STATE OF NEW YORK

JUDICIARY

–REQUEST FOR PROPOSALS–

(This is not an order)
PROPOSAL MUST BE MADE ON THIS SHEET OR AS OTHERWISE SPECIFIED

RFP Number: **RFP # OCA/DOTCR-131**	**Cybersecurity Services**
Opening Date: July 6, 2023 **Time: 3:00 PM EDT** **Issue Date: May 26, 2023**	

NYS OFFICE OF COURT ADMINISTRATION
Office of Grants and Contracts
2500 Pond View, Suite 104
Castleton-on-Hudson, NY 12033

Direct Inquiries to: Kathleen Roberts
E-mail: kmroberts@NYCOURTS.GOV

All prices to be net and inclusive of all services specified herein unless otherwise specified.

OFFICE OF GENERAL SERVICES "GENERAL SPECIFICATIONS" (APRIL 2016) ARE FULLY INCORPORATED HEREIN.

UCS ATTACHMENT I , III, and IV ATTACHED & INCORPORATED HEREIN.	**ALL BID RESPONSES MUST BE ENTERED ON THE ENCLOSED BID RESPONSE FORM UNLESS SPECIFIED OTHERWISE HEREIN.**

NOTICE TO BIDDERS

Pursuant to the Rules and Regulations of the Chief Administrator for the Courts, sealed bids for furnishing the item(s) in this Request for Bid will be received at the above address. When submitting a bid, you must:

1. Complete this form in its entirety using ink or typewriter and return with all other documents.

2. Explain any deviations or qualifications if your bid deviates from the specifications. If necessary, attach a separate sheet setting forth such explanations.

3. Sign the bid. The bid must be completed in the name of the bidder (corporate or other) and must be fully and properly executed by an authorized person.

4. INDICATE THE BID NUMBER, THE BID OPENING DATE AND TIME ON THE ENVELOPE CONTAINING THE SEALED BID.

5. Mail the bid to the above agency address in sufficient time for it to be received before the specified bid opening. **LATE BIDS WILL BE REJECTED.**

BIDDER HEREBY CERTIFIES THAT THE ABOVE QUOTED (OR OTHERWISE NOTED) PRICES ARE APPLICABLE TO ALL CUSTOMERS FOR COMPARABLE QUANTITIES, QUALITY, STYLES OR SERVICES.

BIDS MUST BE SIGNED

Bidder's Firm Name:		Employer's Federal Identification Number: NYS Vendor ID Number:	
Address Street	City	State	Zip
Bidder's Signature		Official Title	
Printed or Typed Copy of Signature		Area Code/ Telephone Number E-mail:	

CONTENTS

DOCUMENT ENCLOSURE CHECKLIST

BID CONTENTS

Attachments

Exhibits

DOCUMENT ENCLOSURE CHECKLIST (2 pages)

☐ Exhibit A – Pricing Sheet: Exhibit A must be fully executed and included in bidder's proposal. *Failure to do so may disqualify bidder's response.*

The following forms must be fully executed and included in bidder's proposal.
Failure to do so may disqualify bidder's response:

☐ UCS Request for Bid/Proposal Form (UCS RFB.001.Cover.(Rev.4.22)) and complete bid response with original signature

☐ Attachment I - Standard Request for Bid Clauses & Forms
- ☐ p.3 - Non-Collusive Bidding Certificate
- ☐ p.4 – Acknowledgment of Individual or Corporation

☐ Attachment II - Not Applicable

☐ Attachment III - Vendor Responsibility Questionnaire
- ☐ Questionnaire filed online via OSC VendRep System and certified within 6 months of the bid opening due date, or
- ☐ Paper questionnaire

☐ Attachment IV - Procurement Lobbying forms
- ☐ Disclosure of Prior Non-Responsibility Determination (UCS 420)
- ☐ Affirmation of Understanding and Agreement (UCS 421)

☐ Certificates of NYS Worker's Compensation and NYS Disability Benefits Insurance, or Certificate of Attestation of Exemption.
Please see paragraph "Insurance Requirements" for a list of accepted forms.

☐ Copies of bidder's certificate(s) of insurance or other adequate proof evidencing the insurance coverages required by the bid specifications.

☐ One (1) complete photocopy of original bid response (applicable only if responding with a paper bid submission).

☐ Signed Document Enclosure Checklist

☐ Proprietary information in separate folder from bid response, if applicable

In addition, bidder shall provide:

☐ Contractor Certification to Covered Agency (Form ST-220-CA)

☐ Firm Offer to the Unified Court System and Conflict of Interest Disclosure (see Exhibit B)

☐ Resolution or equivalent authorization of the bidder organization (see Exhibit B – Firm Offer Letter)

☐ Contractor Certification to Meeting Minimum Bidder Qualifications set forth in Exhibit C

Continued on next page

DOCUMENT ENCLOSURE CHECKLIST (continued)

☐ Narrative Responses indicating how the Bidder's proposal satisfies the technical components set forth in Exhibit D

☐ List of references set forth in Exhibit G

IMPORTANT:

1. All documents requiring an original signature must bear the BLUE INK signature of the same authorized individual. Signatory notarization must be that of the person whose signature is affixed to all required documents.
2. Exhibit A – Pricing Sheet and the other forms listed above must all have the SAME COMPANY NAME AND TAX ID NUMBER in order for a purchase order or contract to be approved by the NYS Comptroller.
3. **Do not alter this solicitation in any manner. Any changes, deletions, or additions (including the addition of supplemental terms and conditions) to this RFP or to any exhibits or appendices to this RFP, including Exhibit A – Pricing Sheet, may result in the rejection of the bid as non-responsive.**
4. Please note that the terms and conditions of this RFP will form the basis of the contract with the Awarded Contractor (defined below).
5. **Bidder Contact Information**

   Bidder's Primary Contact for Bid Matters:

Name:			
Street:			
City:		State:	Zip:
Telephone Number:	Email:		

6. **Verification:**

Authorized representative of Bidder must complete and sign below to verify submission of all documents required per the Document Enclosure Checklist:	
COMPANY NAME:	
AUTHORIZED OFFICER'S NAME AND TITLE:	
SIGNATURE:	DATE:

I. OVERVIEW

1.1 Purpose and Scope

The New York State Unified Court System ("UCS"), Office of Court Administration ("OCA"), Division of Technology and Court Research ("DoTCR") seeks sealed proposals from responsive and responsible organizations able to provide and implement Security Operations Center ("SOC") services as described herein to UCS. SOC services must align with security standards and requirements set forth below, and the services provided must include endpoint detection and response, 24×7×365 monitoring and alerting, incident detection and response, vulnerability management and remediation, and on-demand security expertise. These services will help UCS mitigate security risks and augment staff resources to provide a more secure computing environment.

**** See ARTICLE V BELOW, SCOPE OF WORK for detailed specifications. ****

1.2 Key Bid Dates

EVENT	DATE
Bid Issue Date*	May 26, 2023
Written Bid Question Due Date	June 9, 2023
Pre-Bid Conference Date	June 16, 2023
Publishing of Responses to Questions	June 22, 2023
Bid Submission Deadline Date	July 6, 2023
Selection of Finalists	July 31, 2023
Oral Presentations and/or Product Demonstrations by Finalists	Week of August 14, 2023
Best and Final Offers Deadline from Finalists (if applicable)	August 31, 2023
Estimated Contract Start Date	October 1, 2023

***OCA reserves the right to modify any Key Bid Date as it may deem appropriate.**

II. MINIMUM QUALIFICATIONS AND MANDATORY REQUIREMENTS

Bidders are advised that UCS intends to ensure that only responsive, responsible qualified and reliable entities enter into a contract to perform the work defined in this RFP. UCS considers the following qualifications, sufficiency, capacity, and experience to be prerequisite in order to be considered a qualified bidder for purposes of this RFP.

Using the form set forth in Exhibit C, bidders must certify that they meet the minimum qualifications set forth below and that their proposed solution satisfies the mandatory requirements set forth below.

Minimum Qualifications:

1. The bidder has been in continuous operation providing managed security/SOC services as one of its primary lines of business for at least the past three (3) years;

2. The bidder currently monitors a minimum of 2500 firewall/intrusion detection systems (IDS)/intrusion prevention systems (IPS) devices across its aggregate customer base; and

3. The bidder currently monitors a minimum of 100 billion log lines per month across its aggregate customer base.

Mandatory Requirements:

1. The proposed solution must comply with Systems and Organization Controls 2 (SOC 2®) requirements as developed by the American Institute of Certified Public Accountants;

2. All UCS data must remain in the continental United States, and select data must remain on UCS premises as further outlined herein ("Data Requirements");

3. The proposed solution must comply with Federal Risk and Authorization Management Program (FedRAMP®) Moderate or High Impact Level Security Controls Baseline;

4. The proposed solution must be operational 24 hours/day × 365 days/year with staffing at or exceeding the levels in Section 5.3 (Required Staffing) herein;

5. The proposed solution must integrate with the existing UCS Splunk Security Information and Event Management (SIEM) system (600 GB/day license) and scale up without installation of proprietary vendor hardware;

6. The proposed solution must include access to SOC Level 1, Level 2, and Level 3 analysts as needed for incident response purposes;

7. The proposed solution must operate within and integrate with UCS Software and Environment, including its ticketing system, as defined in Section 5.1 (Current State);

8. The proposed solution must supply a full-time Splunk engineer (staff member or subcontractor) to create custom searches and upgrades as needed for the UCS Splunk environment;

9. The proposed solution must not require UCS to install any applications, programs, or other software on systems owned or maintained by UCS; and

10. The proposed solution must comply with NYS Office of Information Technology Services Security Policy No. NYS-P03-002 (as set forth in Exhibit H), and it must be NIST Tier 4 compliant.

III. AWARD

3.1 Term of Award

A single estimated quantity term contract ("Contract") will be awarded to the successful bidder ("Awarded Contractor") for an Initial Term of three (3) years ("Initial Term"). The Contract is expected to commence on or about October 1, 2023. OCA reserves the right to renew such Contract for two (2) additional one (1) year periods (each, a "Renewal Term") upon the same terms and conditions excluding pricing.

OCA further reserves the right to extend the Contract for a period not to exceed six (6) months ("Extension Term"), upon written notification to Awarded Contractor prior to the expiration date of the Initial Term or a Renewal Term, upon the same terms and conditions including pricing as the preceding Term; provided, the maximum term of the awarded contract will be five (5) years. The Contract, renewals and extension thereof are subject to the approval of the NYS Attorney General and the NYS Comptroller.

3.2 Method of Award

The selected awardee must (1) meet the minimum qualifications and mandatory requirements outlined in Article II above and certified to UCS; (2) be a Responsible Bidder as determined in accordance with the criteria in Article VIII; and (3) receive the highest composite (technical + cost) score in excess of the minimum score as determined by the selection criteria and scoring methodology set forth herein.

Responsibility is determined in accordance with the criteria articulated in the "Responsible Applicant" paragraph set forth in Article VIII (Bid Terms and Conditions).

Proposals will be reviewed and rated by an evaluation committee made up of qualified UCS staff. The technical scores of each committee member will be averaged to determine a preliminary technical score. UCS may deem one or more of the bidders with the top preliminary scores as preliminary finalists and ask that they provide a product demonstration or oral presentation. Any such demonstration or interview will be conducted in accordance with Section 3.3 hereof. Final technical scores, determined pursuant to Section 3.3, will be combined with cost scores as described herein to arrive at a preliminary composite final score. UCS may then either recommend a bidder for award as indicated in this section or request best and final offers (BAFOs) as described in Section 3.4. If BAFOs are requested, a final cost score for each finalist bidder will be determined in accordance with Section 3.4. Final technical scores will then be combined with final cost scores to determine a final composite score among Finalist Bidders (as hereinafter defined).

In the event of a tie composite score, the applicant with the higher cost score will prevail. When price and other factors are found to be substantially equivalent, UCS will select the winning bidder in its sole discretion.

Proposals will be scored as follows:

Technical Criteria	**Maximum Points**
Organizational Capacity	*174*
Business and Technical Specifications	*534*
Maximum Technical Criteria Points	**708**
Cost: Maximum Cost Points	**200**
Maximum Total Points	**908**

3.2.1 Scoring for Technical Criteria

Criteria for organizational capacity and technical proficiency are contained in Exhibit D hereto.

As explained in Section 6.2.2, below, and Exhibit D, bidders must submit a narrative response addressing how the bidder and/or its proposed solution satisfies each desired attribute or needed feature ("Component"). Components appearing in bold text in Exhibit D pertain to a mandatory qualification or minimum requirement set forth in Article II.

Components are grouped in categories (see Section 6.2.2, below, for a list of categories).

Evaluators will rate the response to each Component and assign 0, 1, 2, or 3 points using the following scoring rubric:

Scoring Rubric	
Points	**Criteria**
3	The response thoroughly describes how the solution: (i) will deliver the Component; (ii) is feasible; and (iii) is highly likely to result in the successful implementation of the solution.
2	The response adequately describes how the solution: (i) will deliver the Component; (ii) is feasible; and (iii) is likely to result in the successful implementation of the solution.
1	The response minimally or inadequately describes how the solution will deliver the Component and is unlikely to result in the successful implementation of the solution.
0	The solution either is not feasible or does not describe how the solution will deliver the Component.

Each Component also has a relative weight of 1, 2, 3, or 4 as indicated by the number of stars corresponding to that Component in Exhibit D.

For each Component, evaluators will multiply the points assigned per the scoring rubric above by the relative weight assigned for that Component to arrive at a weighted score. Within each category, the weighted scores for each Component are added together to arrive at a Category Score. The Technical Criteria score is the sum of all Category Scores. The maximum available Technical Criteria score is 708 points.

Note: A minimum Technical Criteria point score of 425 (average of all evaluators) is required for an award to be made.

3.2.2 Scoring for Cost

Proposals will be scored for cost based on information supplied in bidder's Exhibit A – Pricing Sheet. Cost points will be awarded exclusively on the annual costs supplied in Exhibit A – Pricing Sheet for onboarding and SOC services.

The proposal with the lowest Combined Annual Cost as shown in Exhibit A – Pricing Sheet will be awarded two hundred (200) cost points (the maximum available for the category titled "Annualized Costs"). Each proposal with a greater Combined Annual Cost will be awarded cost points in that category according to the following formula:

$$Lowest\ cost\ proposal\ \div Higher\ cost\ proposal\ \times\ 200$$

For example: Assuming the lowest Combined Annual Cost proposed is $100 and the next lowest Combined Annual Cost proposed is $125, the proposal with the $100 Combined Annual Cost would be awarded 200 points, and the proposal with the $125 Combined Annual Cost would be awarded 160 points based on the following computation:

$$100\ \div\ 125 =\ (.8)\ \times\ 200 = 160$$

The result of this equation will be rounded up or down to the nearest whole integer.

Bidders may, but are not required to, supply rates for services billed on a time and materials basis (see section 4.1, below). Any such rates will not be factored into bidder's score for cost.

3.3 Oral Presentations and Product Demonstrations

UCS reserves the right after rating and ranking the Responsible Bidders' proposals based on preliminary technical scores to invite one or more of the highest-scoring bidders to deliver presentations and/or demonstrate their proposed product(s)/service(s) ("Presentation") to UCS personnel. The UCS evaluation committee may revise technical scores based on the information and clarifications provided during the Presentation. Revised technical scores will be averaged among evaluators to develop a final technical score. UCS may, in its sole discretion, require the selected bidders to deliver any such Presentation in person or remotely. At least seven (7) calendar days prior to the scheduled Presentation, UCS will notify each invited bidder's primary contact for bid matters (as indicated in the bidder's Document Enclosure Checklist) of the date, time, location, and method of delivering the bidder's Presentation, and UCS will furnish such invited bidders with the criteria UCS will employ to evaluate each bidder's Presentation.

3.4 Best and Final Offers (BAFO)

UCS may request BAFOs on price from the bidders that are susceptible to award based off their respective preliminary final scores ("Finalist Bidders"). If negotiations or subsequent offers are solicited, Finalist Bidders shall provide BAFO(s) in response. Failure to deliver a BAFO when requested shall disqualify the non-responsive Finalist Bidder from further consideration. UCS will score BAFO(s) among Finalist Bidders in accordance with the cost evaluation methodology in section 3.2.2, above. The BAFO cost score will be combined with the final technical score of each Finalist Bidder to determine final composite scores.

IV. PRICING

4.1 Pricing

All pricing submitted pursuant to the solicitation shall be net f.o.b. destination unless otherwise expressly specified herein.

Other than the pricing submitted on Exhibit A – Pricing Sheet, there shall be no other charge, cost, reimbursement, or expense of any kind payable by UCS in connection with or arising from Awarded Contractor's performance of the services set forth herein. Awarded Contractor shall be solely responsible for all costs and expenses incurred in connection with the performance of such services.

Pricing shall be submitted only on, and in the format prescribed by, Exhibit A – Pricing Sheet. Bidder must provide pricing as requested in Exhibit A – Pricing Sheet.

Pricing will remain unchanged during the Initial Term.

4.2 Price Adjustments

Pricing shall be subject to increase as of the commencement date of each Renewal Term by the percentage equal to the lesser of: (i) the increase (or decrease) in the US City Average Index for all urban consumers for the category of all items before seasonal adjustments ("CPI") as of sixty (60) days prior to the commencement date of each such Renewal Term, over the CPI monthly index from the prior year, or (ii) five percent (5%). Pricing shall thereafter remain unchanged for the balance of each such term, and shall further remain unchanged during an Extension Term.

4.3 Payment

Awarded Contractor shall send true and accurate invoices (see Section 5.4, below).

Payment shall be made quarterly in arrears and shall be made upon submission by Awarded Contractor and approval by UCS of invoices satisfactory to UCS and OSC.

Payment for goods delivered/services performed under the awarded contract shall be conditioned upon the acceptance and approval of such items/services, such that it is sufficiently complete in accordance with the RFP specification, so that UCS can utilize the goods/services for its intended purpose.

V. SCOPE OF WORK

5.1 Current State

UCS employs approximately 16,500 judicial and nonjudicial personnel statewide to deliver equal justice under the law and to achieve the just, fair, and timely resolution of all matters that come before our courts. Cyber threats to government systems, including those of the court system, remain an area of ongoing and growing concern. UCS systems contain sensitive information and any compromise of UCS systems could lead to extensive damage to UCS and those who rely on its systems.

DoTCR provides infrastructure and application support, development, architecture, and engineering throughout the court system. UCS systems feature the following technologies: Avaya™ routers and switches; Barracuda™; Check Point™; Cisco™; CrowdStrike™; DNS; Extreme™ routers and switches; F5™ ASM (Application Security Manager), GTM (Global Traffic Manager), and LTM (Local Traffic Manager); FireEye™; Infoblox™; Jira™; Juniper Networks™; Microsoft Azure™; Microsoft Defender ATP™; Microsoft Office 365™; Microsoft Windows IIS™; Microsoft Windows™; Palo Alto Networks™; Pulse Secure™; Qualys™; Sophos™; Splunk™; Squid Proxy; Tenable.sc™; Trend Micro TippingPoint™; and VMware™ (collectively, "UCS Software and Environment").

The current DoTCR footprint includes 2,200 servers (1,000 physical O/S install, 1,000 VM/HyperV, and 200 Azure) and 65,000 devices on network, including 26,000 Windows PCs; 200 physical locations. UCS devices are deployed in courthouses through New York State; for information about the locations of courthouses, visit the Court Locator application on the UCS website: https://ww2.nycourts.gov/courtlocator

The successful solution must operate within the UCS Software and Environment, including integration with UCS's ticketing system (currently Jira™). Please note, however, that UCS Software and Environment are subject to change, and the Awarded Contractor will be contractually obligated to deliver ongoing SOC services as UCS updates or replaces existing technologies.

UCS Data Requirements: Data, including event logs and network flow data, remains on UCS premises and does not leave the UCS environment; however, metadata regarding security alerts may be entered into the selected contractor's ticketing system.

DoTCR's current Security Operations Center Provider ("SOCP") monitors in excess of 1.2 billion log entries daily from approximately 2,200 servers and 26,000 endpoints. The current SOCP provides access to a central log repository to assist in triaging incidents and uncovering new threats.

5.2 Statement of Work Overview

DoTCR is looking to procure an SOC solution from a responsive and responsible vendor that includes 24 hours/day, 7 days/week, 52 weeks/year capture, monitoring, analysis, and robust correlation of event logs and network flow data from sources such as, but not limited to:

- Intrusion detection systems/intrusion prevention systems
- Firewalls
- End-point Detection Response (EDR)
- Proxies
- Anti-virus
- Virtual Private Network (VPN) appliances
- Domain Name Service (DNS) / Dynamic Host Control Protocol (DHCP) servers

- Directory services
- Network flow monitors

For purposes of this procurement, UCS will follow New York State Office of Information Technology Services (ITS) Security Policy NYS-P03-002, as last updated on November 23, 2021. A copy of that policy is included as Exhibit H to this RFP.

The awarded SOC system must create electronic alerts based on defined priority criteria after validation and triage by an SOC analyst. This information must then be sent to one or more designated UCS security representatives via SMS and/or email. Vendor will be required to use the UCS Splunk™ environment to build correlation alerts, alert on any malicious events, and alert on critical, high, and medium events. Vendor will also tune alerts as needed and work with the UCS Splunk™ Security Orchestration Automation and Response (SOAR) tool within the UCS environment.

UCS will not install any additional software on its systems as part of the SOC solution. All UCS data must remain in systems physically located in the contiguous United States. All work logs will stay on UCS premises.

A portal for access to the raw logs collected and a dashboard for event information must be available for further contextual analysis and response activities. The SOCP team should forward only filtered and verified information for UCS action or take action themselves (e.g., disabling accounts and resetting tokens) consistent with a service level agreement (SLA), runbooks, and playbooks to be negotiated and approved by UCS and the selected bidder. Expertise and guidance are expected; simply forwarding abnormality alerts does not meet the standard of what UCS expects from the selected SOCP.

The SOCP's correlation should focus on detected attacks, known vulnerabilities, and known threat actors, including those that would target UCS. Below are sample cases that would be applicable for the SOC:

- Identify anomalous traffic or activity, such as spikes in log volume;
- Identify and alert on attempted attacks against known critical servers that are vulnerable;
- Identify traffic to or from potentially malicious sites; and
- Identify potential sensitive data exfiltration.

The selected solution is expected to:

- Automate the data collection, normalization, storage, correlation, transformation, and analysis functions to establish security baselines.
- Monitor, detect, respond, and remediate threats in conformity with standards, guidelines, and best practices of the National Institute of Standards and Technology ("NIST").

- Identify potential information security issues that are too complex and might not be visible to human eye.

- Meet or outperform the Service Performance Requirements as specified in Table 2 of Exhibit F (SOC Terms and Conditions).

- Ingest multiple user identity data stores (for example, Active Directory, application database accounts, non-Windows based account, etc.) into the Security Information and Event Management (SIEM) system, correlate and analyze that information, and use it to discover end-user usage patterns to identify anomalies.

- Meet or outperform the managed SIEM service levels in Table 1 of Exhibit F (SOC Terms and Conditions).

As set forth in Exhibit F (SOC Terms and Conditions), the selected bidder will provide a Consensus Assessment Initiative Questionnaire (CAIQ) for UCS's review within thirty (30) days after execution of the contract resulting from this RFP and annually thereafter.

5.3 Required Staffing

Key Personnel: The selected bidder must provide a single point of contact for contract management (Contract Manager) activities and a single point of contact for service management (Service Manager). These points of contact may be the same individual. The contact(s) must be able to respond to routine requests for assistance not more than two business days from initial request and must be available by phone or email during normal business hours (Monday – Friday, 9:00 AM – 5:00 PM Eastern Time). The selected bidder must provide UCS with the contact information for backup personnel if the Contract Manager or Service Manager is unavailable. Pursuant to the contract resulting from this RFP, the selected bidder and UCS will periodically review contact information for personnel supporting the SOC solution and will notify each other of changes to such personnel or to changes to the contact information for such personnel.

Contract Manager: The contract manager will be responsible for the following activities:

- Managing all onboarding and offboarding activities of the SOC Solution

- Communication and scheduling of onboarding and offboarding activities

- Assist with migration from existing service provider's service to bidder's service

- Assist with migration off bidder's service at the end of contract

- Contract issue resolution as needed and requested by UCS

Service Manager: The service manager will be responsible for the following activities:

- Work with UCS's DoTCR designee to document and ensure adherence to service level requirements, including issuance of credits, and develop service level metrics and reports.

- Review service level exceptions, determine contributing factors, and institute changes through a continuous improvement process.

- Develop an escalation process for reported problems or issues related to the services and ensure resolution in coordination with UCS, including, but not limited to, root cause analysis and proposed resolution for any outage or failure to escalate an event.

- Produce service level reports and compare results with negotiated Service Level Agreements, if applicable.

- Train users regarding use cases, reporting functions, features, and overall use of the service portal.

- Provide security advisories and recommendations, as well as new service features the provider may offer, or new releases of existing features, as applicable.

- Advise on tuning of alerts on security devices to reduce false positives and false negatives.

Splunk Engineer: As stated in the Mandatory Requirements set forth in Article II, the proposed solution must supply a full-time Splunk engineer (staff member or subcontractor) to create custom searches and upgrades as needed for the UCS Splunk environment.

In addition to supplying the individuals identified above, the successful SOCP must ensure that at least three (3) qualified security analysts are available to support UCS to respond to identified incidents during daytime (7:00 AM – 5:00 PM Eastern Time) and evening shifts (5:00 PM – Midnight Eastern Time) and that at least two (2) qualified security analysts are available to support UCS to respond to identified incidents during overnight (Midnight to 7:00 AM Eastern Time) shifts. All employees assigned to the UCS account must be physically located in the continental United States. All Awarded Contractor personnel or subcontractors that will have access to the SOC Solution and to UCS data must have a security background check performed prior to commencing work under the resulting contract. Awarded Contractor is responsible for performing all background checks and security clearances of their workforce and subcontractors and shall provide proof of compliance therewith upon request from UCS.

Please note: The scope of work for this RFP excludes onsite incident response (IR) services. UCS currently maintains a relationship with an identified vendor for onsite IR services. The successful SOCP will, however, need to cooperate with the existing onsite IR services vendor as needed.

5.4 Preferred Components of Bidder's Proposal

Bidder's proposal should indicate: (i) the bidder possesses the preferred attributes described below; and (2) the proposed solution includes the preferred features described below. Such attributes and features are in addition to the minimum qualifications and mandatory requirements set forth in Article II and augment the attributes and features discussed in the Statement of Work Overview and Required Staffing (Sections 5.2 and 5.3, respectively) sections of the RFP. The preferences below are reflected in the scoring instrument.

Organizational Capacity – Capabilities

The preferred bidder will have multiple SOCs, and all SOCs assigned to the UCS account will be in the continental United States as specified in Section 5.3 (Required Staffing). Moreover, the preferred bidder will have SOCs in multiple time zones within the United States.

The bidder's proposed solution will feature a ticketing system with role-based access controls so that other customers cannot access UCS data. Additionally, the bidder's policies, procedures, and audit requirements ensure that UCS data is available only to SOC personnel who have passed applicable and appropriate background checks.

The ideal solution will guaranty at least 99.982% uptime, and bidder has a comprehensive plan that relies on redundancies to ensure that bidder can deliver continuity of service to UCS.

While subcontracting is permitted, UCS disfavors proposals where the bidder's subcontractors rely on other entities (i.e., subcontractors of subcontractors) to perform work under the contract resulting from this RFP. All subcontractors must be located in the continental United States.

UCS favors proposals from vendors with experience providing cybersecurity services to public entities comparable to UCS.

Organizational Capacity – Staffing

The preferred bidder will ensure that the employees or subcontractors assigned to the UCS incident response team will have on average a minimum of five (5) years' experience, and the bidder will supply at least fifteen (15) employees to the UCS SOC. Also, the employees assigned to the UCS SOC will work in different time zones in the United States.

To address UCS concerns about turnover, the preferred proposal will demonstrate that bidder's SOC analysts, on average, have been employed with bidder for a longer period than the employees of bidder's competitors.

The preferred proposal will include a comprehensive description of bidder's policies for conducting background, including credit checks, checks of its employees and subcontractors. The preferred proposal will also include a comprehensive description of how bidder provides initial and ongoing training to bidder's security-monitoring staff; proposals indicating that security-monitoring staff must complete initial training covering security and phishing—and that such training is supplied at least once every six months—will be preferred to proposals with a narrower scope of training or with a less frequent schedule of ongoing training. The preferred bidder will also explain how it maintains required knowledge and skills among its staff, with preference given to bidders that pay for staff training and/or third-party certifications.

The preferred bidder will assure UCS that the ratio of monitored security devices to bidder's SOC personnel is reasonable and is highly likely to ensure that UCS's security monitoring needs will be met. Also, the preferred bidder will offer at least four (4) customer support tiers and will ensure that Tier 4 issues will be handled by an engineer.

The preferred bidder will also have experience responding to large enterprise breaches. Experience responding to breaches involving large public-sector entities is preferred to experience responding

to breaches involving large private-sector entities, which in turn is preferred to experience responding to breaches involving smaller entities.

Organizational Capacity – References

As indicated in Section 6.2.5, below, bidders must supply contact information for at least three references. Preference will be given for favorable references from governmental entities comparable to UCS.

Business and Technical Specifications – Implementation and Service

The preferred bidder will include an executive summary of its offered services.

The proposal should explain how the bidder will complete an initial assessment and establish a baseline security level. While that work must be completed within one (1) year of the execution of the contract resulting from this RFP, preference will be given to proposals to complete that work within ninety (90) days of contract execution. The proposal should contain specifics on the implementation timeline, infrastructure requirements, encryption standards, and data transfer, data storage, data segregation, and backup systems.

When evaluating the bidder's methodology for detecting custom or targeted attacks directed at UCS systems or users, preference will be given to proposed solutions that include a built-in custom indicator of compromise (IOC).

When evaluating how the bidder will use external data, such as threat intelligence feeds, to analyze potential threats, preference will be given to solutions that not only feature automated threat intelligence feeds, but also provide automatic alerts on those feeds. Also, the preferred solution will integrate with UCS's Jira™ system.

In the preferred solution, the bidder will commit to regularly scheduled weekly meetings in the beginning phase of this project and then to less frequent regularly scheduled meetings.

Business and Technical Specifications – Service Management

The preferred proposal will describe in detail how problems will be escalated and resolved. It will also describe how UCS data will be stored and protected both at rest and in transit; the preferred solution will encrypt all data (AES 256 or better or SSL 1.3).

The preferred proposal will feature an auditable process for deleting all backups, logs, and keys as part of the SOC's sanitization process within 48 hours of contract termination or expiration.

The preferred proposal must create automated tickets and alerts through UCS's selected ticketing system (currently Jira). In reviewing customer notification and escalation processes, preference will be given to SOCs that have playbooks and runbooks in place and where the SOC will customize UCS notifications upon request. Ideally, proposals will include copies of bidder's runbooks and playbooks; if bidder considers such documents proprietary, bidder's proposal must explain why such documents should exempt from disclosure as specified in the paragraph entitled Public Information and Freedom of Information Law in Exhibit E of this RFP.

The preferred proposal will demonstrate that bidder will be available as needed and that bidder adopts a collaborative, responsive approach when security threats arise. The proposal should also explain how bidder will respond to complaints. UCS prefers solutions that accept complaints submitted via email and that have a defined process in place for resolving complaints.

Business and Technical Specifications – Security Event Monitoring

Proposals should describe bidder's capabilities to monitor various data sources, which include but are not limited to selected firewalls, intrusion detection/prevention system (IDPS), servers, applications, database logs, data loss prevention technology, web security and messaging security technology, user directories, identity and access management systems, end-point detection and response (EDR) tools, email security, proxy logs, and application logs. The preferred proposal will explain how the SOC will correlate such data, and it will confirm that the bidder is able to analyze such data to detect insider threats, mass deletion events, etc.

The preferred bidder will respond to feedback about false positives and work with UCS to fine-tune alerts when false positives and false negatives occur.

Business and Technical Specifications – Security Information Management

When evaluating whether the proposed solution is FedRAMP compliant, preference will be given to security controls that comply with High Impact Level Security Controls Baseline. The preferred SOC can collect upwards of 600GB/day of logs

The preferred proposal will describe the transit process for security event data from UCS endpoints to the SOC, including any intermediate systems located on premise to include guaranteed delivery and encryption, and preference will be given to proposals that ensure security event data from UCS endpoints is collected only during the alert stage.

The preferred SOC will assign a Level 4 Splunk engineer to create searches in UCS Splunk.

Business and Technical Specifications – Incident Response (IR)

When evaluating which IR activities are included as part of the proposed solution, preference will be given to proposals in which the bidder commits to supply a Level 3 IR employee (or subcontractor, which is slightly less ideal).

Business and Technical Specifications – Advanced Analytics and Capabilities

When evaluating how the proposed solution uses big data platforms to support the collection/analysis of network and endpoint data, the proposal should indicate whether the SOC will use UCS's solution or, if not, whether it will instead use bidder's own solution (and what that solution is).

When evaluating the technologies that are used to enable advanced analytics, preference will be given to proposals that clearly convey the advanced analytics tools that are part of the bidder's proposed SOC. Preference will be given to proposals featuring machine learning and/or artificial intelligence.

The ideal solution will offer: (i) specific network monitoring and/or network forensics features, capabilities, or offerings to detect advanced, targeted attacks across network monitoring/forensics; (ii) payload analysis; and (iii) endpoint behavior detection.

5.5 Invoicing

a. Awarded contractor shall submit true and accurate invoices to a point of contact to be designated by UCS in the contract resulting from this RFP.

b. Each invoice shall include:

- Vendor name
- Name of UCS department that ordered the goods or services;
- Description of goods or services requesting payment for (may be in narrative or code values format);
- Quantity of goods, property, or services delivered or rendered; and
- Amount requested

VI. BID RESPONSE DOCUMENTS

6.1 General Requirements

All documentation must be submitted on prescribed forms, without alteration. Where no form is included or specified, submissions must be single-spaced with one-inch page margins (not including attachments or financial forms) using a 12-point font. Pages should be numbered. To facilitate photocopying, do not permanently bind documents.

Bidders must submit every document listed in Sections 6.2 and 6.3, below. Failure to provide all documents in the manner required – including the number of requested copies - may result in disqualification of a bid response. Any changes, deletions, or additions (including the addition of supplemental terms and conditions) to this RFP or to any exhibits or appendices to this RFP, including Exhibit A – Pricing Sheet, may result in the rejection of the bid as non-responsive.

6.2 Required Proposal Documents

6.2.1 Exhibit A – Pricing Sheet

Exhibit A – Pricing Sheet must be completed in full, fully executed, and included in bidder's proposal. Failure to do so may disqualify bidder's response.

6.2.2 Responses to Exhibit D – Technical Components Proposal and Weighting

Bidders must submit with their bid response a narrative which demonstrates how the bidder and/or its proposed solution satisfies the desired attributes and needed features (collectively,

"Components") described in Article V and set forth in Exhibit D – Technical Components Proposal and Weighting. The narrative should include a description of the bidder's capability to produce and deliver similar services required hereunder on an as-needed basis.

The submitted narrative must address each and every Component set forth in Exhibit D. Each response must indicate which question(s) the response answers.

Components are grouped in the following categories:

Organizational Capacity – Capabilities
Organizational Capacity – Staffing
Organizational Capacity – References
Business and Technical Specifications – Implementation and Service
Business and Technical Specifications – Service Management
Business and Technical Specifications – Virtualization
Business and Technical Specifications – Security Event Monitoring
Business and Technical Specifications – Security Information Management
Business and Technical Specifications – Incident Response
Business and Technical Specifications – Vulnerability Management
Business and Technical Specifications – Advanced Analytics Capabilities
Business and Technical Specifications – Security Services Management
Business and Technical Specifications – Reporting Capabilities
Business and Technical Specifications – Project Management
Business and Technical Specifications – Compatibility with Information Security Policies

The narrative should not exceed 25 pages. References are not included in this page limit.

6.2.3 Bidder Contact Information

Bidder shall designate, where specified in the Document Enclosure Checklist, a person as primary contact for all questions UCS may have regarding bidder's bid response.

6.2.4 Firm Offer and Conflict of Interest Disclosure

Bidder shall submit a letter on bidder's letterhead confirming that any proposal submitted in response to this RFP is a binding offer to UCS and that such proposal meets or exceeds all terms, conditions, and requirements set forth in this RFP. Such letter shall conform to the template set forth in Exhibit B (Firm Offer to Unified Court System And Conflict of Interest Disclosure).

In addition to submitting the above-referenced letter, bidder shall include a resolution or equivalent authorization from bidder's Board of Directors, managing member, general partner, or equivalent governing office or body authorizing the officer or employee signing such letter to submit the bidder's proposal and confirming that such officer or employee possesses the requisite authority and legal capacity to act on behalf of the bidder and execute a contract with UCS.

6.2.5 References

Each bidder must submit three (3) references, other than UCS, for whom the bidder has provided similar services at any time during the past three (3) years. Such references must include the company/agency name, its complete address, a description of the services provided, the budget for the client's engagement, the start and end dates of the client's engagement, and the name, title,

telephone number and email address for a primary contact and an alternate contact. The bidder must supply such information using the template in Exhibit G.

6.3 NYS Bid Forms

6.3.1 Attachment I - Standard Request for Bid Clauses & Forms and Attachment IV- Procurement Lobbying Law required forms

In addition to such other specifications and criteria as are presented herein, the NYS Unified Court System Attachment I - Standard Request for Bid Clauses & Forms, and Attachment IV - Disclosure of Prior Non-Responsibility Determination (UCS 420) and Affirmation of Understanding and Agreement (UCS 421) pursuant to the Procurement Lobbying Act, which must be downloaded or printed from the UCS Contract & Procurement website under "Addenda" for the appropriate solicitation, are incorporated and made a part of this solicitation.

6.3.2 Attachment III - Vendor Responsibility Questionnaire

The UCS is required to conduct a review of a prospective vendor to provide reasonable assurances that the vendor is responsible. The required Vendor Responsibility Questionnaire is designed to provide information to assist UCS in assessing a vendor's responsibility prior to entering into a contract with the vendor. Vendor responsibility is determined by a review of each prospective Vendor's legal authority to do business in New York State, business integrity, financial and organizational resources, and performance history (including references).

The UCS recommends that vendors file the required Vendor Responsibility Questionnaire online via the New York State VendRep System. However, vendors may choose to complete a paper questionnaire and submit it with their proposal.

Online Questionnaire: To enroll in and use the New York State VendRep System, see the VendRep System Instructions available at http://www.osc.state.ny.us/state-vendors/vendrep/vendrep-system or go directly to the VendRep System online at https://onlineservices.osc.state.ny.us/Enrollment/login?1. Vendors must provide their New York State Vendor Identification Number when enrolling (see paragraph headed New York State Vendor File Registration' for instructions on obtaining a Vendor Identification Number.) For VendRep System assistance, contact the Office of the State Comptroller's Help Desk at 866-370-4672 or 518-408-4672 or by email at ITServiceDesk@osc.state.ny.us.

Bidders who file the Vendor Responsibility Questionnaire online via the OSC VendRep System are requested to checkmark the appropriate box on the Document Enclosure Checklist. Please note that online submissions must be certified and dated/updated not more than six (6) months prior to the bid opening date of this RFB/RFP. Bidders' authorized signature of the RFB/RFP form will serve as confirmation that bidders have knowingly filed their questionnaire online if the paper questionnaire is not included with the bidder's submission.

Paper Questionnaire: Vendors opting to complete and submit a paper questionnaire can obtain the appropriate questionnaire from the VendRep website www.osc.state.ny.us/vendrep/forms_vendor.htm or may contact the UCS or the Office of the State Comptroller's Help Desk for a copy of the paper form.

6.3.3 New York State Vendor File Registration

Prior to being awarded a contract pursuant to this solicitation, the bidder(s) must be registered in the New York State Vendor File (Vendor File) administered by the OSC. This is a central registry for all vendors who do business with New York State agencies and the registration must be initiated by a State agency. Following the initial registration, a unique New York State ten-digit vendor identification number (Vendor ID) will be assigned to vendors for usage on all future transactions with New York State. Additionally, the Vendor File enables vendors to use the Vendor Self-Service application to manage certain vendor information in one central location for all transactions related to the State of New York.

If the bidder is already registered in the Vendor File, the vendor must enter the vendor's ten-digit Vendor ID on the first page of this bid document.

If the bidder is not currently registered in the Vendor File, upon award of a contract the Bidder must complete the OSC Substitute W-9 Form (https://www.osc.state.ny.us/sites/default/files/vendors/2017-11/vendor-form-ac3237s-fe.pdf) and submit the form to UCS. **The UCS will initiate the vendor registration process** for the Vendor. Once the process is initiated, Vendor will receive an e-mail identifying their unique ten-digit Vendor ID and instructions on how to enroll in the online Vendor Self-Service application. For more information on the Vendor File please visit the following website: https://esupplier.sfs.ny.gov/psc/fscm/SUPPLIER/ERP/c/NUI_FRAMEWORK.PT_LANDINGPAGE.GBL?&.

6.3.4 Electronic Payments

Vendors not currently receiving electronic payments, and who wish to do so, should enroll in ePayment – New York State's electronic payment program for vendors. To do so, vendors need to log onto the Vendor Self-Service Portal and enter their bank account information. ePayments will ensure you are receiving payments faster and in a more secure manner. If you need assistance in accessing the Vendor Self-Service Portal, please contact the SFS Helpdesk at helpdesk@sfs.ny.gov or 1-877-737-4185.

6.3.5 Proof of Insurance

Bidder must provide together with its bid response all documentation required pursuant to the "Insurance Requirements" set forth in Exhibit E (Contract Terms and Requirements).

6.4 Additional Bid Documents

6.4.1 Financial Stability

Upon request by UCS, bidder shall provide its audited financial statements prepared in accordance with GAAP-Generally Accepted Accounting Principles for the past three (3) consecutive years and a copy of its last three (3) annual reports. Disclosures in such financial statements may affect determinations regarding bidder's responsibility.

VII. BID SUBMISSION PROCEDURES

7.1 Submission of Paper Bid Proposals by Mail

Bids/Proposals must be clearly addressed and submitted to:

NYS OCA Office of Grants and Contracts
2500 Pond View, Suite 104
Castleton-on-Hudson, NY 12033
ATTN: Kathleen Roberts

All envelopes/cartons must also be labeled with the following information on two sides:

"Deliver immediately to Kathleen Roberts"
"Sealed bid - Do not open"
RFB# OCA/DoTCR-131 due Thursday, July 6, 2023 at 3:00 PM Eastern

Failure to seal and mark the bid/proposal as prescribed may result in non-delivery and/or rejection of the bid/proposal. Please note that bids/proposals must be received by the above-named OCA-designated person by Thursday, July 6, 2023 at 3:00 PM (Eastern Daylight Time) at the latest or bids will be declared late bids and they will be disqualified. It is recommended that bidders allow several extra days for shipping in order to meet the deadline.

7.2 Submission of Electronic (email) Bid Proposals

As an alternative to the Bid Submission Procedures contained in Section 7.1, above, bidders may submit Bid proposals electronically to: **UCS-Bid-Submissions@nycourts.gov**. The email subject line must state: "**Bid Proposal – RFP # OCA/DoTCR-131**" and per subsection (b) below, indicate the email sequence number, as appropriate.

Bid proposals submitted electronically must meet all requirements set forth in the bid for proposals submitted by mail, including, but not limited to, delivery on or before the Bid Submission Deadline Date and completion of required acknowledgments.

Additionally, electronically submitted Bid proposals must conform to the following requirements:

(a) All Bid proposal documents must be in "PDF" searchable format.

(b) The size limitation for individual emails is 25MB (megabytes) per email (including message plus attachments). If documents cannot be grouped within one .zip file and/or one email so as to conform to the 25MB size requirement, bidders may transmit Bid proposals in multiple emails, in which case, each email must be labeled "Email X of X" (e.g., "Email 1 of 3").

(c) Notwithstanding the number of emails submitted, all Bid proposal emails must be submitted on the same date.

UCS will not accept Bid proposals submitted electronically that require UCS personnel to download files, including the Bid proposal, from a cloud storage service, such as Dropbox, Google Drive, Microsoft OneDrive, etc.

Bidders who submit a Bid proposal electronically will receive a reply email confirming the date and time of receipt of their submission. Bidders are advised to notify kmroberts@nycourts.gov if they have not received an email response within one (1) business day after submission of their Bid proposal.

7.3 Amendment of Proposals

Bidders may only amend submitted proposals prior to the proposal due date. Amended proposals must be submitted in packaging or email which clearly indicates "**Amended Proposal for RFP # OCA/DoTCR-131**." Amended proposals must be signed by an individual who is duly authorized to amend the bidder's original proposal. Amended proposals should be submitted in the same manner as original proposals described herein. Amended proposals received by UCS after the proposal due date and time may be rejected as "late."

7.4 Withdrawal of Proposal Prior to Proposal Opening

A proposal may be withdrawn at any time prior to the proposal due date and time. If multiple proposals are submitted by the same bidder, the bidder must clearly indicate the proposal to which the withdrawal applies.

7.5 Bidder Confidential/Proprietary Information

If applicable, bidders should specifically identify those portions of the proposal deemed to contain confidential or proprietary information or trade secrets, and must provide justification why such material, upon request, should not be disclosed to parties other than UCS. Bidders are advised that any material deemed confidential by bidder may still be subject to disclosure in connection with any governmental or judicial proceeding or inquiry or as may be required by applicable law, including but not limited to Article 6 of the New York Public Officers Law (Freedom of Information Law). Such confidential/proprietary information must be in a separate folder from the non-confidential sections of the proposal.

7.6 No-Bids

Bidders deciding not to answer this solicitation are requested to send a no-bid letter to OCA, Attn: Kathleen Roberts, Court Analyst, Office of Grants and Contracts, 2500 Pond View, Castleton-on-Hudson, NY 12033. The envelope shall be clearly marked in the lower left corner as follows: **RFP # OCA/DoTCR-131**. No-bid letters may be sent by email to kmroberts@nycourts.gov. Please indicate in "Subject" field: **RFP # OCA/DoTCR-131– No-Bid**.

7.7 Questions

Any and all questions bidders may have in connection with this solicitation are to be directed by email only to:

Kathleen Roberts, Court Analyst
kmroberts@nycourts.gov

Please indicate in "Subject" field: "**RFP # OCA/DoTCR-131 - Question(s)**."

The deadline to submit written questions is Friday, June 9, 2023 at 3:00 PM. A written response to all submitted questions in the form of a Questions & Answers (Q&A) sheet will be posted on the UCS website at www.nycourts.gov/admin/bids under **RFP # OCA/DoTCR-131**.

IMPORTANT: All questions regarding this solicitation must be in writing by email and directed solely to the attention of the above designated person. Contact by any prospective bidder, or any representative thereof, with any other personnel of the UCS in connection with this RFB/RFP may violate the Procurement Lobbying Act of 2005 (see Attachment IV), will jeopardize the respective bidder's standing, and may cause rejection of its proposal.

7.8 Pre-Bid Conference

A pre-bid conference will be held virtually on the Microsoft Teams platform on Friday, June 16, 2023 at 12:00 Noon. Bidders who attend the pre-bid conference may pose questions, and responses will be included in the official Q&A document. Bidders may also attend by conference call. While this conference is not mandatory, bidders are strongly encouraged to attend to benefit most directly and immediately from any issues or clarifications presented. Bidders must notify Kathleen Roberts at kmroberts@nycourts.gov in advance of their planned attendance. A link to the pre-bid conference will be sent to Bidders by email several days prior to the pre-bid conference.

VIII. BID TERMS AND CONDITIONS

Online RFB/RFP Package: Disclaimer

Bidders accessing any UCS/OCA solicitations and related documents from the New York State UCS website www.nycourts.gov/admin/bids under "Current Solicitations" shall remain solely and wholly responsible for reviewing the respective solicitation and bid documents on the internet regularly, up to the scheduled date and time of the bid/proposal due date, to ensure their knowledge of any amendments, addenda, modifications or other information affecting the solicitation or bid documents in question. UCS reserves the right, prior to bid opening, to amend the RFP specifications to correct errors or oversights or to supply additional information as it becomes available.

Binding Nature of Bid/Proposal on Bidders

All bids/proposals shall remain binding on bidders for a minimum of 270 days from the date of proposal submission or until a Contract is approved by the NYS Comptroller and executed by UCS, unless bidder requests a withdrawal of its bid/proposal in writing and such withdrawal is accepted by UCS/OCA in its sole discretion in accordance with applicable law.

Estimated Quantities

Any quantities specified in this solicitation constitute estimates only, and accordingly no commitment or guarantee to reach any specified volume of business is made or implied.

Awarded Contractor must accept all requests for services placed by UCS during the term of an awarded contract.

UCS's Reserved Rights to Reject Bids/Proposals, Set Aside Awards, and Withdraw the RFP

UCS reserves the right to reject any or all proposals or bids submitted in response to this solicitation. In addition, UCS may reject any bids/proposals from any bidder:

i. Who is in arrears to the State of New York upon any debt or performance of any contract;

ii. Who has previously defaulted on any contractual obligations (as contracting party, surety or otherwise) or on any obligation to the State of New York;

iii. Who has been declared not responsible or disqualified by any agency of the State of New York;

iv. Who has any proceeding pending against it relating to the responsibility or qualification of the bidder to receive public contracts;

v. Whose proposal is incomplete or otherwise non-responsive in any material respect;

vi. Who is found to be non-responsible based on any of the criteria specified in the section headed "Responsible Bidder";

vii. Whose facilities and/or resources are, in the opinion of OCA, inadequate or too remote from the UCS locations to render services in a timely manner in accordance with all requirements of this solicitation;

viii. Who does not provide references in accordance with the bid specifications, or whose references report significant failure to comply with specifications;

ix. Who is otherwise, in the opinion of OCA, unable to meet specifications; or

x. Whose conduct or proposal fails to conform to the requirements of the RFP.

UCS further reserves the right to set aside a bid award to a successful bidder if it is unsuccessful in negotiating a satisfactory contract within a time frame acceptable to the UCS, in which event UCS may then invite the bidder with the next highest evaluation score to enter into negotiations for purposes of executing a contract.

UCS reserves the right to withdraw the RFP at any time, in UCS's sole discretion.

Responsible Bidder

A bidder shall be defined as "responsible" in accordance with, but not limited to, references, past performance history, financial stability, the criteria set forth in paragraph 2 of the General Specifications (Attachment III-Vendor Responsibility Questionnaire), and the criteria set forth in the paragraph headed "Rejected and Unacceptable Bids/Proposals" as well as any other criteria necessary and reasonable to establish the bidder's responsibility.

Clarification/Correction and Evaluation of Bids/Proposals

In addition to any rights articulated elsewhere in this solicitation, UCS reserves the right to require clarification at any time during the procurement process and/or require correction of arithmetic or other apparent errors for the purpose of assuring a full and complete understanding of a bidder's proposal and/or to determine a bidder's compliance with the requirements of this solicitation. This clarifying information, if required in writing by UCS, must be submitted by the bidder, in accordance with formats as prescribed by UCS at the time said information is requested and, if received by the due date set forth in UCS's request for clarification, shall be included as a formal part of the bidder's proposal. Clarifying information, if any, whether provided orally, visually or in writing will be considered in the evaluation process. Failure to provide required information by its associated due date may result in rejection of the bidder's proposal. UCS may also use proposal information obtained through site visits, management interviews, and UCS's investigation of a bidder's qualifications, experience, ability, or financial standing in the course of evaluation or selection under the RFP. Nothing in the foregoing shall mean or imply that it is obligatory upon UCS to seek or allow clarifications or corrections as provided for herein.

Minor Bid Irregularities

Provided the same will not materially benefit or disadvantage any particular bidder or substantially alter the requirements of this bid, UCS may: (i) waive technicalities, (ii) waive minor irregularities, omissions or incompletions in the bid or a bid response, (iii) waive any bid requirements that are unmet by all bidders; (iv) consider any and/or all alternatives and/or enhancements suggested by the successful bidder; (v) make an award under the bid in whole or in part and negotiate contract terms and conditions with the successful bidder to meet UCS requirements consistent with such award.

Unified Court System Self-Insurance

UCS, a New York State governmental entity, is self-retained for risk of loss and liability.

Inspection of Bidder's/Awarded Contractor's Facilities

The UCS/OCA reserves the right to inspect bidder's proposed facilities, as part of the bid evaluation. Subsequent to award, Awarded Contractor's printing facilities shall be made available for periodic inspection. In all instances, advance notification will be communicated by appropriate court personnel.

Access to Court Facilities

Awarded Contractor must comply with all applicable location rules, policies, guidelines and procedures in order to be granted access to court facilities. Where applicable to the performance of work under an awarded contract, bidders shall be wholly responsible for familiarity with the physical layout and access to the courts and buildings in question, including but not limited to, roadways, overhangs, parking, security, elevators, required access permits or insurance certificates. No special accommodations can or will be made by court staff with respect to security measures, access or parking.

Subcontracting

Subcontracting and any other transfer of any duties or obligations to be performed hereunder will be permitted only with the prior written consent of UCS to the proposed subcontractors. In the event that bidder proposes to use one or more subcontractors, the specific subcontractors and the services proposed to be performed by such subcontractors, must be listed in bidder's proposal. If a bidder that proposes to use one or more subcontractors is awarded the contract, the award will constitute the prior written approval of UCS to the subcontractors named in the bidder's proposal.

The Awarded Contractor will be the prime contractor and will be responsible for all services required by this RFB/RFP. The UCS will communicate only with Awarded Contractor and the Awarded Contractor shall remain wholly liable for the performance by and payment to any such subcontractors, their employees, agents, consultants, or representatives. UCS may require subcontractors to provide evidence of insurance or submit to a background check, as applicable, prior to UCS approval.

Implied Requirements

Products and services that are not specifically requested in this solicitation, but which are necessary to provide the functional capabilities proposed by the bidder, shall be included in the offer except as specified herein.

Silence of the Specifications

The apparent silence of the specifications contained as part of this package as to any detail or to the apparent omission of a detailed description concerning any point, shall be regarded as meaning that only the best commercial practices are to prevail. All interpretations of these specifications shall be made on the basis of this statement.

IX. CONTRACT TERMS AND REQUIREMENTS

The RFP, the Bidder's proposal, and the contract that results from this RFP are subject to and incorporate the terms and conditions as stated in Appendix A – Standard Clauses for UCS Contracts (as set forth in Attachment I to this RFP), Exhibit E – Contract Terms and Requirements, and Exhibit F – SOC Terms and Conditions.

The successful bidder shall be required to comply with the provisions set forth in this Article, as well as such other provisions contained in an agreement, in form and content satisfactory to UCS its sole discretion.

EXHIBIT A: PRICING SHEET

Enter rates, costs, or other requested information in the fields highlighted in yellow. Do not otherwise alter this Pricing Sheet in any manner. Any changes, deletions, or additions to the Pricing Sheet (other than in fields highlighted in yellow) may result in rejection of the bid response.

Category	Annual Costs Year 1	Year 2	Year 3	Total Year 1 + Year 2 + Year 3
One-time onboarding costs				
Security operations center (SOC) services				
Total costs from all categories				
Combined Annual Cost				

In the space below, provide the name of the company submitting the proposal, the name and title of the authorized officer submitting the proposal, and that authorized officer's signature and the date of that signature.

Company Name:	
Authorized Officer's Name and Title:	
Signature:	Date:

EXHIBIT B: FIRM OFFER TO UNIFIED COURT SYSTEM AND CONFLICT OF INTEREST DISCLOSURE

TO BE COMPLETED ON OFFEROR'S LETTERHEAD

Date

Kathleen Roberts
Court Analyst
NYS OCA Office of Grants and Contracts
2500 Pond View, Suite 104
Castleton-on-Hudson, NY 12033

Dear Ms. Roberts:

Re: RFP # OCA/DoTCR-131

Firm Offer to the New York State Unified Court System and Conflict of Interest Disclosure

[INSERT OFFEROR NAME] hereby submits this firm and binding offer to the New York State Unified Court System in response to Request for Proposals (RFP) # OCA/DoTCR-131. The Bid Proposal hereby submitted meets or exceeds all terms, conditions, and requirements set forth in the above-referenced RFP. This formal offer will remain firm and non-revocable for a minimum period of 270 days from the date proposals are due to be received by UCS, or until a Contract is approved by the NYS Comptroller and executed by UCS.

[INSERT OFFEROR NAME]'s complete offer is set forth in three, separately bound assembled volumes or electronically via email.

[INSERT OFFEROR NAME] hereby affirms that the solution proposed by the Offeror in the Bid Proposal meets or exceeds the service level requirements set forth in the above-referenced RFP, including referenced attachments.

[INSERT OFFEROR NAME] hereby affirms that, at the time of bid submission, Offeror knows of no factors existing at time of bid submission or which are anticipated to arise during the procurement or Contract term, which would constitute a potential conflict of interest in successfully meeting the contractual obligations set forth in the above-referenced RFP and the Bid Proposal hereby submitted, including, but not limited to:

1. No potential for conflict of interest on the part of the Offeror or any Subcontractor due to prior, current, or proposed contracts, engagements, or affiliations; and

2. No potential conflicts in the sequence or timing of the proposed award under this procurement relative to the timeframe for service delivery, or personnel or financial resource commitments of Offeror or proposed subcontractors to other projects.

To comply with the Vendor Responsibility requirements outlined in Section 6.3.2 of the above-referenced RFP, Bidder hereby affirms (enter an "X" in the appropriate box):

☐ An online Vendor Responsibility Questionnaire has been updated or created within the last six (6) months at the website of the Office of the Comptroller: https://onlineservices.osc.state.ny.us/Enrollment/login?1

☐ A hard copy Vendor Responsibility Questionnaire is included with this proposal and is dated within the last six (6) months.

☐ A Vendor Responsibility Questionnaire is not required due to an exempt status. Exemptions include governmental agencies, public authorities, public colleges and universities, public benefit corporations, and Indian Nations.

By signing, the undersigned individual affirms and represents that he or she has the legal authority and capacity to sign and make this offer on behalf of, and has signed using that authority to legally bind [INSERT OFFEROR NAME] to the offer, and possesses the legal capacity to act on behalf of Offeror to execute a Contract with the New York State Unified Court System. The aforementioned legal authority and capacity of the undersigned individual is affirmed by the enclosed Resolution of the Corporate Board of Directors of [INSERT OFFEROR NAME].

_____

Signature
[INSERT OFFEROR NAME]
[INSERT TITLE]
[INSERT COMPANY NAME]

EXHIBIT C: CONTRACTOR CERTIFICATION OF MINIMUM BIDDER QUALIFICATIONS AND MANDATORY REQUIREMENTS

Use this form to address Minimum Bidder Qualifications and Mandatory Requirements (Pass/Fail)

BIDDER'S NAME: _____

Qualifications	
Qualification # 1: The Bidder has been in continuous operation providing managed security/ security operation center (SOC) services as one of its primary lines of business for at least the past three (3) years.	
The Bidder certifies that it has been in continuous operation providing managed security/SOC services as one of its primary lines of business for at least the past three years.	☐ **YES** ☐**NO***
Qualification # 2: The Bidder currently monitors a minimum of 2500 firewall / intrusion detection systems (IDS) / intrusion prevention systems (IPS) devices across its aggregate customer base.	
The Bidder certifies that it currently monitors a minimum of 2500 firewall / IDS / IPS devices across its aggregate customer base	☐ **YES** ☐**NO***
Qualification # 3: The Bidder currently monitors a minimum of 100 billion log lines per month across its aggregate customer base.	
The Bidder certifies that it currently monitors a minimum of 100 billion log lines per month across its aggregate customer base.	☐ **YES** ☐**NO***
Mandatory Requirements	
Mandatory Requirement # 1: The proposed solution must comply with Systems and Organization Controls 2 (SOC 2®) requirements as developed by the American Institute of Certified Public Accountants.	
The Bidder certifies that the proposed solution complies with SOC 2® requirements as developed by the AICPA.	☐ **YES** ☐**NO***
Mandatory Requirement # 2: All UCS data must remain in the continental United States, and select data must remain on UCS premises as outlined in the RFP.	
The Bidder certifies that all UCS data will remain in the continental United States, and select data will remain on UCS premises as outlined in the RFP.	☐ **YES** ☐**NO***
Mandatory Requirement # 3: The proposed solution must comply with Federal Risk and Authorization Management Program (FedRAMP®) Moderate or High Impact Level Security Controls Baseline Requirements.	
The Bidder certifies that the proposed solution complies with FedRAMP® Moderate or High Impact Level Security Controls Baseline Requirements.	☐ **YES** ☐**NO***
Mandatory Requirement # 4: The proposed solution must be operational 24 hours/day × 365 days/year with staffing at or exceeding the levels set forth in Section 5.3 of the RFP.	
The Bidder certifies that the proposed solution will be operational 24 hours/day × 365 days/year with staffing at or exceeding the levels set forth in Section 5.3 of the RFP.	☐ **YES** ☐**NO***
Mandatory Requirement # 5: The proposed solution must integrate with the existing UCS Splunk Security Information and Event Management (SIEM) system (600 GB/day license) and scale up without installation of proprietary vendor hardware.	
The Bidder certifies that the proposed solution will integrate with the existing UCS Splunk SIEM system and scale up without installation of proprietary vendor hardware.	☐ **YES** ☐**NO***

EXHIBIT C: CONTRACTOR CERTIFICATION OF MINIMUM BIDDER QUALIFICATIONS AND MANDATORY REQUIREMENTS

Mandatory Requirement # 6: The proposed solution must include access to SOC Level 1, Level 2, and Level 3 analysts as needed for incident response purposes.	
The Bidder certifies that the proposed solution will include access to SOC Level 1, Level 2, and Level 3 analysts as needed for incident response purposes.	☐ **YES** ☐**NO***
Mandatory Requirement # 7: The proposed solution must operate within and integrate with UCS Software and Environment, including its ticketing system, as defined in Section 5.1 (Current State).	
The Bidder certifies that the proposed solution will operate within and integrate with UCS Software and Environment, including its ticketing system, as defined in Section 5.1 (Current State).	☐ **YES** ☐**NO***
Mandatory Requirement # 8: The proposed solution must supply a full-time Splunk engineer (staff member or subcontractor) to create custom searches and upgrades as needed for the UCS Splunk environment.	
The Bidder certifies that the proposed solution will supply a full-time Splunk engineer (staff member or subcontractor) to create custom searches and upgrades as needed for the UCS Splunk environment.	☐ **YES** ☐**NO***
Mandatory Requirement # 9: The proposed solution does not require UCS to install any applications, programs, or other software on systems owned or maintained by UCS.	
The Bidder certifies that the proposed solution will not require UCS to install any applications, programs, or other software on systems owned or maintained by UCS.	☐ **YES** ☐**NO***
Mandatory Requirement # 10: The proposed solution is compatible with NYS Office of Information Technology Service Security Policy No. NYS-P03-002 (as set forth in Exhibit H), and it must be NIST Tier 4 compliant.	
The Bidder certifies that the proposed solution is: (i) compatible with NYS Office of Information Technology Services Security Policy No. NYS-P03-002 (as set forth in Exhibit H); and (ii) NIST Tier 4 compliant.	☐ **YES** ☐**NO***

*** A "NO" response to any of the minimum qualifications or mandatory requirements will result in Bidder disqualification.**

EXHIBIT C: CONTRACTOR CERTIFICATION OF MINIMUM BIDDER QUALIFICATIONS AND MANDATORY REQUIREMENTS

CERTIFICATION

By signing this form, you certify your express authority to sign on behalf of the Bidder and that all information provided is complete, true, and accurate.

Date: _____

Legal Business Name of Bidder: _____

Doing Business As (d/b/a) (if appropriate): _____

Signature: _____

Print Name: _____

EXHIBIT D – TECHNICAL PROPOSAL COMPONENTS AND WEIGHTING

As indicated in Article VI, bidders must submit a narrative response addressing how the bidder and/or its proposed solution satisfies the desired attribute or needed feature ("Component") set forth below.

Each response must indicate the Component number to which it responds.

Each response will be assigned a score 0, 1, 2 or 3 according to the following rubric:

Points	Criteria
3	The response thoroughly describes how the solution: (i) will deliver the Component; (ii) is feasible; and (iii) is highly likely to result in the successful implementation of the solution.
2	The response adequately describes how the solution: (i) will deliver the Component; (ii) is feasible; and (iii) is likely to result in the successful implementation of the solution.
1	The response minimally or inadequately describes how the solution will deliver the Component and is unlikely to result in the successful implementation of the solution.
0	The solution either is not feasible or does not describe how the solution will deliver the Component.

In addition, each Component is assigned a weighting factor of 1, 2, 3 or 4 indicated by a corresponding number of stars. Evaluators will multiply the assigned score by the weighting factor to determine how many overall points each response receives. For example, a response that receives three (3) points for a component with a weighting factor of ★★★★ will be assigned twelve (12) overall points. The sum of assigned overall points will constitute the bidder's technical proposal score.

Components are grouped according to the following categories:

If the Component # begins with the letter…	…then the desired attribute or needed feature pertains to
A	Organizational Capacity – Capabilities
B	Organizational Capacity – Staffing
C	Organizational Capacity – References
D	Business and Technical Specifications – Implementation and Service
E	Business and Technical Specifications – Service Management
F	Business and Technical Specifications – Virtualization
G	Business and Technical Specifications – Security Event Monitoring
H	Business and Technical Specifications – Security Information Management
I	Business and Technical Specifications – Incident Response
J	Business and Technical Specifications – Vulnerability Management
K	Business and Technical Specifications – Advanced Analytics Capabilities
L	Business and Technical Specifications – Security Services Management
M	Business and Technical Specifications – Reporting Capabilities
N	Business and Technical Specifications – Project Management
O	Business and Technical Specifications – Compatibility with Information Security Policies

Note: Components appearing in **bold text** pertain to a mandatory qualification or minimum requirement set forth in Article II of the RFP.

Component #	Desired Attribute or Needed Feature (Component)	Weighting Factor
A1	**Bidder has been in continuous operation providing managed security/ security operation center (SOC) services as one of its primary lines of business for at least the past three (3) years.**	★★
A2	**Bidder currently monitors a minimum of 2500 firewall / intrusion detection systems (IDS) / intrusion prevention systems (IPS) devices across its aggregate customer base.**	★★
A3	**Bidder currently monitors a minimum of 100 billion log lines per month across its aggregate customer base.**	★★
A4	**Bidder is compliant with Systems and Organization Controls 2 (SOC 2®) requirements as developed by the American Institute of Certified Public Accountants.**	★★
A5	Bidder's headquarters are in the United States, and the bidder's SOCs that would serve UCS are in the continental United States.	★★
A6	Bidder's documented policies, procedures, and audit requirements will ensure the privacy and confidentiality of UCS data. They will also ensure UCS data is maintained separately from the data of bidder's other customers.	★★
A7	Bidder will guarantee at least 99.982% uptime to ensure continuity of service for UCS.	★★
A8	Bidder's alliances with other companies, such as those providing third-party software as part of bidder's SOC portfolio, will enable bidder to deliver the SOC services needed under this RFP. If bidder has no such alliances, confirm that bidder does not rely on third parties to deliver the proposed solution.	★★
A9	Bidder has experience providing cybersecurity services to public or private entities comparable to UCS.	★★★
B1	**Bidder will ensure that all personnel or subcontractors who will have access to the SOC solution and/or UCS data complete a background check acceptable to UCS prior to commencing work under the resulting contract.**	★★★
B2	**Bidder will ensure that at least three (3) qualified security analysts are available to support UCS to respond to identified incidents during daytime (7:00 AM – 5:00 PM Eastern Time) and evening (5:00 PM – Midnight Eastern Time) shifts and that at least two (2) qualified security analysts are available to support UCS to respond to identified incidents during overnight (Midnight – 7:00 AM Eastern Time) shifts.**	★★★★
B3	**Bidder will ensure that employees or subcontractors assigned to the UCS account will be located physically in the continental United States when delivering SOC services.**	★
B4	**Bidder will ensure that UCS has access to SOC Level 1, Level 2, and Level 3 analysts as needed for incident response purposes.**	★★★★
B5	Bidder will provide an incident response team whose members have an average of five (5) years' experience.	★
B6	Bidder's incident response team will include at least fifteen (15) employees or subcontracted personnel.	★
B7	Bidder's personnel will be deployed in different time zones within the United States to enhance coverage for UCS.	★
B8	Bidder is an industry leader in screening and hiring SOC staff, and bidder performs background checks, including credit checks, for all employees (including but not limited to those assigned to the UCS account).	★
B9	Bidder is an industry leader in providing initial and ongoing training for its security-monitoring staff. Discuss the topics covered in initial training (including, ideally, security and phishing) and how frequently staff must complete ongoing training on those topics.	★
B10	Bidder maintains required knowledge and skills among its staff.	★★
B11	Bidder's personnel will review automated detections that require isolation or resetting of account credentials. Automated responses alone are not sufficient.	★★★★
B12	Bidder is an industry leader in ensuring that the ratio of monitored security devices to personnel is at or below that of its competitors.	★★
B13	Bidder has a comprehensive, tiered strategy for providing customer support, including ensuring that an engineer is available and assigned to cases assigned to the highest tier.	★★
B14	Bidder's SOC holds one or more industry certifications, such as Statement on Standards for Attestation Engagements (SSAE) 16 Type 2 or International Organization for Standardization (ISO) 27001, and bidder's proposal includes supporting documentation confirming such certification(s).	★★
B15	Bidder has a comprehensive plan to deploy its incident response expertise for threat detection.	★★
B16	Bidder has extensive experience responding to large enterprise breaches, including breaches of large public-sector clients.	★★

Component #	Desired Attribute or Needed Feature (Component)	Weighting Factor
B17	Bidder proposes a comprehensive solution for responding to targeted threat actors and, if bidder has experience responding to targeted threat actors, bidder describes how it responded to at least one such targeted threat actor in the past.	★★
C1	Consistent with Section 6.2.5 on page 17 of the RFP, Bidder's proposal includes at least three (3) references from entities other than UCS for which Bidder provided SOC services at any time during the past three (3) years. Preference will be given for favorable references from governmental entities comparable to UCS.	★★★★
D1	**The proposal will provide 24×7×365 remote security event monitoring and device/agent management.**	★★
D2	The proposal includes an executive summary of the proposed SOC solution.	★★
D3	Bidder will complete an initial assessment and establish a baseline security level. Include specifics on the implementation timeline (including when such initial assessment will be completed and when such baseline security level will be established; infrastructure requirements; data transfer, data storage and segregation, and backup systems; and encryption standards.	★★
D4	Bidder has a sound methodology for detecting custom or targeted attacks directed at UCS users or systems.	★★
D5	The proposal describes the architecture of Bidder's SOC delivery capability, including elements of its SOC, data center, and network, as well as the centrally delivered log management, analytics, and portal tiers. It also describes capabilities for collecting event logs and data from other locations, such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The proposal includes example architectural diagrams and descriptions, which identify any elements delivered by third-party vendors. The SOC does not rely on colocation of data.	★★
D6	The SOC will interface with products UCS has in place for enterprise monitoring and incident response.	★★
D7	UCS can disengage from the SOC with minimal disruption if funding is not available and/or UCS does not renew the contract.	★★
D8	The SOC uses external data (e.g., threat intelligence feeds) to analyze potential feeds, and the proposal describes how much access UCS will have to that information.	★★
D9	The solution can integrate with enterprise directories and configuration management databases (CMDBs), and the proposal explains how those integrations support delivery of the proposed services.	★★
D10	The proposal includes opportunities for continuous improvement during the implementation phase, and it proposes regularly scheduled meetings that occur less frequently after the implementation phase.	★★
D11	The proposal describes Bidder's test methodology for alerts.	★★★★
D12	The proposal describes how Bidder's SOC detected and responded to a recent security incident.	★★
D13	The proposal itemizes the primary tools Bidder's SOC uses to deliver the proposed solution. It also lists any third-party tools that will be used.	★★
D14	The proposal describes how SOC services will scale to meet UCS needs, and it identifies any related variable costs.	★★
E1	The proposal describes Bidder's problem resolution and escalation procedure.	★★
E2	The proposal offers a process for adding services or new technologies if requested by OCS (e.g., if UCS adopts a deep packet inspection firewall technology, the proposal explains how this would be supported and incorporated into a service level agreement [SLA]).	★★
E3	The proposal includes a change control process to modify the original scope of the supplied technology for a new feature. The proposal also describes how the costs will be determined.	★★
E4	The solution's data sanitization process will ensure a timely and complete removal of data and data remnants for meta data.	★★
E5	The solution will store and protect UCS data, including data generated by Bidder about security events and incidents) both at rest and in transit.	★★
E6	The solution meets federal regulatory or statutory requirements concerning handling of data, including, but not limited to, criminal justice information (including sealed data), information protected pursuant to the Health Insurance Portability and Accountability Act (HIPAA), tax information, and Personally Identifiable Information (PII).	★★
E7	The proposal describes the expected working relationship, roles, and responsibilities between Bidder's security staff and selected UCS security staff.	★★

Component #	Desired Attribute or Needed Feature (Component)	Weighting Factor
E8	The proposal describes device/agent management and real-time event management notification service levels, and it explains how they are measured and how they will be communicated to UCS.	★★
E9	The proposal describes Bidder's SLA performance reporting.	★★
E10	The solution's documentation process is explained. The proposal explains how access will be granted for various stakeholders (auditors, customers, or business partners requiring this documentation in support of legal, regulatory, or contractual requirements), It also describes: (a) how access to documents for different groups will be managed; (b) the process for requesting documentation; and (c) the time frames in which requested documents will be produced.	★★
E11	Bidder will have a process for dealing with complaints from UCS, and the proposal explains that process.	★★
F1	The proposal explains whether the solution can operate in a virtualized environment. If the solution cannot operate in a virtualized environment, the proposal explains why not. The proposal identifies and describes all differences, restrictions, or limitations of bidder's proposed solution with respect to operation, licensing, support, certification, warranties, and any other details that may impact the proposed solution when hosted in a virtualized environment.	★★
G1	The SOC will monitor various data sources, which include, but are not limited to, selected firewalls, intrusion detection/prevention system (IDPS), servers, applications, database logs, data loss prevention technology, web security and messaging security technology, user directories, identity and access management systems, end-point detection and response (EDR) tools, email security, proxy logs, and application logs.	★★★★
G2	The SOC will monitor the data described in Component # G1 and provide real-time event correlation between data sources as well as real-time alerting of security incidents and system health incidents.	★★★★
G3	The SOC will monitor the data described in Component # G1 to identify when changes in behaviors of users or systems represent a risk to the UCS environment.	★★
G4	The SOC will use signature-based and/or behavior-based detection as well as correlation rules. The proposal describes how the SOC will use artificial intelligence and/or machine learning for this purpose.	★★
G5	The proposal describes the extent to which the proposed solution will monitor, detect, respond, and remediate threats in conformity with standards, guidelines, and best practices of the National Institute of Standards and Technology ("NIST").	★★
G6	The proposal includes support for creating and managing customized correlation rules.	★★
G7	The SOC will effectively manage false positives and false negatives, and the proposal describes how Bidder will adapt in response to feedback from UCS regarding false positives.	★★
G8	The proposal describes the typical workflow and process that occurs when the security analytics detects a security event, beginning with how that is presented to a SOC analyst for evaluation through the triage, validation, prioritization, and customer alerting/notification process. The proposal indicates and distinguishes which activities are automated versus manually performed by analysts.	★★★★
G9	Bidder's SOC staff will interact with and support UCS staff to assess, investigate, and respond to incidents. Additionally, Bidder's analysts will report confirmation of an event within the timeframes set forth in Table One (Event Security Level Notification and Response Requirements) on page 50 of the RFP.	★★
G10	The proposal describes any limitations to security event monitoring, such as data sources, age, and query frequency.	★★
G11	The solution can attach pictures and/or video files to specific transactions, and the proposal explains any limitations on this feature.	★★
G12	The solution can utilize workflows to route reports to a user's email automatically.	★★
G13	The proposal recounts how the Bidder supported a customer during a ransomware attack, and the proposal describes the steps Bidder took to respond and recover that customer during a ransomware incident.	★★
H1	**Bidder's security controls are FedRAMP compliant, and the proposal describes whether they comply with Moderate Impact Level Security Controls Baseline requirements or High Impact Level Security Controls Baseline requirements.**	★★★★
H2	**The Bidder will ensure that all UCS data to which the Bidder has access will remain in systems physically located in the continental United States.**	★★

Component #	Desired Attribute or Needed Feature (Component)	Weighting Factor
H3	**Delivery of SOC services does not require UCS to install any applications, programs, or other software on systems owned or maintained by UCS.**	★★★★
H4	The solution complies with the security guidelines outlined in the National Institute of Standards and Technology (NIST) Special Publications in the 800 series.	★★
H5	The proposal clearly describes the transit process for security event data from UCS endpoints to the SOC, including any intermediate systems located on premise to include guaranteed delivery and encryption, collects only the information necessary.	★★
H6	The proposal clearly identifies any limitations to bidder's log collection capabilities, such as peak event rates, volume, or sources, and such limitations are not likely to impede the successful monitoring of UCS data.	★★
H7	Bidder offers to supply Splunk admin/engineers to create customized Splunk searches/dashboard and to correlate log data. The proposal explains whether such personnel are employees or subcontractors, and it describes any limitations to this capability.	★★★★
H8	Bidder's staff can create and modify reports based on collected log data, and the proposal indicates any limitations, such as number of reports, complexity of queries, and age of data.	★★
H9	Bidder's standard data retention policies are described, and the proposal describes under what conditions bidder will modify them to meet UCS requirements.	★
H10	**The proposal describes how the solution will integrate with UCS's ticketing system (currently Jira).**	★
I1	The proposal identifies any remote incident response (IR) services, including breach response services, as part of the proposed solution. The proposal distinguishes which remote IR services are included as core services and which are available as an additional service/offering. The proposal also indicates whether IR staff are bidder's employees or subcontractors.	★★★★
I2	The proposal indicates whether Bidder's security portal provides external threat intelligence feeds and, if so, which sources are included in the proposed solution. The proposal also indicates whether Bidder will assist with creating specific IR use cases and maintain a run book; if Bidder proposes such activities, the proposal identifies how such activity will be achieved.	★★★★
I3	The proposal describes which methodology is used by IR analysts for threat detection, threat hunting, and attribution (for example, MITRE ATT&CK®, etc.).	★★★★
I4	The proposal identifies which self-service features for IR are provided via the portal (e.g., automated malware analysis, custom signature, or correlation rule implementation).	★★★★
J1	The proposed solution monitors vulnerability scans internally and externally within UCS.	★★
J2	The proposal describes Bidder's methodology for collecting and analyzing vulnerability and asset data (e.g., configuration) from all sources in scope.	★★
J3	The proposal describes how vulnerabilities are triaged and prioritized prior to reporting, including the integration of previous scan results and actions carried out.	★★
K1	The SOC uses big data platforms to support the collection/analysis of network and endpoint data. The proposal indicates whether the SOC will rely on UCS's network data collection/analysis solution or whether the SOC will rely on Bidder's solution; if it relies on Bidder's solution, the proposal describes that solution.	★★
K2	The proposal describes which technologies are used to enable advanced analytics.	★★
K3	The solution will profile and monitor entity and user activities and behaviors (e.g., user and entity behavior analytics [UBEA]), and the proposal describes the specific approaches and models/algorithms the SOC will use.	★★
K4	The solution will use predictive analytics, and the proposal describes the specific approaches and models/algorithms to be used.	★★
K5	The proposal describes specific network monitoring and/or network forensics features, capabilities, or offerings to detect advanced, targeted attacks across network monitoring/forensics, payload analysis, and endpoint behaviors.	★★
K6	The SOC supports streamed data with real-time advanced analytics, and the proposal describes any technologies supported (e.g., Apache Kafka® or Apache NiFi).	★★
K7	The proposal describes the offered data and threat visualization capabilities offered via Splunk.	★★
K8	The SOC will leverage big data platforms to collect, retain, and analyze large volumes of operational and security data, and it will use security solutions already operationalized by UCS.	★★
L1	Bidder's processes for updating software, including signature updates and system patches, are unlikely to disrupt UCS operations.	★★★★

Component #	Desired Attribute or Needed Feature (Component)	Weighting Factor
M1	The proposal describes how Bidder will report alerts to UCS.	★★★★
M2	The proposal includes an escalation chart describing methods of communication at various levels of severity, and the proposed protocol will ensure UCS receives prompt, accurate notifications at each level of severity.	★★★★
M3	The proposal describes Bidder's operational, regulatory, and executive reporting capabilities, and it includes an example of executive-level reports that can be produced within the security portal or provided via other methods.	★★★★
M4	The solution will enable UCS staff to create customized, ad hoc queries and reports. The proposal discloses any limitations to generating ad hoc queries or reports, such as data sources, data age, and query frequency.	★★★★
M5	The proposal describes which convention(s), such as STIX, TAXII, or OpenIOC, Bidder's SOC will use to report threat information to UCS.	★★★★
N1	The proposal includes an initial schedule and associated Work Breakdown Structure (WBS). Such documents identify significant phases, activities, tasks, milestones, deliverables, and resources requirements necessary for UCS to evaluate Bidder's implementation plan.	★★★★
O1	**Bidder's proposal is: (i) compatible with NYS Office of Information Technology Services Security Policy No. NYS-P03-002 (as set forth in Exhibit H); and (ii) NIST Tier 4 compliant.**	★★

EXHIBIT E: CONTRACT TERMS AND REQUIREMENTS

As discussed in Article IX of the RFP, the terms and conditions set forth below, along with those set forth in Appendix A – Standard Clauses for UCS Contracts (see Attachment I), and Exhibit F – SOC Terms and Conditions are binding on and incorporated in the RFP, the Bidder's proposal, and the contract that results from the RFP.

Background Checks / Onboarding

All Contractor Staff, prior to the commencement of any services, including off-site services, shall comply with all UCS onboarding and security clearance requirements, including any necessary training, for access to UCS Data or UCS Facilities. Contractor agrees that its workers performing services under this contract or who will have access to UCS Data shall be required to undergo at least the same security clearances as those required of UCS Employees. Unless otherwise approved by UCS in its sole discretion, each prospective or current worker of Contractor designated to work on this Contract with UCS shall submit identifying information to UCS and be fingerprinted. UCS will arrange for the scheduling of fingerprinting. Such fingerprints shall be submitted to the NYS Division of Criminal Justice Services for state criminal history check and, where authorized, the Federal Bureau of Investigation ("FBI") for national criminal history check. All expenses, including travel and lodging, associated with the onboarding and security clearance process including fingerprinting of Contractor staff are the responsibility of the Contractor and are not reimbursable.

UCS shall make all suitability determinations on Contractor Staff. For purposes hereof, a "suitability determination" is a determination that there are reasonable grounds to believe that an individual will likely be able to perform the Contract requirements without undue risk to the interests of UCS. Failure of a security clearance or non-compliance with this provision will disqualify any Contractor staff from performing any Services on the Contract. If any Contractor staff are removed from providing Services under the resulting Contract, they may be subject to all onboarding and security clearance requirements if they are returned to performing Services under the Contract.

Compliance with Laws

Contractor must comply with all applicable federal, state, and local laws, rules and regulations, including but not limited to, fire, health and safety codes, prior to and during the provision of all services under the contract resulting from this RFB/RFP ("Contract").

Confidentiality and Data Security

Contractor acknowledges that any and all information, records, files, documents, or reports contained in any media format provided to the Contractor by UCS, including information about UCS systems, or which may be otherwise encountered by Contractor shall be considered extremely confidential and shall be handled accordingly at all times (hereinafter "UCS Confidential Information"). Secondary disclosure of the UCS Confidential Information may only be made to Contractor's employees, officers, directors, auditors, representatives, or other third-party contractors who have a reasonable need to know such UCS Confidential Information for purposes of carrying out Contractor's obligations under its agreement with UCS. Neither the Contractor nor any of its employees, servants, vendors, agents, or volunteers shall at any time be permitted to utilize UCS Confidential Information for any purpose outside the scope of any resulting agreement without the express prior written authorization of UCS. Any breach of this confidentiality by the Contractor or by any of its employees, servants, subcontractors, agents, or volunteers may result in the immediate termination of any resulting agreement by UCS and may subject the Contractor to further penalties.

Contractor shall use, and require its employees and authorized agents to use, at least the same degree of care to secure and protect UCS Confidential Information that it exercises to secure and protect its own similar confidential information.

Contractor is prohibited from maintaining UCS Confidential Information provided to or generated by Contractor in a mobile or portable device. Remote access to the UCS confidential information is prohibited unless such access complies with New York State Information Technology Standard No. NYS-S14-010 as issued by the New York State Office of Information Technology Services[1] or other similar protocols as approved by UCS in its sole discretion, including two-factor user authentication, are in place (e.g., SSL, VPN). In addition, Contractor will be required to comply with the data security and confidentiality requirements of other government agencies that supply data to UCS as well as notice of any actual or potential security breach involving the UCS Confidential Information to UCS within 24 hours and also as required by the New York State Information Security Breach and Notification Act.

Data Ownership, Migration, Accessibility, Location, Storage, Transport, Protection, and Destruction

Data Ownership: All UCS data is owned exclusively by UCS and will remain the property of UCS. Contractor is permitted to use data solely for the purposes set forth in the RFP and the Contract, and for no other purpose. At no time shall Contractor access, use, or disclose any confidential information (including personal, financial, health, or criminal history record information or other sensitive criminal justice information) for any other purpose. The Contractor is strictly prohibited from releasing or using data or information for any purposes other than those purposes specifically authorized by UCS. Contractor agrees that UCS data shall not be distributed, used, repurposed, transmitted, exchanged, or shared across other applications, environments, or business units of the Contractor or otherwise passed to other contractors, agents, subcontractors, or any other interested parties, except as expressly and specifically agreed to in writing by UCS.

Migration: Contractor's services performed under the Contract will ensure easy migration of UCS's data, including UCS's Confidential Information under the Contract by providing its solution in a manner designed to do so. This may include Contractor keeping UCS data separate from processes of the software itself and maintaining that information in a format that allows UCS to easily transfer it to an alternative application platform. Contractor will make its Application Programming Interfaces (APIs) available to UCS.

Data Storage, Access and Location: Contractor must ensure that all UCS data related to this Contract is stored within the continental United States (CONUS), in a controlled access environment to ensure data security and integrity. All access to UCS data, physical or virtual, must be conducted within CONUS and have adequate security systems in place to protect against the unauthorized access to the facilities and data stored therein. Contractor shall not send or permit to be sent to any location outside of the CONUS, any UCS data related to the Contract. Contractor will provide UCS with a list of the physical locations where UCS data is stored at any given time and will update that list if the physical location changes. Access into and within the facilities must be restricted through an access control system that requires positive identification as well as maintains a log of all accesses (e.g., date and time of the event, type of event, user identity, component of the information system, outcome of the event). Contractor shall have a formal procedure in place for granting computer system access to the data and to track access. Access for projects outside of those approved by UCS are prohibited.

Data Protection and Transmission: Contractor shall use appropriate means to preserve and protect UCS data. This includes, but is not limited to, use of stable storage media, regular data backups and archiving, password protection of volumes, and data encryption. All UCS data in transit and at rest will be encrypted. At a minimum, cryptographic modules used for data transmission between UCS and Contractor must be validated to FIPS 140-2 or 140-3 for the protection of sensitive information (http://csrc.nist.gov/groups/STM/cmvp/index.html).

Data Return and Destruction: At the expiration or termination of the Contract, at UCS's option, Contractor must provide UCS with a copy of UCS data, including metadata and attachments, in a mutually agreed upon, commercially standard format and give UCS continued access to UCS data for no less than ninety (90) days beyond the expiration or termination of the Contract. Thereafter, except for data required to maintained by

1 Available for download: https://tinyurl.com/4xjj3wj2

law or the Contract, Contractor shall destroy UCS data from its systems and wipe all its data storage devices to eliminate any and all UCS data from Contractor's systems. The sanitization process must be in compliance with New York State Security Policy NYS-S13-003 (https://www.its.ny.gov/document/sanitizationsecure-disposal-standard), and, where required, sanitization and disposal standards published by the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS). If immediate purging of all data storage components is not possible, Contractor will certify that any data remaining in any storage component will be safeguarded to prevent unauthorized disclosures. Contractor must then certify to UCS, in writing, that it has complied with the provisions of this paragraph. UCS may withhold payment to Contractor if UCS data is not released to UCS in accordance with the preceding sections.

If the requirements set forth in the RFP and/or Contract are not the same as the policies of the NYS Office of Information Technology Services (ITS), then the more restrictive requirement applies.

Contractor shall be strictly prohibited from using UCS data in any fashion other than that defined herein or authorized in writing by UCS.

Contractor must, in accordance with applicable law and the instructions of UCS, maintain such data for the time period required by applicable law, exercise due care for the protection of data, and maintain appropriate data integrity safeguards against the deletion or alteration of such data. In the event that any data is lost or destroyed because of any act or omission of Contractor or any non-compliance with the obligations of the Contract, then Contractor shall, at its own expense, use its best efforts in accordance with industry standards to reconstruct such data as soon as feasible. In such event, Contractor shall reimburse UCS for any costs incurred by UCS in correcting, recreating, restoring, or reprocessing such data or in providing assistance therewith.

Contractor agrees that any and all UCS data will be stored, processed, and maintained solely on designated target devices, and that no UCS data at any time will be processed on or transferred to any portable computing device or any portable storage medium, unless that device or storage medium is a necessary and approved component of the authorized business processes covered in the Contract or any addendum thereof, or Contractor's designated backup and recovery processes, and is encrypted in accordance with all current Federal and State statutes, regulations, and requirements.

Default

If either party breaches a material provision of this Contract, which breach remains uncured for a period of thirty (30) days after written notice thereof from the other party specifying the breach (or if such breach cannot be completely cured within the thirty day period, such longer period of time provided that the breaching party proceeds with reasonable diligence to completely cure the breach) or if Contractor shall cease conducting business in the normal course, become insolvent, make a general assignment for the benefit of creditors, suffer or permit the appointment of a receiver for its business or assets or shall avail itself of or become subject to any proceeding under the Federal Bankruptcy Act or any statute of any other state relating to insolvency or the protection of rights of creditors then and in any such event, the other party may, at its option, terminate this Contract upon ten (10) days' written notice and exercise such other remedies as shall be available under this Contract, at law or in equity.

No failure by UCS to insist upon the strict performance of any covenant, term, or condition of this Agreement, or to exercise any right or remedy consequent upon a breach thereof, and no acceptance of full or partial performance during the continuance of any such breach, shall constitute a waiver of any such breach or such covenant, term, or condition. No covenant, term, or condition of this Agreement to be performed or complied with by Contractor, and no breach thereof, shall be waived, altered, or modified except by a written instrument executed by UCS. No waiver of any breach shall affect or alter this Agreement but each and every covenant, term, and condition of this Agreement shall continue in full force and effect with respect to any other then existing or subsequent breach thereof.

Indemnity

Contractor shall indemnify, defend and hold harmless UCS, its officers and employees from and against any and all claims, causes of action, damages, costs, liabilities and expenses of any kind (including reasonable attorney's fees and the cost of legal defense) which UCS may incur by reason of: (i) Contractor's breach of any term, provision, covenant, representation or warranty contained in the contract awarded as a result of this bid; (ii) any act, omission, negligence or intentional misconduct of Contractor or its employees, subcontractors, agents, volunteers or of other persons under its direction and control; (iii) Contractor's performance or failure to perform under the contract; and (iv) enforcement by UCS of the awarded contract or any provisions thereof.

Independent Contractor Status

It is expressly understood and agreed that Contractor's status shall be that of an independent provider of services and that no officer, employee, servant, agent, or subcontractor of Contractor is an employee of the UCS, OCA or State of New York. Contractor shall be solely responsible for the work, assignment, compensation, benefits and personal conduct and standards of all such persons assigned to the provision of services. Nothing herein shall be construed to impose any liability or duty on the UCS, OCA or State of New York to persons, firms, consultants or corporations employed or engaged by Contractor either directly or indirectly in any capacity whatsoever, nor shall the UCS, OCA or State of New York be liable for any acts, omissions, liabilities, obligations or taxes of any nature including, but not limited to, unemployment and Workers' Compensation insurance of the Contractor or any of its employees or subcontractors.

Insurance Requirements

Contractor shall be required to maintain during the term of any contract awarded pursuant to this RFP, including any renewal terms, at its own cost and expense:

1. Workers' compensation and disability benefit insurance coverage as required under NYS law. Each vendor must provide with its proposal proof of such workers' compensation and disability benefits insurance coverage or, if it is legally exempt from such coverage, proof of exemption. Vendor must obtain the appropriate Workers Compensation Board forms from its insurance carrier or licensed agent or must follow the procedures set forth by the Workers' Compensation Board for obtaining an exemption from coverage. See Workers' Compensation Board website at http://www.wcb.ny.gov under "Forms" for a manual listing required forms and procedures. Any questions regarding workers' compensation coverage requirements or debarments should be directed to:

   Workers' Compensation Board
   Bureau of Compliance
   (518) 462-8882
   (866) 298-7830

   Only the following forms will be accepted:

   Proof of Workers' Compensation Coverage

   - **Form C-105.2** - Certificate of Workers' Compensation Insurance issued by private insurance carriers; or
   - **Form U-26.3** issued by the State Insurance Fund; or
   - **Form SI-12** - Certificate of Workers' Compensation Self-Insurance; or
   - **Form GSI-105.2** - Certificate of Participation in Workers' Compensation Group Self-Insurance; or
   - **Form CE-200** - Certificate of Attestation of Exemption from NYS Workers' Compensation and/or Disability Benefits Coverage.

   Proof of Disability Benefits Coverage

- **Form DB-120.1** - Certificate of Disability Benefits Insurance, or
- **Form DB-120.2** - Certificate of Participation in Disability Benefits Group Self-Insurance; or
- **Form DB-155** - Certificate of Disability Benefits Self-Insurance; or
- **Form CE-200** - Certificate of Attestation of Exemption from NYS Workers' Compensation and/or Disability Benefits Coverage.

On forms that have a space for a certificate holder to be listed, the carrier must enter:

NYS Unified Court System
Office of Court Administration
Office of Grants and Contracts
2500 Pond View, Suite 104
Castleton-on-Hudson, NY 12033

The insurance carrier will notify the certificate holder if a policy is canceled.

Please note: An ACORD Certificate of Insurance is not acceptable proof of NYS workers' compensation or disability benefits insurance coverage.

For additional information regarding worker's compensation and disability benefits requirements, please refer to the New York State Workers' Compensation Board website at: http://www.wcb.ny.gov under (Employers/Businesses."

2. Commercial General Liability Insurance (bodily injury and property damage on an occurrence basis), contractual and products/completed operations liability coverage, and auto liability with minimum limits as follows:

Bodily Injury and Property Damage	$2 million, per occurrence, $2 million, aggregate
Personal Injury and Advertising:	$1 million, per occurrence $2 million, aggregate
Contractual and Products/ Completed Operations	$2 million aggregate
Business, Auto Liability, Combined single limits	$1 million

The policy shall not contain exclusions for contractual liability, independent contractors, gravity-related injuries, or injuries sustained by employee of an insured or any insured.

3. Professional and Data Breach/Cyber Liability Insurance (Cyber Insurance) at not less than a $5,000,000 limit providing coverage for damages arising out of wrongful acts, errors, and omissions of Contractor. Cyber Insurance will provide third-party liability coverage and include Data Breach and Privacy Liability Insurance, including coverage for the failure to protect confidential information and failure of the security of the Contractor's computer systems or the UCS's systems due to the actions of the Contractor resulting in unauthorized access of UCS or its data.

4. Technology Errors and Omissions Insurance at not less than a $5,000,000 limit providing coverage for damages arising under computer related services, including, but not limited to consulting, data processing, programming, etc. The policy shall include coverage for third party fidelity including cyber theft.

5. Please note that if the policy is written on a Claims-Made basis, the Awarded Contractor must submit to UCS an endorsement providing proof that the policy provides the option to purchase Tail Coverage providing coverage for no less than one year after work is completed in the event that coverage is canceled or not renewed. This requirement applies to both primary and excess liability policies, as applicable.

6. Insurance Compliance:

   All policies shall be written with insurance companies authorized to do business in the State of New York and rated no lower than A-8 in the most current edition of A.M. Best's Property-Casualty Key Rating Guide. Policies should be endorsed to the New York State Unified Court System as an "additional insured" and "certificate holder." Contractor agrees to waive its right of recovery or subrogation against UCS and all indemnified parties and additional insureds. All policies shall allow waiver of subrogation in favor of UCS and indemnified parties and additional insureds. All policies must be endorsed to provide that in the event of cancellation, non-renewal or material modification UCS will received thirty (30) days' prior written notice thereof. Contractor must provide UCS with appropriate certificates of insurance in compliance with these requirements no later than five business days prior to commencement of the Contract. Contractor must furnish complete policies, including all endorsements thereto, to UCS upon request. By requiring insurance, UCS does not represent that certain coverage and limits will necessarily be sufficient to protect Contractor, and such coverage and limits shall not be deemed a limitation on Contractor's liabilities under any indemnity granted to UCS under any resulting agreement. Prior to the commencement of any work by a subcontractor, the Contractor shall require such subcontractor to procure policies of insurance as required herein and maintain the same in force during the terms of any work performed by that subcontractor.

Intellectual Property

If Contractor is required to produce specially commissioned materials pursuant to this Agreement (the "Work"), whether in written form, on tape, computer-readable media or other tangible form, Contractor acknowledges and agrees that UCS shall have the option to: (i) retain a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or otherwise use the Work or (ii) be the sole owner of the Work (the Work shall be considered a "work made for hire"), each of the foregoing at no additional cost to UCS.

Notice of Substantial Change in Contractor Status

In addition to complying with the requirements of State Finance Law Section 138 (requiring prior approval of subcontractors and assignments or conveyances), Contractor shall notify UCS of any substantial change in the ownership or financial viability of the Contractor, its affiliates, subsidiaries, divisions, or partners, in writing immediately upon occurrence. "Substantial change" means: (i) sales, acquisitions, mergers, or takeovers of the Contractor, its affiliates, subsidiaries, divisions, or partners that result in a change in the controlling ownership or assets of such entity after the submission of the bid; (ii) entry of an order for relief under Title 11 of the U.S. Code; (iii) the making of a general assignment for the benefit of creditors; (iv) the appointment of a receiver of Contractor's business or property or that of its affiliates, subsidiaries, divisions, or partners; or action by Contractor, its affiliates, subsidiaries, divisions, or partners under any State insolvency or similar law for the purposes of its bankruptcy, reorganization, or liquidation; or (v) court-ordered liquidation of Contractor, its affiliates, subsidiaries, subdivisions, or partners.

Upon UCS's receipt of such notice it shall have thirty (30) business days to review the information. Contractor may not transfer the Contract to or among affiliates, subsidiaries, divisions, or partners, or to any other person or entity, without the express written consent of UCS. In addition to any other remedies available at law or equity, UCS shall have the right to cancel the Contract, in whole or in part, for cause, if it finds, in its sole judgment, that such substantial change adversely affects the delivery of Services or is otherwise not in the best interests of UCS.

Outstanding Tax Liabilities

Contractor warrants that there are no outstanding tax liabilities against the Contractor in favor of the State of New York, or in the event such liabilities exist, a payment schedule has been arranged for their speedy satisfaction before contract execution.

Public Information and Freedom of Information Law

Disclosure of information related to this procurement and the resulting contract shall be permitted consistent with the laws of the State of New York and specifically, Article 6 of the New York Public Officers Law (FOIL). UCS shall take reasonable steps to protect from public disclosure any records or portions thereof relating to this procurement that are exempt from disclosure under FOIL. Information constituting trade secrets or critical infrastructure information for purposes of FOIL must be clearly marked and identified as such by Contractor upon submission in accordance with the RFP provisions. If Contractor intends to request an exemption from disclosure under FOIL for trade secret materials or critical infrastructure information, Contractor shall at time of submission, request the exemption in writing and provide an explanation of (i) why the disclosure of the identified information would cause substantial injury to the competitive position of Contractor, or (ii) why the information constitutes critical infrastructure information which should be exempted from disclosure pursuant to Section 87(2) of FOIL. Acceptance of the identified information by UCS does not constitute a determination that the information is exempt from disclosure under FOIL. Determinations as to whether materials or information may be withheld from disclosure will be made in accordance with FOIL at the time a request for such information is received by UCS.

Registration with NYS Department of State

Prior to being awarded a contract and throughout the duration of the resulting Contract, Contractor shall be registered with the NYS Department of State as an entity authorized to conduct business in New York State.

Sales and Compensating Use Tax Certification

Tax Law Section 5-a applies to all Agreements valued in excess of $100,000 for the sale of goods or services as defined in Article XI of the State Finance Law, and/or tangible personal property or taxable services as defined by the Tax Law.

FORM ST-220-CA ("CONTRACTOR CERTIFICATION TO COVERED AGENCY") MUST BE COMPLETED AND SIGNED AND SUBMITTED WITH THE PROPOSAL.

BIDDERS ARE RESPONSIBLE FOR FILING FORM ST-220-TD ("CONTRACTOR CERTIFICATION") WITH THE NYS DEPARTMENT OF TAXATION & FINANCE.

- Note: Form ST-220-CA provides a certification that the Bidder has submitted Form ST-220-TD to the New York State Department of Taxation and Finance.

Form ST-220-CA is available at: https://www.tax.ny.gov/pdf/current_forms/st/st220ca_fill_in.pdf

Form ST-220-TD is available at: https://www.tax.ny.gov/pdf/current_forms/st/st220td_fill_in.pdf

The Unified Court System is not authorized to address questions regarding the Tax Law or its interpretation. Any questions regarding the Law must be directed to the New York State Department of Taxation and Finance.

Savings/Force Majeure

A force majeure occurrence is an event or effect that cannot be reasonably anticipated or controlled. Force majeure includes, but is not limited to, acts of nature, acts of war, acts of public enemies, strikes, fires, explosions, actions of the elements, floods, or other similar causes beyond the control of the Contractor or the UCS in the performance of the Contract which non-performance, by exercise of reasonable diligence, cannot be prevented. Contractor shall provide the UCS with written notice of any force majeure occurrence as soon as the delay is known.

Neither the Contractor nor the UCS shall be liable to the other for any delay in or failure of performance under the Contract due to a force majeure occurrence. Any such delay in or failure of performance shall not constitute

default or give rise to any liability for damages. The existence of such causes of such delay or failure shall extend the period for performance to such extent as determined by the Contractor and the UCS to be necessary to enable complete performance by the Contractor if reasonable diligence is exercised after the cause of delay or failure has been removed.

Notwithstanding the above, at the discretion of the UCS where the delay or failure will significantly impair the value of the Contract to the State, the UCS may:

a. Accept allocated performance or deliveries from the Contractor. The Contractor, however, hereby agrees to grant preferential treatment to UCS with respect to Product subjected to allocation; and/or

b. Purchase from other sources (without recourse to and by the Contractor for the costs and expenses thereof) to replace all or part of the Products which are the subject of the delay, which purchases may be deducted from the Contract quantities without penalty or liability to the State; or

c. Terminate the Contract or the portion thereof which is subject to delays, and thereby discharge any unexecuted portion of the Contract or the relative part thereof.

In addition, the UCS reserves the right, in its sole discretion, to make an equitable adjustment in the Contract terms and/or pricing should extreme and unforeseen volatility in the marketplace affect pricing or the availability of supply. "Extreme and unforeseen volatility in the marketplace" is defined as market circumstances which meet the following criteria: (i) the volatility is due to causes outside the control of Contractor; (ii) the volatility affects the marketplace or industry, not just the particular Contract source of supply; (iii) the effect on pricing or availability of supply is substantial; and (iv) the volatility so affects Contractor's performance that continued performance of the Contract would result in a substantial loss.

Subcontractors

UCS will contract directly with the Bidder as the Prime Contractor. The Prime Contractor is the sole contractor with regard to the provisions of the solicitation and the contract resulting from the solicitation. No subcontract entered into by the Contractor shall relieve the Contractor of any liabilities or obligations in this RFP or the resultant contract. The Contractor agrees not to subcontract any of its services, unless as indicated in its proposal, without the prior written approval of the UCS. Approval shall not be unreasonably withheld upon receipt of written request to subcontract. The Contractor may arrange for a portion/s of its responsibilities under this Agreement to be subcontracted to qualified, responsible subcontractors, subject to approval of the UCS. If the Contractor determines to subcontract a portion of the services, the subcontractors must be clearly identified and the nature and extent of its involvement in and/or proposed performance under this Agreement must be fully explained by the Contractor to the UCS.

The Contractor retains ultimate responsibility for all services performed under the Agreement.

All subcontracts shall be in writing and shall contain provisions, which are functionally identical to, and consistent with, the provisions of this Agreement including, but not limited to, the body of this Agreement, Appendix A – Standard Clauses for UCS Contracts and the solicitation/procurement document, including additional contract terms outlined therein. Unless waived in writing by the UCS, all subcontracts between the Contractor and subcontractors shall expressly name UCS as the sole intended third party beneficiary of such subcontract. The UCS reserves the right to review and approve or reject any subcontract, as well as any amendment to said subcontract(s), and this right shall not make the UCS or the State a party to any subcontract or create any right, claim, or interest in the subcontractor or proposed subcontractor against the UCS. If total compensation to a

subcontractor exceeds $100,000, the subcontractor must submit and certify a Vendor Responsibility Questionnaire.

The UCS reserves the right, at any time during the term of the Agreement, to verify that the written subcontract between the Contractor and subcontractors is in compliance with all of the provisions of this Section and any subcontract provisions contained in this Agreement. Subcontractors may be required to submit to a background check in accordance with the solicitation or resulting contract.

The Contractor shall give the UCS immediate notice in writing of the initiation of any legal action or suit which relates in any way to a subcontract with a subcontractor or which may affect the performance of the Contractor's duties under the Agreement. Any subcontract shall not relieve the Contractor in any way of any responsibility, duty and/or obligation of the Agreement.

Suspension of Work

UCS reserves the right to suspend any and all activities under this Contract, at any time should funding become unavailable. In the event of such suspension, the Contractor will be given a formal written notice outlining the particulars of such suspension, and will be paid for services performed prior to suspension in accordance with the Contract. Any such suspension will not be deemed to extend the term of the Agreement beyond the expiration date of the term, including any renewal or extension term. Nothing in this paragraph shall diminish UCS's right to terminate the Contract as provided therein.

Termination

A. FOR CONVENIENCE

By written notice, the Contract may be terminated at any time by UCS for convenience upon ninety (90) days' written notice without penalty or other early termination charges due. Such termination of the Contract shall not affect any project or purchase order that has been issued under the Contract prior to the date of such termination. If the Contract is terminated pursuant to this paragraph, UCS shall remain liable for all accrued but unpaid charges incurred through the date of termination.

B. FOR BUDGET MODIFICATION

1. Notwithstanding any other provision contained in this RFP, if the UCS Budget ("Budget") is modified (a "Budget Modification", defined in subsection 2 below) for any State fiscal year included in the term of the awarded contract, in whole or in part (including any renewal or extension term), such that UCS determines, in its sole discretion, that it is necessary to reduce, eliminate or otherwise modify the budget allocation covering payment thereunder, UCS shall have the option to terminate the awarded contract upon not less than thirty (30) days' notice to awarded contractor, without liability for costs, expenses or damages as a result thereof.
2. For purposes of this subsection A, Budget Modification shall mean and include, with respect to the Budget or any appropriation contained therein:
    i. any reduction, elimination or restriction upon access thereto as provided by law; or
    ii. any restriction placed on UCS spending authority, including any restriction imposed by UCS upon itself in response to a request of the Executive or Legislative Branch of government.
3. Termination hereunder shall be further governed by the termination provisions contained in the awarded contract, as applicable.

C. FOR CAUSE

For a material breach that remains uncured for more than thirty (30) days from the date of written notice to the Contractor, the Contract may be terminated by UCS at Contractor's expense where Contractor become unable or incapable of performing, or meeting any requirements or qualifications set forth in the Contract, or for non-performance, or upon a determination that Contractor is non-responsible or for any other reason stated in this section with the exception of termination for convenience. Such termination shall be upon written notice to the Contractor. In such event, UCS may complete the contractual requirements in any matter it may deem advisable and pursue available legal or equitable remedies for breach. Early termination of the contract for cause may result in, among other consequences, all remedies available to UCS and New York State, the Contractor both being declared non-responsible by the UCS/OCA, pursuant to the UCS and Office of the State Comptroller's guidelines on vendor responsibility and in the Awarded Contractor's removal from the UCS/OCA's bidders list for future solicitations.

D. FOR FINDINGS RELATED TO VENDOR RESPONSIBILITY

UCS may, in its sole discretion, terminate the Contract if it finds at any time during the term of the Contract that the Contractor is non-responsible or that any information provided in the Vendor Responsibility Questionnaire submitted with Contractor's bid was materially false or incomplete, or if the Contractor fails to timely or truthfully comply with UCS's request to update its Vendor Responsibility Questionnaire.

E. FOR SUSPENSION OR DELISTING OF CONTRACTOR'S SECURITIES

If the Contractor's securities are suspended or delisted by the New York Stock Exchange, the American Stock Exchange, or the NASDAQ, as applicable, if the Contractor ceases conducting business in the normal course, becomes insolvent, makes a general assignment for the benefit of creditors, suffers or permits the appointment of a receiver for its business or assets or avails itself of or becomes subject to any proceeding under the Federal Bankruptcy Act or any statute of any state relating to insolvency or the protection of rights of creditors, UCS may, in its sole discretion, terminate the Contract or exercise such other remedies as shall be available under the Contract, at law, or in equity.

Warranties and Guarantees

Contract Deliverables: Contractor warrants and represents that the Services required by the RFP and the Contract shall be performed or provided in accordance with all the terms and conditions, covenants, statements, and representations contained in the Contract. Contractor's failure to meet pre-defined service levels may result in a credit or chargeback in an amount pre-determined by the parties.

Personnel Warranty: Contractor warrants and represents that all personnel performing Services under this Contract are qualified to provide Services and eligible for employment in the United States and shall remain so throughout the terms of the Contract. Contractor shall provide such proof of compliance as is required by UCS.

Product Performance: Contractor hereby warrants and represents that products acquired by UCS under this Contractor conform to the manufacturer's specifications, performance standards, and documentation and that the documentation fully describes the proper procedure for using the products.

Title and Ownership: Contractor warrants and represents that it has (i) full ownership, clear title free from al liens or (ii) the right to transfer or deliver specified license rights to any product acquired by UCS under this Agreement. Contractor shall be solely liable for any costs of acquisition associated therewith. Contractor shall indemnify UCS and hold UCS harmless from any damages and liabilities, including reasonable attorneys' fees and costs, arising from any breach of Contractor's warranties as set forth herein.

Workmanship Warranty: Contractor warrants and represents that all services and deliverables shall meet the completion criteria set forth in the Contract, and that services will be provided in a professional and

workmanlike manner in accordance with the highest applicable industry standards. Contractor further warrants and represents that all products, components or parts specified and furnished by and through Contractor, whether specified and furnished individually or as a system, shall be free from defects in material and workmanship and will conform to all requirements in the Agreement for the manufacturer's standard commercial warranty period, if applicable, or for a minimum of one year from the date of acceptance, whichever is longer.

EXHIBIT F: SECURITY OPERATIONS CENTER TERMS AND CONDITIONS

The Procurement, the Bidder's Proposal, and the contract award that results from this Request for Proposal (RFP) are subject to and incorporate the following terms and conditions:

I. GENERAL

A. Within 30 days of Contract approval, Contractor will provide a Consensus Assessment Initiative Questionnaire (CAIQ) for UCS's review. Thereafter on an annual basis, on the anniversary of the Contract Award or as otherwise fixed in a writing signed by both parties, Contractor will provide a current CAIQ for UCS' review. The form is available at Cloud Security Alliance (https://cloudsecurityalliance.org/). The completion of this requirement is at the Contractor's expense with no additional cost to UCS.

B. Within 30 days of Contract approval, Contractor will provide, at Contractor's expense, an independent third-party audit of controls related to the security, availability, or processing integrity of a system or the confidentiality or privacy of the information processed by that system for all systems used to perform the services under the resulting Contract showing no deficiencies. Such audit must meet the requirements of a Service Organization Control (SOC) 2 Type 2 audit report or approved equivalent. Thereafter on an annual basis, at the Contractor's expense, a full version of the audit report will be provided to the UCS, within 30 days of the anniversary date of the Contract. Any deficiencies identified in the audit report or where the Contractor is found to be noncompliant with Contract safeguards, must be remedied, within 90 days of the issue date of the audit report with proof of remediation provided to the UCS. The completion of this requirement is at the Contractor's expense with no additional cost to UCS.

C. All data center(s) used to perform the services under the resulting Contract must be NIST Tier 4 compliant.

D. Contractor agrees that the SOC services provided pursuant to this Contract shall comply with applicable federal and/or New York State laws, regulations, and requirements.

E. The technical and professional activities required for establishing, managing, and maintaining the mirrored Splunk environment used to provide SOC services are the responsibilities of the Contractor.

F. Within ten (10) business days of Contract approval, Contractor must provide a copy of its Standard Operating Procedures for SOC. Any updates to this manual must be provided within ten (10) business days of the change throughout the course of the engagement.

G. Audit logs must capture all access to UCS Data (log information to include username, event type, event operation, event details, successful/unsuccessful authentication events, system start/stop, hardware attachment/detachment, system alerts and error messages and other security events, unsuccessful attempts to access/modify/delete data being logged or data in the event table).

H. Contractor agrees that it shall perform the SOC service in a manner consistent with the following requirements:

1. Host all UCS metadata and maintain and implement procedures to logically segregate and secure UCS data from Contractor's data and data belonging to Contractor's other customers, including other governmental entities.

2. Establish and maintain appropriate environmental, safety and facility procedures, data security procedures and other safeguards against the destruction, corruption, loss, or alteration of the SOC and any UCS data, and to prevent unauthorized access, alteration, or interference by third parties of the same.

3. Utilize industry best practices and technology (including appropriate firewall protection, intrusion prevention tools, and intrusion detection tools) to protect, safeguard, and secure the SOC and UCS data against unauthorized access, use, and disclosure. Contractor shall constantly monitor for any attempted unauthorized access to, or use or disclosure of, any of such materials and shall immediately take all necessary and appropriate action in the event any such attempt is discovered, promptly notifying UCS of any material or significant breach of security with respect to any such materials.

II. SERVICE LEVEL REQUIREMENTS:

A. The SOC, including the Web Portal, shall be available 99.982% of the time (uptime) per month and must not be rendered inoperable for the purpose of maintenance, upgrades, or hardware additions. Any disputes regarding unavailability of the SOC shall be managed using an established dispute resolution procedure.

B. Contractor shall ensure the SOC is scalable to maintain performance during peak periods of network activity and user access.

C. Contractors must provide the UCS the root cause, analysis and proposed resolution plan for any outage or failure to escalate an event.

D. It is critical to the success of this Contract that the SOC be maintained in a timely manner and that the Contractor operate in an extremely reliable manner. It would be impracticable and extremely difficult to fix the actual damage sustained by UCS in the event of certain delays or failures in administration and provision of services under this Contract. In the event that SLAs are not achieved and that the failure is attributable to the Contractor or third parties working on behalf of the Contractor, service credits will be issued to UCS as follows:

Table 1: Event Security Level Notification and Response Requirements

Security Level	Title	Description	Initial Notification* Timeframe	Acknowledged**	Response***	Service Credit
1	Emergency	Issue requiring immediate action to minimize risk to UCS	10 minutes	30 minutes	30 minutes	1/30th of Contractor's total monthly invoice at the time of the event that gave rise to the Service Credit
2	Critical	High-risk attacks or possible compromises. Immediate action is necessary to mitigate	15 minutes	60 minutes	60 minutes	
3	Warning	Suspicious events which may require additional investigation by UCS. Not high-risk and do not require immediate action to mitigate.	1 hour	4 hours	20 hours	
4	Low / Information	Routine events with no known impact to UCS. Provided for information / reporting purposes	2 hours	24 hours	96 hours	

* Initial Notification Timeframe is from when an alert is received through security monitoring and UCS is notified of the event. Notification methods are based on approved escalation procedures as documented in the SOC/ UCS runbook. If a dispute arises as to the severity level of an Event, UCS will consult with the Contractor to determine the appropriate level. If no agreement can be reached, UCS will be the final determiner of the level assigned to a particular Event.

** "Notification / Acknowledged" is measured from the time when notification of an outage or service degradation, either through monitoring or an authorized technical contact, is detected until an engineer is assigned. This timeframe runs concurrently with the Initial Notification Timeframe.

*** "Response" is measured from the time when an incident is assigned, triaged, and escalated to UCS detailing remediation action(s) necessary to restore service.

Table 2: Service Performance Requirements			
	Service Performance	**Metric**	**Service Credit**
1	Service Availability	Available > 99.982% per calendar month	1/30th of the Contractor's total monthly invoice at the time of the event that gave rise to the Service Credit.
2	Continuous Downtime	Over 30 minutes in a 24-hour period	
3	Failure to Report Root-Cause and Proposed Fix	Over one (1) hour	

- Service Availability. UCS shall receive an Availability Service Credit if it experiences performance issues in which MSS SOC Availability (measured in a calendar month) is less than 99.982% and the source of the performance issue is within the sole control of the Contractor or their agents. Service Availability includes, but is not limited to, full functionality of the monitoring services, including the SOC, as well as access to and full functionality of the Portal.

- Continuous Downtime in Excess of 30 Minutes. In addition to Service Availability credits, UCS shall receive an Availability Service Credit if it experiences performance issues in which SOC is unavailable for a continuous period that exceeds thirty (30) minutes within any 24-hour period and the source of the performance issue is within the sole control of the Contractor or their agents.

- Failure to Report Root-Cause and Proposed Fix of Downtimes in Excess of one (1) Hour. UCS shall receive an Availability Service Credit if the Contractor fails to provide a report of the root cause and proposed fix of the downtime within the time periods described.

III. SERVICE CREDITS (AVAILABILITY SERVICE CREDIT OR DEVICE SERVICE CREDIT)

A. **Maximum Service Credits**. In the event that UCS experiences downtime, in other than a catastrophic event, it shall be eligible to receive from the Contractor a service credit. The aggregate maximum number of service credits to be issued by the Contractor in a single calendar month shall not exceed the total monthly invoice for the month that gave rise to the Service Credits. Contractor will provide the Service Credit(s) on the next monthly invoice. Credits can accumulate due to multiple incidents in the same month.

B. UCS, at its sole discretion, may elect to waive any service credits based upon precipitating events such as: catastrophic failure, multiple simultaneous failures and/or acknowledgement of Contractor's best effort to sustain/restore service.

C. Amounts due hereunder shall be in addition to any other amount due UCS and no provision of this section precludes the State from pursuing any other remedies to which it may be entitled under the Contract.

IV. SERVICE REPORTING REQUIREMENTS

A. The Contractor will provide the following reporting, monthly, quarterly and annually and ad hoc, as requested, or as otherwise agreed upon by the parties:

1. Service Availability Reports

2. Outage Summary Report to include:

- The start and end time of each outage;
- The duration of the outage;
- Reason for the outage, if not known then a delivery date of a root cause analysis report will be given by the Contractor;
- Description of the actions required to resolve the outage problem; and
- Total time the Service was unavailable.

B. The Contractor shall provide the reports/documentation as a condition precedent to payment under the Contract. Failure to provide a report required within the due dates set forth in the paragraph, below, shall subject the Contractor to the penalties set forth herein. Upon notice, the Contractor shall have an opportunity to cure the default or be subject to Contract termination. UCS's failure to demand or receive required documentation shall not be deemed a waiver of rights under this paragraph.

C. All reports shall be delivered electronically. The parties to the Contract shall agree to an electronic format (e.g., application and required data elements) for each of the reports set forth in this section. Each report shall be transmitted to UCS electronically via the internet utilizing encryption standards and protocols approved by UCS and the system used shall generate an electronic ticket acknowledging transmission.

D. All reports required under this Section shall be due within ten (10) business days after the last day of the required reporting period. In the event the Contractor fails to produce and deliver the specified report within this time frame the State shall receive a quarter (.25) of an Availability Service Credit per business day until the report is received in writing by UCS to the designated contact.

E. The (i) failure of UCS to collect said amounts or to provide the foregoing notice, or (ii) the payment by UCS of amounts otherwise due Contractor shall not be deemed a waiver by UCS of the right to enforce the provisions of this paragraph.

F. UCS reserves the right upon written notice to Contractor, to modify the frequency and reporting deadlines set forth above.

V. Ordering and Invoicing Process

A. **Estimated Quantities**: The Contract resulting from this solicitation is an estimated quantity contract.

B. **Ordering Process**

1. The products/services to be provided to UCS will be specified in an initial Letter Order with associated pricing as agreed to in the resulting Contract, and in a form acceptable to UCS. After the initial Letter Order, UCS may use the Letter Order Change process to either order additional Products/Services, within scope of this RFP or terminate Products/Services at UCS's discretion. In order to terminate an existing service, or any portion hereof, the UCS must submit a revised Letter Order to Contractor specifying the Services to be terminated and the applicable termination dates. UCS shall make payment for terminated Services up to the date of termination. The date of termination will be the date specified in the order terminating the service. There will be no cost to UCS to terminate a service.

2. UCS is only responsible for the quantities actually ordered via the Letter Order process during the engagement.

3. The Contractor may invoice and UCS will be responsible for payment on any Services ordered when the Service is operational (e.g., when logs are being received and analyzed by the SOC). When Services are ordered or terminated in between Contractor's billing cycle, UCS will only be responsible for the pro rata share for that Service for the applicable month. If a Service is terminated in between Contractor's billing cycle, Contractor will issue UCS a credit for the pro rata share of any unused services to be included in the next billing cycle.

VI. Final Migration Plan

Within thirty (30) calendar days of Contract award, the selected SOC must provide a final migration plan to UCS that includes the chronological outline of all activities to be performed during the on-boarding phase including key timelines, deliverables, and party(-ies) responsible. SOC must maintain prompt (within 24–72 hour response) and ongoing communication with the UCS project management team and provide advice, consultation, and written opinions/recommendations as needed during the migration process. The final plan will be negotiated with the Contractor and approved by UCS

VII. Dispute Resolution Plan

The Contractor and UCS shall agree upon a final dispute resolution plan within one month of contract award.

EXHIBIT G: REFERENCES

Bidders must use this form to furnish the references required in Section 6.2.5 of the RFP.

BIDDER'S NAME: _____

REFERENCE # 1				
Name of the Client Firm:				
Client Firm's Address:				
Briefly describe the type and scope of services of the engagement (include # of sites, devices, and users)				
Engagement Budget:				
Engagement Term:	Start Date: (Month/Year)		End Date: (Month/Year)	
Was a subcontractor used? If so, describe subcontractor's role				
Client Contact Name and Title:				
Phone Number:		Email:		
Alternate Client Contact Name and Title:				
Phone Number:		Email:		

REFERENCE # 2				
Name of the Client Firm:				
Client Firm's Address:				
Briefly describe the type and scope of services of the engagement (include # of sites, devices, and users)				
Engagement Budget:				
Engagement Term:	Start Date: (Month/Year)		End Date: (Month/Year)	
Was a subcontractor used? If so, describe subcontractor's role				
Client Contact Name and Title:				
Phone Number:		Email:		
Alternate Client Contact Name and Title:				
Phone Number:		Email:		

EXHIBIT G: REFERENCES (continued)

REFERENCE # 3				
Name of the Client Firm:				
Client Firm's Address:				
Briefly describe the type and scope of services of the engagement (include # of sites, devices, and users)				
Engagement Budget:				
Engagement Term:	Start Date: (Month/Year)		End Date: (Month/Year)	
Was a subcontractor used? If so, describe subcontractor's role				
Client Contact Name and Title:				
Phone Number:		Email:		
Alternate Client Contact Name and Title:				
Phone Number:		Email:		

Exhibit H

NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Policy	**No:** NYS-P03-002
IT Policy: **Information Security**	**Updated:** 11/23/2021
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

This policy defines the mandatory minimum information security requirements for all State Entities (SEs) as defined below in Section 3.0 Scope. Any SE may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this policy, but must, at a minimum, achieve the security levels required by this policy.

This policy acts as an umbrella document to all other Office of Information Technology Services' (ITS) security policies and associated standards. This policy defines the responsibility of all SEs to:

- protect and maintain the confidentiality, integrity, and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- ensure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss, or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity, and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions, and vital government functions; compromise data; and result in legal and regulatory non-compliance.

This policy benefits SEs by defining a framework that will ensure appropriate measures are in place to protect the confidentiality, integrity, and availability of New York State (NYS) information; and ensure staff and all other affiliates understand their role and responsibilities, have adequate knowledge of security policy, procedures, and practices, and know how to protect SE information.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117*[1], issued January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy*, NYS-P08-002, Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

3.0 Scope

This policy applies to all SEs, defined as "State Government" entities as defined in *Executive Order 117*[1], issued January 2002, or "State Agencies" as defined in *Section 101 of the State Technology Law* including their employees, and all third parties (e.g., local governments, consultants, vendors, and contractors), that use or access any IT resource for which the SE has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. While an SE may adopt a different policy, it must include the requirements set forth in this one.

This policy encompasses all systems, automated and manual, for which New York State has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. It addresses all information, regardless of the form or format, which is created or used in support of business activities of SEs.

4.0 Information Statement

4.1 Organizational Security

a. Information security requires both an information risk management function (including cyber-related risk management) and an information technology security function. Depending on the structure of the SE, an individual or group can serve in both roles or a separate individual or group can be designated for each role. It is

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

recommended that these functions be performed by a high-level executive or a group that includes high level executives.

1. Each SE must designate an individual or group to be responsible for the risk management function. For the purposes of clarity and readability, this policy will refer to the individual, or group, so designated as the Cyber Risk Coordinator (CRC) (*see* Exhibit 1 for a more detailed description of the role). The CRC is responsible for ensuring that:

    i. risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed from the perspective of the SE as an enterprise regarding the overall strategic goals and objectives of the SE in carrying out its core missions and business functions; and

    ii. the management of information assets, information system-related security risks, and other cyber-security risks is consistent across the SE, reflects the risk tolerance of the SE, and is considered along with other types of risks to ensure mission/business success.

2. Each SE must designate an individual or group to be responsible for the technical information security function. For purposes of clarity and readability, this policy will refer to the individual, or group, designated as the Information Security Officer (ISO)/designated security representative. This function will be responsible for evaluating and advising on information security risks. For SEs that receive IT services as a member of one of the portfolios within ITS, the information security function may be fulfilled by the Chief Information Security Office (CISO) and Security Services Teams.

b. Information security risk decisions must be made through consultation with both function areas described in **a.** above.

c. Although the technical information security function may be outsourced to third parties, each SE retains overall responsibility for the security of the information that it owns. The function of the CRC must be performed within the SE.

4.2 Functional Responsibilities

4.2.1 State Entity executive management is responsible for:

1. evaluating and accepting risk on behalf of the SE;

2. identifying SE information security responsibilities and goals and integrating them into relevant processes;

3. supporting the consistent implementation of information security policies and standards;

4. supporting security within the SE through clear direction and demonstrated commitment of appropriate resources;

5. promoting awareness of information security best practices through the regular dissemination of materials provided by the ISO/designated security representative;

6. implementing a process for determining information classification and categorization, based on industry recommended practices, State directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information;

7. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;

8. determining who, within the SE, will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;

9. participating in the response to security incidents;

10. complying with applicable notification requirements in the event of a breach of private information;

11. adhering to specific legal and regulatory requirements related to information security;

12. communicating legal and regulatory requirements to the ISO/designated security representative; and

13. communicating the requirements of this policy and the associated standards, including the consequences of non-compliance, to the SE workforce and third parties, and addressing adherence in third party agreements.

4.2.2 The ISO/designated security representative is responsible for:

1. maintaining familiarity with SE business functions and requirements;

2. maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;

3. assessing SE compliance with information security policies and legal and regulatory information security requirements;

4. evaluating information security risks and assisting the SE in understanding its information security risks and how to appropriately manage those risks;

5. representing and ensuring security architecture considerations are addressed;

6. advising on security issues related to procurement of products and services;

7. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;

8. disseminating threat information to appropriate parties;

9. participating in the response to potential security incidents;

10. participating in the development of enterprise policies and standards for NYS that consider SE needs; and

11. promoting information security awareness.

4.2.3 IT management is responsible for:

1. supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;

2. providing resources needed to maintain a level of information security control consistent with this policy;

3. identifying and implementing all processes, policies, and controls relative to security requirements defined by the SE's business and this policy;

4. implementing the proper controls for information owned by the SE based on the SE's classification designations;

5. providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);

6. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures; and

7. implementing business continuity and disaster recovery plans.

4.2.4 The State Entity workforce is responsible for:

1. understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information entrusted to SEs;

2. protecting State information and resources from unauthorized use or disclosure;

3. protecting personal, private, sensitive information (PPSI) from unauthorized use or disclosure;

4. abiding by ITS Policy, NYS-P14-001, Acceptable Use of Information Technology Resources; and

5. reporting suspected information security incidents or weaknesses to the appropriate manager and ISO/designated security representative.

4.2.5 The CISO is responsible for:

1. providing in-house expertise as information security consultants to the SEs as needed;
2. developing the State's information security program and strategy, including measures of effectiveness;
3. establishing and maintaining enterprise information security policy and standards;
4. assessing SE compliance with information security policies and standards;
5. advising on secure system engineering;
6. providing incident response coordination and expertise;
7. monitoring the State networks for anomalies;
8. monitoring external sources for indications of SE data breaches, defacements, etc.
9. maintaining ongoing contact with security groups/associations and relevant authorities;
10. providing timely notification of current threats and vulnerabilities; and
11. providing awareness materials and training resources.

Associated Standard: NYS-S10-001, Continuing Professional Education Requirements for ISOs/Designated Security Representatives Standard

4.3 Separation of Duties

a. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.

b. Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails, and management supervision.

c. The audit and approval of information security controls must always remain independent and segregated from the implementation of said controls.

4.4 Information Risk Management

a. Any system or process that supports SE business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.

b. Risk assessments are required for new projects, implementations of new technologies, any significant updates, or changes to the operating environment, or in response to the discovery of significant vulnerabilities. Risk assessments are

required regardless if the work is done by SE, vendor/contractor, or any other third party on behalf of the SE.

c. SEs are responsible for selecting the risk assessment approach they will use based on their needs and any applicable laws, regulations, and policies.

d. Risk assessments must include additional considerations when systems, services, or information will reside, or be accessed from, outside of the Contiguous United States (CONUS) to ensure compliance with relevant statutory, regulatory, and contractual requirements.

e. Risk assessment results, and the decisions made based on these results, must be documented.

Associated Standard: NYS-S14-001, Information Security Risk Management Standard; NYS-S13-001, Secure System Development Lifecycle (SSDLC) Standard

4.5 Information Classification and Handling

a. All information, which is created, acquired, or used in support of SE business activities, must only be used for its intended business purpose.

b. All information assets must have an information owner established within the SE's lines of business.

c. Information must be properly managed from its creation, through authorized use, to proper disposal.

d. All information assets must be reviewed and reclassified (if needed) on a recurring basis, with a frequency determined by the SE. Any changes to the individual data elements of an information asset requires an immediate review.

e. An information asset must be classified based on the highest level necessitated by its individual data elements.

f. If the SE is unable to determine the confidentiality classification of information then it must have a high confidentiality classification and, therefore, is subject to high confidentiality controls.

g. Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.

h. All reproductions of information in its entirety must carry the same confidentiality classification as the original. Partial reproductions need to be evaluated to determine if a new classification is warranted.

i. Each classification has an approved set of baseline controls designed to protect the data asset and is aligned with NIST 800-53B Control Baselines for Information

Systems and Organizations. These controls must be evaluated, tailored, and implemented to meet business requirements.

j. The SE must communicate the requirements for secure handling of information to its workforce.

k. A written or electronic inventory of all SE information assets must be maintained by the SE.

Associated Standards: NYS-S14-002, Information Classification Standard; NYS-S13-003, Sanitization/Secure Disposal Standard; NYS-S14-003, Information Security Controls

4.6 Information Sharing

a. SE content made available to the general public must be reviewed according to a process to be defined and approved by the SE. The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted.

b. PPSI must not be made available without appropriate safeguards approved by the SE.

c. For non-public information to be released outside a SE or shared between SEs, a process must be established that, at a minimum:

   1. ensures that an information classification has been performed and documented for the information to be released or shared;

   2. documents the intended use of the information;

   3. identifies the responsibilities of each party for protecting the information;

   4. defines the process and minimum controls required to transmit, store, and use the information;

   5. records the measures that each party has in place to protect the information;

   6. defines a method for compliance measurement;

   7. provides a signoff procedure for each party to accept responsibilities,

   8. establishes a schedule and procedure for reviewing the controls; and

   9. identifies an end date for the use of the information (if applicable).

d. In addition to the requirements in Section 4.6.c, when information classified as having a High Confidentiality requirement is to be released or shared, the SEs must ensure that they:

1. have a formal written agreement (e.g., Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU), etc.), which contains the requirements for the handling of information, in place prior to sharing that information with any other SE or other third-party.

2. designate the level of management who can give written approval for:

    i. the transportation or storage of information outside of an approved storage facility and
    ii. the transmission of information outside the SE.

Associated Standards: NYS-S14-002, Information Classification Standard

4.7 IT Asset Management

a. All IT hardware and software assets must be assigned by the SE to a designated business unit or individual within the SE.

b. SEs are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting. This inventory must be automated where technically feasible.

c. Processes, including regular scanning, must be implemented to identify unauthorized hardware and/or software and notify appropriate staff when discovered.

Associated Standard: NYS-S14-008, Secure Configuration Standard

4.8 Personnel Security

a. The SE workforce must receive general information security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on SE specific information security procedures, if required, must be completed before access is provided to specific SE sensitive information not covered in the general information security training. All information security training must be reinforced at least annually and must be tracked by the SE.

b. A SE must require its workforce to abide by the ITS Policy, NYS-P14-001, Acceptable Use of Information Technology Resources, and an auditable process must be in place for users to acknowledge that they agree to abide by the policy's requirements.

c. All job positions must be evaluated by the SE to determine whether they require access to sensitive information and/or sensitive information technology assets.

d. For those job positions requiring access to sensitive information and sensitive information technology assets, SEs must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation, or contract.

Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state, and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for the SE to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the State.

e. A process must be established within the SE to repeat or review suitability determinations periodically and upon change of job duties or position.

f. SEs are responsible for ensuring all State-issued property is returned prior to an employee's separation and accounts are disabled and access is removed immediately upon separation.

Associated Standard: NYS-S14-013, Account Management/Access Control Standard

4.9 Information Security Incident Management

a. SEs must have an incident response plan, consistent with New York State standards, to effectively respond to information security incidents.

b. All observed or suspected information security incidents or weaknesses are to be reported to appropriate management and the ISO/designated security representative as quickly as possible. If a member of the workforce feels that information security concerns are not being appropriately addressed, they may confidentially contact the New York State Cyber Command Center directly.

c. The New York State Cyber Command Center must be notified of any information security incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to follow proper incident response procedures and guarantee coordination and oversight.

Associated Standard: NYS-S13-005, Cyber Incident Response Standard; See also: Cyber Incident Reporting Procedure

4.10 Physical and Environmental Security

a. Information processing and storage facilities must have a defined security perimeter and appropriate security barriers and access controls.

b. A periodic risk assessment must be performed for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary.

c. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.

d. All information technology equipment and information media must be secured and concealed to the extent possible to prevent a compromise of confidentiality, integrity, or availability.

e. Visitors to information processing and storage facilities, including maintenance personnel, must be escorted at all times. Any maintenance performed remotely must be virtually escorted.

f. For SE information that has a High Confidentiality requirement, written procedures must be created and implemented to keep track of individual documents, files, devices, or media and the individuals who have possession of them.

Associated Standard: NYS-S14-001, Information Security Risk Management Standard

4.11 Account Management and Access Control

a. All accounts must have an individual employee or group assigned to be responsible for account management. This may be a combination of the business unit and information technology (IT) unit.

b. Except as described in the ITS Policy NYS-S14-013, Account Management/Access Control Standard, access to systems must be provided through the use of individually assigned, unique identifiers known as user-IDs.

c. Associated with each user-ID is an authentication token (e.g., password, key fob, biometric) which must be used to authenticate the identity of the person or system requesting access.

d. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.

e. Automated techniques and controls must be implemented to terminate a session after specific conditions are met as defined in NYS IT Policy NYS-S14-013, Account Management/Access Control Standard.

f. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.

g. Tokens must not be stored on paper, or in an electronic file, hand-held device, or browser, unless they can be stored securely and the method of storing (e.g., password vault) has been approved by the ISO/designated security representative.

h. Information owners are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (e.g., read, update, etc.).

i. Access privileges will be granted by the SE in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with SE missions and business functions (i.e., least privilege).

j. Users of privileged accounts must use a separate, non-privileged account when performing normal business transactions (e.g., accessing the Internet, e-mail).

k. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for SE business or other approved use consistent with SE policy, and that user activities may be monitored and the user should have no expectation of privacy.

l. Advance approval for any remote access connection must be provided by the SE. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved, and the contractual, process, and technical controls required for such connection to take place.

m. All remote connections must be made through managed points-of-entry reviewed by the ISO/designated security representative.

Working from a remote location must be authorized by SE management and practices which ensure the appropriate protection of SE data in remote environments must be shared with the individual prior to the individual being granted remote access. Working from international locations requires special legal, human resource, and security considerations and should only be allowed after careful SE analysis of these risks.

Associated Standards: NYS-S14-013, Account Management/Access Control Standard; NYS-S14-006, Authentication Tokens Standard; ; NYS-S20-001 Digital Identity Standard; NYS-S14-010 Remote Access Standard; NYS-S14-005, Security Logging Standard

4.12 Systems Security

a. Systems include but are not limited to servers, platforms, networks, communications, databases, and software applications.

1. An individual or group must be assigned responsibility for maintenance and administration of any system deployed on behalf of NYS. A list of assigned individuals or groups must be centrally maintained.
2. Information security must be considered at system inception and documented as part of the decision to create or modify a system.
3. All systems must be developed, maintained, and decommissioned in accordance with a secure system development lifecycle (SSDLC).
4. Each system must have a set of controls commensurate with the classification of any information that is stored on or passes through the system.

5. All system clocks must synchronize to a centralized reference time source set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources.
6. Environments and test plans must be established to validate the system works as intended prior to deployment in production.
7. Separation of environments (e.g., development, test, quality assurance, production) is required, either logically or physically, including separate environmental identifications (e.g., desktop background, labels).
8. Formal change control procedures for all systems must be developed, implemented, and enforced. At a minimum, any change that may affect the production environment and/or production data must be included.

    a. Databases and software (including in-house or third party developed and commercial off the shelf [COTS]):
        1. All software written for or deployed on SE systems must incorporate secure coding practices, to avoid the occurrence of common coding vulnerabilities and to be resilient to high-risk threats, before being deployed in production.
        2. Once test data is developed, it must be protected and controlled for the life of the testing in accordance with the classification of the data.
        3. Production data may be used for testing only if a business case is documented and approved in writing by the information owner and the following controls are applied:
            i. All information security measures, including but not limited to access controls, system configurations, and logging requirements for the production data are applied to the test environment and the data is deleted as soon as the testing is completed; or
            ii. sensitive data is masked or overwritten with fictional information.
        4. Where technically feasible, development software and tools must not be maintained on production systems.
        5. Where technically feasible, source code used to generate an application or software must not be stored on the production system running that application or software.
        6. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
        7. Privileged access to production systems by development staff must be restricted.
        8. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

b. Network Systems:

1. Connections between systems must be authorized by the executive management of all relevant SEs and protected by the implementation of appropriate controls.
2. All connections and their configurations must be documented and the documentation must be reviewed by the information owner and the ISO/designated security representative annually, at a minimum, to ensure:
    i. the business case for the connection is still valid and the connection is still required; and
    ii. the security controls in place (e.g., filters, rules, access control lists, etc.) are appropriate and functioning correctly.
3. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:
    i. Internet accessible systems and internal systems;
    ii. systems with high security categorizations (e.g., mission critical, systems containing PPSI) and other systems; and
    iii. user and server segments.
4. Network management must be performed from a secure, dedicated network.
5. Authentication is required for all users connecting to State internal systems.
6. Network authentication is required for all devices connecting to State internal networks.
7. Only SE authorized individuals or business units may capture or monitor network traffic.
8. A risk assessment must be performed in consultation with the SE ISO/designated security representative before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

Associated Standards: NYS-S13-001, Secure System Development Lifecycle Standard; NYS-S13-002, Secure Coding Standard; NYS-S14-005, Security Logging Standard; NYS-S14-008, Secure Configuration Management Standard

4.13 Collaborative Computing Devices

a. Collaborative computing devices must:

1. prohibit remote activation; and
2. provide users physically present at the devices with an explicit indication of use.

b. SEs must provide simple methods to physically disconnect collaborative computing devices.

4.14 Vulnerability Management

a. All systems must be scanned for vulnerabilities before being installed in production and periodically thereafter.

b. All systems are subject to periodic penetration testing.

c. Penetration tests are required periodically for all critical environments/systems.

d. Where a SE has outsourced a system to another SE or a third party, vulnerability scanning/penetration testing must be coordinated.

e. Vulnerability scanning/penetration testing and mitigation must be included in third party agreements.

f. The output of the vulnerability scans/penetration tests will be reviewed in a timely manner by the system owner. Copies of the scan report/penetration test must be shared with the ISO/designated security representative for the evaluation of risk.

g. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities. For any discovered vulnerability, a plan of action and milestones must be created, and updated accordingly, to document the planned remedial actions to mitigate vulnerabilities.

h. Any vulnerability scanning/penetration testing must be conducted by individuals who are authorized by the ISO/designated security representative. The CISO must be notified in advance of any such tests. Any other attempts to perform such vulnerability scanning/penetration testing will be deemed an unauthorized access attempt.

i. Anyone authorized to perform vulnerability scanning/penetration testing must have a formal process defined, tested and followed at all times to minimize the possibility of disruption.

Associated Standards: NYS-S15-001, Patch Management Standard; NYS-S15-002, Vulnerability Management Standard

4.15 Operations Security

a. All systems, and the physical facilities in which they are stored, must have documented operating instructions, management processes, and formal incident management procedures related to information security matters which define roles and responsibilities of affected individuals who operate or use them.

b. Any systems or services operated outside of CONUS must not connect to State networks or the State datacenter.

c. System configurations must follow approved configuration standards.

d. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.

e. Where a SE provides a server, application, or network service to another SE, operational and management responsibilities must be coordinated by all impacted SEs.

f. Host based firewalls must be installed and enabled on all SE workstations to protect from threats and to restrict access to only that which is needed.

g. Controls must be implemented (e.g., anti-virus, software integrity checkers, web filtering) across SE systems where technically feasible to prevent and detect the introduction of malicious code or other threats.

h. Controls must be implemented to disable automatic execution of content from removable media.

i. Controls must be implemented to limit storage of SE information to SE authorized locations.

j. Controls must be in place to allow only SE approved software to run on a system and prevent execution of all other software.

k. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.

l. All security patches must be reviewed, evaluated, and appropriately applied in a timely manner. This process must be automated, where technically possible.

m. Any system, software, or Operating System environment which is no longer supported and cannot be patched to current versions (e.g. end of life hardware/software) must be decommissioned and removed from service.

n. Systems and applications must be monitored and analyzed to detect deviation from the access control requirements outlined in this policy and the Security Logging Standard, and must record events to provide evidence and to reconstruct lost or damaged information.

o. Audit logs recording exceptions and other information security-relevant events must be produced, protected, and kept consistent with SE record retention schedules and requirements.

p. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic locations to monitor inbound, outbound, and internal network traffic.

q. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.

r. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly. At a minimum, these plans must include:

    1. An evaluation of the criticality of systems used in information processing (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).

    2. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.

s. Backup copies of SE information, software, and system images must be taken regularly in accordance with SE defined requirements.

t. Backups and restoration must be tested regularly. Separation of duties must be applied to these functions.

u. Procedures must be established to maintain information security during an adverse event. For those controls that cannot be maintained, compensatory controls must be in place.

Associated Standards: NYS-S14-008, Secure Configuration Management Standard; NYS-S14-005, Security Logging Standard; NYS-S13-005, Incident Response Standard; NYS-S14-013, Account Management/Access Control Standard

4.16 Citizens' Cyber Security Notification

a. All SEs are required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with State Technology Law, Article II, Internet Security and Privacy Act.

b. Beyond the requirements of the Act, SEs must also notify non-NYS residents when there has been or is reasonably believed to have been a compromise of the individual's private information.

c. This policy also applies to information maintained on behalf of an SE by a third party.

d. The SE must consult with the CISO to help determine the scope of the breach and restoration measures.

5.0 Compliance

This policy shall take effect upon publication. Compliance is required with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, SEs shall request an exception

through the CISO. Details regarding the exception process and the Exception Request Form can be found in ITS Policy, NYS-P13-001, Information Security Exception Policy.

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The SE will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-P03-002
NYS Office of Information Technology Services
1220 Washington Avenue, Bldg. 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This policy shall be reviewed at least once every two years to ensure relevancy.

Date	Description of Change	Reviewer
04/18/2003	Original Policy Release (*released under the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC)*)	CIO/OFT
06/20/2014	Full revision	Deborah A. Snyder, Acting Chief Information Security Officer
09/19/2014	Added annual reporting requirement to Compliance section	Deborah A. Snyder, Acting Chief Information Security Officer
10/17/2014	Added bullet to Systems Security section to require security consideration at system inception; re-worded bullet on secure coding	Deborah A. Snyder, Acting

Date	Description of Change	Reviewer
		Chief Information Security Officer
02/20/2015	Added Collaborative Computing Devices section and definitions for collaborative computing and explicit indication; added links to associated standards for Vulnerability Management section	Deborah A. Snyder, Deputy Chief Information Security Officer
06/19/2015	Added EISO responsibility to monitor external sources for indications of breach, defacements, etc., removed hardware tagging requirement, clarified requirement for incident response plan, added definition of critical infrastructure.	Deborah A. Snyder, Deputy Chief Information Security Officer
05/04/2016	Changed NYS Cyber Incident Response Team (CIRT) to Cyber Command Center and updated email in Section 7.0	Deborah A. Snyder, Deputy Chief Information Security Officer
02/15/20197	Update of contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
09/07/2018	Updated Authority, Scope, and title of office	Deborah A. Snyder, Chief Information Security Officer
09/20/2018	Corrected numbering in section 4.14	Deborah A. Snyder, Chief Information Security Officer
12/07/2018	Revised to clarify State Entity and workforce responsibilities to understand information security controls and to protect State information and resources, and personal, private, sensitive information, from unauthorized use or disclosure.	Deborah A. Snyder, Chief Information Security Officer
11/23/2021	Added language for CONUS and international work considerations, incorporated content from Security Controls standard, added Cyber Risk Coordinator description, and routine updates to remain consistent with other policy/standard changes.	Karen Sorady, Chief Information Security Officer

9.0 Related Documents

National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

International Standard ISO/IEC 27002, Information Technology – Security Techniques – Code of Practice for Information Security Controls

SANS Institute, Critical Security Controls for Effective Cyber Defense ("Top 20 Critical Security Controls")

State Technology Law, Article II, Internet Security and Privacy Act

Internal Revenue Service Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies

Exhibit 1

Cyber Risk Coordinator Description

As outlined in Section 4.1., SEs must designate an individual or group to be responsible for cyber-related risk management. The Cyber Risk Coordinator (CRC) is the SE-assigned individual who ensures that cyber-related risk is managed within an SE. Organizations can implement this role either as a function of a current role (e.g., counsel, internal controls, etc.), or by creating a new role. The CRC must understand the SE's strategic goals and objectives. This individual should be either authorized to or made able to facilitate risk-based decision making, working with executive leadership. Where cyber security is a shared responsibility between SEs and ITS, the SE is responsible for managing security requirements and risk, by performing and/or participating in the following functions:

- Identification of critical assets
- Data classification
- Account management and control of agency resources
- Incident response and management
- Employee awareness and training
- Developing requirements for systems that support business functions
- Preparation and review of agency policies and procedures
- Disaster Recovery & Business Continuity planning
- Routine assessments where the SE must play a lead role (e.g., annual Nationwide Cyber Security Review)