unauthorized entry. A security vendor monitors the network. Antivirus software is on all desktops, physical servers, and cloud servers to prevent and detect any malicious code. We complete vulnerability scans regularly as well as logging and monitoring against external service providers.

Response Planning (RS.RP): *Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.*

Questar maintains incident management and breach notification processes and policies to ensure efficient and effective response to detected cybersecurity incidents. The policies are periodically reviewed and, per the policy, the processes are tested annually.

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 case of New York, we understand Questar's duty 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 breach).

As required by the RFP, the program manager will immediately notify the Director of State Assessment, or his/her designee, via telephone and in writing of the issue and Questar's proposed solution. Questar will also include the issue and NYSED approved solution on any subsequent report(s).

We will also abide by additional requirements to which we are subject, which may include providing notifications in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified mail, and must to the extent available, include a description of the breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Questar's investigation; and the name of a point of contact.

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.*

Questar'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.*

Once a security incident is discovered, Questar's Chief Information Security Officer (CISO) works with the technology teams to implement a plan to recover from a breach. The plan takes into consideration the scope, impact, and vector of the attack.

NYSED's online production environment, related applications, and data are subject to strategies designed to minimize risk in the event of disaster and ensure business continuity. These include redundant server configuration, frequent backup of data, and the ability to rapidly failover.

In particular, the servers that will support NYSED will be virtualized so the application sits on a virtual container or virtual machine on the server and will be clustered and work in unison to support core applications and processes. They are then load-balanced to create two separate processing domains that can work in conjunction with each other and can be maintained separately.

Constant monitoring is maintained between the devices to determine the state of any one device. Questar's servers are configured with failover partners, so if a server becomes unresponsive, the secondary server takes over processing.

Our standard maintenance processes include verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs and using actual NYSED data sets that mirror production data.

In addition to our redundant server configuration, Questar's business continuity and disaster recovery strategy is significantly enhanced by the strategies and resources of our hosted data center, AWS. AWS provides exceptional resources for the redundancy and continuity strategies, including their renowned 99.99 percent uptime SLA.

Availability Zones are the core of the AWS infrastructure architecture and they form the foundation of AWS reliability and operations. AWS builds its data centers in multiple geographic regions as well as across multiple Availability Zones within each region; regions are isolated from each other and Availability Zones are in completely separate buildings miles apart for complete redundancy.

Availability Zones are designed for physical redundancy and provide resilience, enabling uninterrupted performance, even in the event of power outages, internet downtime, floods, and other natural disasters.

Availability Zones are structured so that Questar can architect applications that automatically fail-over between Availability Zones without interruption. Through the use of Availability Zones and data replication, AWS provides extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

Questar also employs a data backup solution for added levels of assurance to our clients. We work with Veeam Backup to centrally manage backups, creating a backup frequency and retention policy, including client data/environments. This ensures automatic backup to our AWS hosted data provides tools for monitoring backup compliance and restoring data.

With Veeam Backup, Questar can configure backup policies from a central backup console, simplifying backup management and better ensuring that application data is backed up and protected. Veeam Backup will encrypt NYSED data in transit and at rest.

Improvements (RC.IM): *Recovery planning and processes are improved by incorporating lessons learned into future activities.*

Questar's CISO performs a post-incident retrospective to discover and prioritize improvements to process and technology to prevent future breaches.

One tool that Questar uses to ensure lessons learned are methodically incorporated into future actions is a formal Corrective and Preventive Actions (CAPAs) plan, which is a form of documentation generated by our post-incident retrospectives

CAPAs are assigned with a true focus on action and closely tracked to completion. The goal of all CAPAs identified is to have them implemented within thirty days of assignment. To ensure adequate operationalization of CAPAs, critical CAPAs will be audited for their implementation and effectiveness.

CAPAs will be collected for each completed causal analysis. The CAPAs are stored in the causal analysis repository with other artifacts for the completed causal analysis. Each CAPA will have the following information collected:

1. A description of the action to be taken
2. The owner to whom the action is assigned
3. Identification of the cause (root or contributing cause) the action is meant to address
4. The date the action is to be completed
5. A designation if the CAPA is to be audited and, if so:
    a. The measurement of effectiveness (how is the action to be audited?)
    b. The date to complete the audit
6. Status of the action – updated periodically to completion

To ensure adequate operationalization of CAPAs, all CAPAs will be audited for their implementation and effectiveness. The criteria for measuring a CAPAs effectiveness will be identified as the CAPA is identified and assigned.

Also, the date to complete the audit of the CAPA is identified. It may be the case that a CAPA cannot be audited until many weeks or months after it has been implemented due to the cyclical nature of the business.

The status of the CAPA audit will also be tracked with the CAPA itself including any evidence to support the findings of the CAPA audit. CAPAs that do not provide sufficient evidence of effectiveness and/or operationalization will be escalated as appropriate.

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).*

Questar's VP of Partner Effectiveness and the State Director 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.