NYSTEC

YOUR INDEPENDENT TECHNOLOGY ADVISOR

Security:
Designed In
Not Bolted On

Cybersecurity Risk Assessment

Information Security Officer
Information Technology Department
Street Address
County, NY

Proposal No. NYSAC PXXXX
OGS Contract No. PN205XX

November 13, 2017

NYS SFS – New York State Technology Enterprise Corporation – Vendor ID 1000016166

500 Avery Lane
Rome, NY 13441
315.338.5818
www.nystec.com

Illustrative Proposal:

Cybersecurity Risk Assessment

Submitted to:
Information Technology Officer
Information Technology Department
Street Address
County, NY

Proposal Number NYSAC PXXXX
OGS Contract No. PN205##

November 13, 2017

NYSTEC CONTACT INFORMATION

Account Executive:

Bill Cunningham

Direct Line:	(518) 431-7020
Mobile Phone:	(518) 573-0074
Fax:	(518) 431-7037
Email:	bcunningham@nystec.com

Practice Leader:

Rob Zeglen

Direct Line:	(518) 431-7023
Mobile Phone:	(518) 368-4277
Fax:	(518) 431-7037
Email:	rzeglen@nystec.com

President & CEO:

Michael Walsh

Direct Line:	(518) 431-7027
Mobile Phone:	(518) 852-3406
Fax:	(518) 431-7037
Email:	mwalsh@nystec.com

Office Locations:

NYSTEC (Rome)
500 Avery Lane, Suite A
Rome, NY 13441

NYSTEC (Albany)
540 Broadway, 3rd Floor
Albany, NY 12207

NYSTEC (New York City)
27 West 24th Street, Suite 501
New York, NY 10010

NYSTEC Website URL: www.nystec.com
OGS Contract site: http://www.ogs.ny.gov/purchase/snt/awardnotes/7953622957can.HTM

NYS SFS - New York State Technology Enterprise Corporation - Vendor ID 1000016166

CONTENTS

1 EXECUTIVE SUMMARY

NYSTEC is pleased to submit this proposal to COUNTY to assist with a Cybersecurity Risk Assessment. New York State (NYS) counties are taking proactive steps to help ensure that their government operations are properly identifying cybersecurity risk and taking steps to mitigate it. We understand that NYS counties are being asked to align with the NYS Technology Law to be compliant with cybersecurity standards. This will help ensure that the counties have a solid cybersecurity posture through alignment with National Institute of Standards and Technology Special Publications (NIST SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, which has become a standard in the industry and New York State.

This effort will focus on the recently established Center of Internet Security (CIS) Top 20 Controls. These 20 control families are quickly becoming the baseline and starting point for cybersecurity risk assessments as they represent critical controls that can mitigate a significant number of cybersecurity-related risks to county data and services. NYSTEC is already very familiar with the CIS Top 20, which has been woven into our existing NIST SP 800-53-based Cybersecurity Risk Assessment process.

Figure 1, CIS Top 20 Controls

At NYSTEC, our philosophy is that security must be designed in, not bolted on. Security cannot be an afterthought. It must be an integral and evolving cultural fabric that protects the county across via many layers of controls. It must be fundamental in project planning and to the ongoing processes and practices of any technology-oriented county. To be responsive to evolving threats, security should be a continuous effort encompassing policy, process, procedure, education, technical controls, monitoring, and enforcement.

NYSTEC is uniquely qualified to support risk assessments across NYS counties. Our well-qualified team has completed numerous risk assessments within government as well as the private sector. We understand the goals, timing, criticality, and scope of these risk assessments as they encompass counties that provide critical services within New York State. We bring experience, strong references, skills, and a standards-based methodology that has been developed through our experience with conducting risk assessments for New York State.

As a trusted advisor, we bring the following strengths to all of our Cybersecurity Risk Assessments:

- Our cybersecurity consultants have significant experience conducting risk assessments for NYS organizations, including:
    - NYS Office of Mental Health
    - NYS Department of Health
    - NYS Office of the State Comptroller
    - NYS Office of the Attorney General
    - NYS Department of Tax and Finance
    - NYS cloud vendors
- Our approach and methodologies align with NIST SP 800-30 and focus on the CIS Top 20 Controls baseline.
- Our Cybersecurity Risk Assessment program includes tailored site visits as well as efficient online tools, WebEx meetings, and videoconferencing consultations that give you a high-quality, reliable, tailored customer experience in a cost-effective and efficient way.
- Our final Cybersecurity Risk Assessment reports are actionable and easy to understand.
- Our consultants average more than 20 years of experience in the Information Technology (IT) and security fields. They typically have advanced degrees, required certifications such as Certified Information Systems Security Professional (CISSP) and other leading security credentials, and extensive experience with NYS entities.

- We use local resources, including the Air Force Research Laboratory (AFRL) and vetted M/WBE certified partners.
- Our work with the federal Centers for Medicare & Medicaid Services (CMS) has kept us abreast of what other states are doing with regard to alignment with NIST SP 800-53. We have touch points with California and New Hampshire, and we remain familiar with national efforts concerning risk assessments through consultant training.
- As an independent, not-for-profit technology consulting company, we do not contract with other vendors that provide hardware or software solutions. We know many of the leading security software, solution, and service companies, but we do not accept any software or service-related commissions from these vendors. As your trusted advisor, we will give you an objective analysis. We work for *you*.

Balancing security and business needs is often a difficult task. However, the execution of a cybersecurity risk assessment is an excellent way to focus remediation efforts on the most critical areas. NYSTEC is excited and pleased to present an approach that we believe will meet the stated goals in a manner that is both efficient and appropriate for your county's size and IT presence.

Understanding that counties differ in size and complexity, we have provided a three-tiered approach for the cybersecurity risk assessments. NYSTEC fully understands that every county is different and as such, the classifications provided in Section 4 serve as a guideline.

- **Small.** Designed for small counties that have few critical assets or a small cyber presence. The risk assessment begins with an easy-to-complete online self-assessment, a discovery phase consisting of video consultations, and an organizational artifact review. NYSTEC will deliver a draft Risk Assessment and Mitigation Strategy report and the opportunity to ask questions and receive clarification before the assessment is finalized. The report includes vulnerability scanning.
- **Medium**. Designed for medium-sized counties with critical assets and a significant cyber footprint. This risk assessment consists of hybrid activities for data gathering including interviews, online self-assessments, and a review of documentation artifacts. During this risk discovery phase, the fact finding consists of a mix on in-person consultants, video conferencing consultations, and secure artifact reviews with limited vulnerability scanning. NYSTEC will deliver a draft Risk Assessment, Vulnerability Scan Results, and Mitigation Strategy Report and you will have the opportunity to ask questions and receive clarification before your assessment is finalized.
- **Large.** Designed for larger counties with significant cyber assets and a large footprint. This risk assessment utilizes interviews, hands-on observation, artifact reviews, and vulnerability scanning. We offer several site visits and in-person progress meetings over the course of the engagement. NYSTEC will deliver a draft Risk Assessment, Vulnerability Scan Results, and Mitigation Strategy Report and you will have the opportunity to ask questions and receive clarification before your assessment is finalized.

Details of each offering are described in Section 4.

2 STATEMENT OF WORK

2.1 TASK: EXECUTE CYBERSECURITY RISK ASSESSMENT

The basis for this task will be NYSTEC's Risk Assessment and Management methodology, which aligns with NIST SP 800-30, Risk Management Guide for Information Technology Systems and the CIS Top 20 Controls approach. As part of this assessment, NYSTEC will focus the vulnerability and control-identification phases on those NIST SP 800-53 controls that we have mapped to the CIS Top 20. These will serve as a baseline for security controls that may or may not be present across the systems under review.

In this task, NYSTEC will use a variety of methods to collect information and review material related to the systems and controls that are within scope of the assessment. Typically, throughout the larger assessments, NYSTEC will seek to observe and document evidence that security controls are in place and operating properly. For smaller-scoped assessments, we will rely largely on self-reporting.

In the execution of this task, NYSTEC will work with designated county representatives to complete the online surveys and participate in interviews related to completion of the prepared CIS Top 20 Security Controls Assessment Worksheets. The worksheets will focus on the critical data, systems, and services provided by the county and this will be assured by the NYSTEC consultant or consultants assigned to that county as part of the system characterization phase.

An outline of how NYSTEC will execute the steps within this methodology is seen in Figure 2 (on the following page). Descriptions of these steps follow.

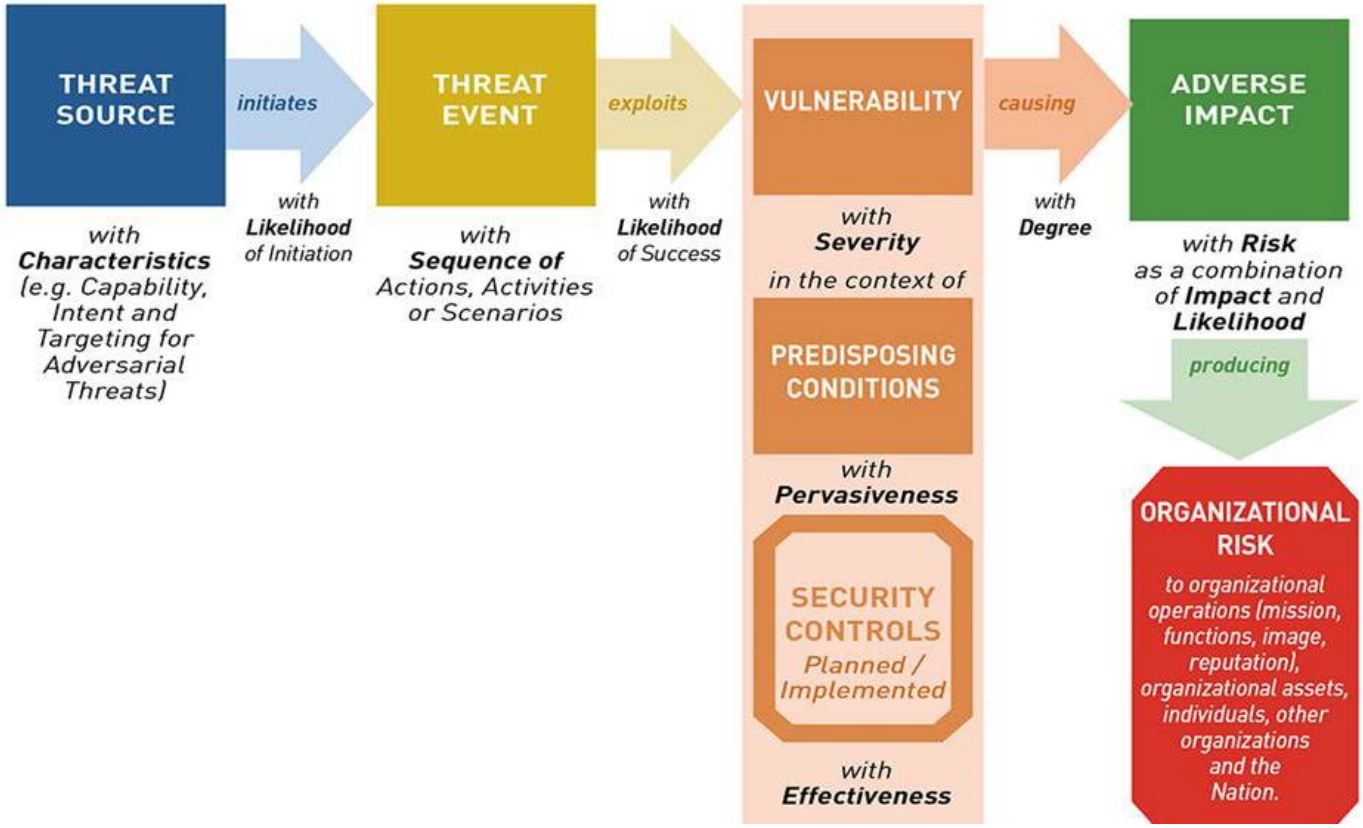

Figure 2, NIST SP 800-30 Risk Assessment Framework

SYSTEM CHARACTERIZATION

In this first step, the information systems under review, boundaries, and county business processes will be identified to characterize the environment and identify critical assets. It will be necessary to identify those places where sensitive information is created, received, maintained, stored, processed, or transmitted.

NYSTEC will provide asset inventory templates to be completed by county staff, or the county can provide the required information with existing documentation. Interviews, artifact reviews, and documentation reviews will be executed to verify the characterization and to discover any new areas where sensitive data is maintained or processed.

THREAT IDENTIFICATION

This step (often performed in parallel with Vulnerability Identification, below) will identify the potential realistic threat sources that exist for the county and are relevant to the assets under

review. The list of potential realistic threats will be determined for each of the sensitive information sources identified in the System Characterization step.

In the Threat Identification step, NYSTEC will largely consider industry standard threats, as well as threats that may be specific to the county. This step considers common adversarial as well as non-adversarial threat sources.

INFORMATION GATHERING

This step includes all of the surveys and interviews (via WebEx and in person) with key county stakeholders including business managers and technical staff as well as reviews of documentation relating to information security controls and assets. NYSTEC will (under non-disclosure agreement) seek to review all relevant network diagrams, security plans, test plans, prior assessment results, and any other system-related documentation, including policies, procedures, and standards.

VULNERABILITY IDENTIFICATION

Potential threat sources identified in the previous step could exploit vulnerabilities across the county. NYSTEC will utilize, based on the level of assessment, a variety of methods to determine vulnerabilities that include but are not limited to:

- Interviews and self-assessment templates
- CIS Top 20 compliance workbooks
- Vulnerability scanning results
- Web application scanning results
- Firewall rule network device vulnerability analysis results
- Direct observation
- County-provided artifacts (prior assessments, scan results, etc.)

This step will identify and consider vulnerabilities that could enable a threat source and will typically form the basis for remediation recommendations.

CONTROL ANALYSIS

Vulnerabilities are typically the result of lack of a control. Here, NYSTEC will, through surveys, interviews, and documentation, determine what controls have been implemented to mitigate the risk of threat agents acting on vulnerabilities. NYSTEC will use a Security Controls Assessment Worksheet to document control status. When possible, NYSTEC will seek artifacts to validate controls; however, testing for control existence and effectiveness is out of scope for these assessments.

LIKELIHOOD DETERMINATION

In this step, an analysis will be completed to determine the likelihood of the realistic threat sources exploiting a vulnerability that could affect the county.

IMPACT ANALYSIS

This Impact Analysis step will determine the effect (reputational damage, financial loss, loss of productivity, legal impact, etc.) and likelihood of a threat agent successfully exploiting vulnerabilities to compromise confidentiality, integrity, accountability, or availability of county systems. The basis for the classification will be determined through interviews with county stakeholders.

RISK DETERMINATION

Using the information gathered from the previous steps, the Risk Determination step will seek to determine the level of residual risk for the county systems being analyzed. A risk-level matrix will be created to illustrate the relative effect and probability of risks resulting from threats and vulnerabilities. Risk descriptions will identify related NIST control families and risk category (i.e., People, Process, Technology, or a combination).

CONTROL RECOMMENDATIONS

In this step, controls will be recommended to reduce risks to levels acceptable to the county.

2.2 TASK DELIVERABLES

- **Risk Assessment Report.** Report in Microsoft Word that provides the documented results of the risk assessments and includes a heat map (see Figure 3, next page) for the county against the CIS Top 20 criteria as well as risk mitigation recommendations for each identified risk. Examples of this report are included in Appendix C.
- **Risk Assessment Workbook.** Excerpts from workbooks in PDF as needed to explain findings and document how risk levels were achieved.

CONTROL	CONTROL DESCRIPTION	EXPLANATION %	ARTIFACTS %
CSC 1	Inventory of Authorized and Unauthorized Devices	80	75
CSC 2	Inventory of Authorized and Unauthorized Software	73	67
CSC3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	69	57
CSC 4	Continuous Vulnerability Assessment and Remediation	87	83
CSC 5	Controlled Use of Administrative Privileges	60	25
CSC 6	Maintenance, Monitoring and Analysis of Audit Logs	63	55
CSC 7	Email and Web Browser Protections	69	57
CSC 8	Malware Defenses	60	40
CSC 9	Limitation and Control of Network Ports and Protocols	20	0
CSC 10	Data Recovery Capability	100	60
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers and Switches	66	38
CSC 12	Boundary Defense	73	48
CSC 13	Data Protection	76	40
CSC 14	Controlled Access Based on the Need to Know	80	40
CSC 15	Wireless Access Control	92	60
CSC 16	Account Monitoring and Control	57	30
CSC 17	Security Skills Assessment and Appropriate Training	20	0
CSC 18	Application Software Security	4	0
CSC 19	Incident Response and Management	31	14
CSC 20	Penetration Tests and Red Team Exercises	73	67
	AVERAGE SCORES	63	43

Figure 3, Sample Risk Assessment Heat Map

3 CONTRACT PROCESS

NYSTEC was awarded an easy-to-use OGS centralized contract that allows counties to contract directly with NYSTEC for services such as those in this illustrative proposal.

The NYSTEC OGS contract (OGS Contract PN20500) may be found here: http://www.ogs.ny.gov/purchase/snt/awardnotes/7953622957can.HTM

NYSTEC anticipates that each engagement will be through a separate contract with the requesting county. The easy-to-use process, as defined in OGS Contract PN20500, is as follows:

- Contact Bill Cunningham (518-431-7020) at NYSTEC to schedule a meeting.
  - NYSTEC and our subject matter experts will work with you to clarify expectations regarding the specific scope and desired outcomes for the project.
  - NYSTEC will develop a Statement of Work, at no cost to you, which will identify the steps, resources, and timing to accomplish the proposed project.
  - NYSTEC will develop a cost proposal in accordance with the Cybersecurity Risk Assessment offerings defined in this proposal.
    - If additional NYSTEC services are requested to supplement the tiered offerings contained in this proposal, NYSTEC will work to define those additional services in accordance with OGS Contract PN20500 and our most favored rates: http://www.ogs.ny.gov/purchase/snt/awardnotes/7953622957can.HTM
- Review NYSTEC's proposed Statement of Work and collaborate with NYSTEC to make any necessary refinements.
- Request a final Statement of Work.
- Obtain internal county approval.
- Approve any necessary purchase order(s).
- NYSTEC begins work immediately.

The process can take only weeks from the initial contact to the start of work.

4 SERVICES

Service Component/Offering	Small @ $25,000	Medium @ $50,000	Large @ $100,000
Description	*For small counties that have few critical assets or a small cyber presence*	*For medium-sized counties with critical assets and a significant cyber footprint*	*For larger counties with significant cyber assets and a large footprint*
Self-assessment surveys	Yes	Yes	Yes
CIS Top 20 gap-assessment worksheets	Yes	Yes	Yes
Project kickoff meeting	WebEx	WebEx	On site
Phone interviews	Up to three two-hour phone/web conference interviews	As needed up to three two-hour phone/web conference interviews to supplement in person interviews	As needed up to six two-hour phone/web conference interviews to supplement in person interviews
In-person interviews	No	As needed up to three two-hour meetings	Up to six two-hour meetings
System characterization of critical assets	Organizational level	System level, up to three representative critical systems	System level, up to six representative critical systems
Review of documentation at the policy/ procedure level	Yes	Yes	Yes
Review of security maturity-related documentation and artifacts	No	As needed	Yes
Completion of NYSTEC Risk Assessment Matrix worksheet (heat map)	Yes	Yes	Yes
Review of completed Risk Assessment matrix with client for validation	No	Yes	Yes
Network device vulnerability analysis against known issues (unauthenticated)	Yes	Yes	Yes
Vulnerability scanning of internet facing assets	Up to 25 external IP addresses	Up to 50 external IP addresses	Up to 100 external IP addresses
Vulnerability scanning of internal assets	No	Up to 100 internal representative IP addresses	Up to 250 internal representative IP addresses
Web application scanning (unauthenticated)	No	Up to five URLs, three levels, 25 pages	Up to 15 URLs, three levels, 75 pages

APPENDIX A: REDACTED NYSTEC CYBERSECURITY RISK ASSESSMENT SAMPLE REPORTS

CIS Top 20 Heat Map. Included in each report across all three assessment levels will be a heat map diagram that will identify county compliance with the CIS Top 20. This diagram serves to identify an overall view of the completeness and maturity of security controls representing the CIS Top 20 Controls. Those areas in the orange-to-red colors will typically result in identified risks.

CONTROL	CONTROL DESCRIPTION	EXPLANATION %	ARTIFACTS %
CSC 1	Inventory of Authorized and Unauthorized Devices	80	75
CSC 2	Inventory of Authorized and Unauthorized Software	73	67
CSC3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	69	57
CSC 4	Continuous Vulnerability Assessment and Remediation	87	83
CSC 5	Controlled Use of Administrative Privileges	60	25
CSC 6	Maintenance, Monitoring and Analysis of Audit Logs	63	55
CSC 7	Email and Web Browser Protections	69	57
CSC 8	Malware Defenses	60	40
CSC 9	Limitation and Control of Network Ports and Protocols	20	0
CSC 10	Data Recovery Capability	100	60
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers and Switches	66	38
CSC 12	Boundary Defense	73	48
CSC 13	Data Protection	76	40
CSC 14	Controlled Access Based on the Need to Know	80	40
CSC 15	Wireless Access Control	92	60
CSC 16	Account Monitoring and Control	57	30
CSC 17	Security Skills Assessment and Appropriate Training	20	0
CSC 18	Application Software Security	4	0
CSC 19	Incident Response and Management	31	14
CSC 20	Penetration Tests and Red Team Exercises	73	67
	AVERAGE SCORES	63	43

CIS Top 20 Control Level Reporting. Colors in the heat map are explained in an alternative representation.

Function ID	Category Unique ID	CIS Top 20 Controls	Overall	**Fully Compliant (5).** This activity is fully documented, implemented and reviewed on a regular basis. Compliance is tested for on a regular basis.	**Mostly Compliant.(4)** The activity may not be fully documented, but is implemented and compliance is tested/reviewed on a regular basis.	**Partially Compliant(3).** Compliance only partially documented and tested/reviewed.	**Minimally Compliant(2).** Compliance is limited to a minimal number of areas and there is no testing or review.	**Non-Compliant (1)** Activity is not performed
ID	CIS.1	Inventory of Authorized & Unauthorized Devices	1					x
	CIS.2	Inventory of Authorized & Unauthorized Software	3					x
	CIS.3	Secure Configurations for Hardware and Software	3			x		
	CIS.4	Continuous Vulnerability Assessment & Remediation	4		x			
	CIS.5	Controlled Use of Administrative Privilages	2				x	
	CIS.6	Maintenance, Monitoring, & Analysis of Audit Logs	2					x

Risk Overview. Each report will contain a high-level chart of discovered risks by severity.

Figure 2 Risk Assessment Results

Risk Report Summary. Each risk will also be documented as in the example below. The Risk Identifier is linked to a detailed assessment process that aligns with NIST SP 800-30 and is shown below. Each Risk Identifier can be mapped in the detailed matrix to ensure clarity and transparency on how the score was determined.

The example below is from a New York State agency.

Lack of an Active <Agency Name> Incident Response Program Leads to Increased Impact and Risk

Attribute	Score	Risk Summary
Risk Identifier	Adv-26	Because it is impossible to prevent all breaches, organizations must be prepared to handle breaches with a documented and rehearsed incident response plan. When a breach happens, a lack of or improper response can increase the impact of the breach and result in an increased chance that <Agency Name> will be subject to an audit and possible fines.
Likelihood	High	
Impact	Very High	
Risk Score	High	
Recommendations		
<Agency Name> should consider implementing the following control(s): • Immediately review the <Agency Name> Incident Response Procedures and implement them across the organization. • Include incident response as part of regular awareness training. • Implement a dry run of the incident response procedures on a yearly basis. • Institute an active auditing capability to monitor all logs.		

Risk Assessment Methodology. The screen shots below and on the following pages visualize the type of data elements that NYSTEC uses to capture all elements that compromise a resulting risk. They are presented here in tabular format but may also exist within our Risk Assessment software solution.

The example, from a New York State agency, represents a typical threat scenario and the resulting risk to the organization.

	Non-Adversarial Threat					
ID	Threat Source	Threat Event Scenario	Threat Information Source	Threat Source Taxonomy	Range of Effects	Relevance
NAdv-XX	Title Field	Bibliography TAB	Table V-1	Table D2	Table D-6	Table E4
NAdv-01	Environmental	Severe natural weather occurrences, failure of an industrial control system such as central air conditioning or lighting, or some other event, like the flu.	Published Industry Expertise	Environmental	Moderate	Anticipated

	Likelihood					
ID	**Threat Source**	**Likelihood of Threat or Attack Event Initiation**	**Principal Control for Risk** (Select from CONTROLS Tab)	**Likelihood that Event Would Result in Adverse Impact**	**Rationale for Selected Likelihood Values** (List any sources in BIBLIOGRAPHY tab, as necessary)	**Overall Likelihood** G5 f(G3,G4)
NAdv-XX	**Title Field**	Table G3	Controls TAB	Table G4	Bibliography TAB	Table G5
NAdv-01	Environmental	Low	C-01: CP - Agency DR Site.	Moderate	Severe natural weather occurrences, failure of an industrial control system such as central air conditioning or lighting, or an outbreak of flu or disease may threaten the safety of employees or reduce the staff's ability to conduct business at agency facilities, causing delays or outages to production operations, at these sites.	Low

	Vulnerability					
ID	**Threat Source**	**Vulnerability** (Select from VULNERABILITIES tab)	**Vulnerability Severity** [Populated automatically from VULNERABILITIES tab]	**Predisposing Condition** (Select from PREDISPCOND tab)	**Pervasiveness of Predisposing Condition** [Populated automatically from PREDISPCOND tab]	**Relevance**
NAdv-XX	**Title Field**	Vulnerabilities TAB	Table F-2	Predisp Cond TAB	Table F-5	Table E4
NAdv-01	Environmental	V-03: Outdated and undocumented back-up procedures. V-05: BC/DR procedures may not exist and DR testing is not performed.	Moderate	PC-11: Agency policies do not address incident response.	Moderate	Anticipated

	Impact			
ID	Threat Source	Description of what happens if Attack Succeeds / Adverse Impacts Occur	Type of Impact	Level of Adverse Impact
NAdv-XX	Title Field	Comment Field	Table H2	Table H3
NAdv-01	Environmental	Reduced ability to serve its clients	Harm to operations	Moderate

		Risk			Recommended Actions	Notes
ID	Threat Source	Risk I-2 f(G5, H3)	Risk Name Title to be used on the final report for the associated risk row	Risk Summary Description of the entire row, to be placed in the final report in the 'Risk Summary' box for the associated risk.	Recommended Actions Describe the recommended approach to mitigating the risk	
NAdv-XX	Title Field	Table I-2				
NAdv-01	Environmental	Low	Occupational and Situational Threats	Severe natural weather occurrences, failure of an industrial control system such as central air conditioning or lighting, or an outbreak of flu or disease may threaten the safety of employees or reduce the staff's ability to conduct business at agency facilities, causing delays or outages to production operations, at these sites.	Consider implementing the following control(s): - Ensure that facilities exist to house information workers during disaster events. - Create disaster recovery plans that include relocating workers, as needed. - Perform adequate table-top and physical testing of plans on an annual basis.	

APPENDIX B: NYSTEC BACKGROUND

NYSTEC is a not-for-profit corporation based in Rome, New York, with offices in Albany and New York City. We serve as a trusted advisor to entities needing assistance with IT strategy, technology acquisition, information security, converged networks, health IT, and education IT. Among other services, we perform technology needs analyses; assist clients with requirements development and the generation of Requests for Proposals (RFPs) or other solicitation instruments; help evaluate technology solutions and vendor proposals; provide a wide range of consulting services for converged networks, health IT, and education IT; conduct security evaluations of client networks and infrastructure; and make recommendations for technology improvements.

NYSTEC was incorporated in 1996 to help leverage technologies and expertise from the Air Force Research Laboratory (AFRL) in Rome to benefit government entities and businesses statewide. Following successful projects with New York State government, NYSTEC evolved into a trusted technology advisor to both government and the private sector. We continue to tap AFRL expertise, processes, and technology on client projects.

The professionals of NYSTEC have exceptional experience in the areas of network design, business analysis, information security, systems planning, systems acquisition, integration, testing, and quality assurance. These methodologies have been developed in conjunction with the AFRL, and NYSTEC professionals continue to collaborate on these methodologies and techniques with the AFRL. This will afford counties access to the specified resources per NYSTEC's enabling legislation.

Our professionals are certified in more than 35 technology disciplines. In addition to Air Force standards and practices, NYSTEC's methodologies incorporate the Project Management Institute's Project Management Body of Knowledge (PMBOK), the International Institute of Business Analysis' Business Analysis Body of Knowledge (BABOK), the Capability Maturity Model Integration (CMMI) for Systems Engineering and Software Engineering, the Software Development Life Cycle (SDLC) methodology, and many other proven standards and best practices.

NYSTEC's not-for-profit business model, combined with our experience in evaluating and deploying large, complex IT solutions, enables us to deliver strategies, on demand, tailored for both the client and the project scope of work. Counties will benefit from our vendor-neutral IT guidance, which has enabled numerous clients to acquire and implement technically optimized, cost-effective solutions.

NYSTEC was awarded an easy-to-use OGS centralized contract that allows counties to contract directly with NYSTEC for services such as those in this illustrative proposal.

APPENDIX C: NYSTEC QUALIFICATIONS

B.1 INTRODUCTION

Since 1999, NYSTEC has provided a wide variety of information security services to clients in the public and private sectors. To address the identification of specific security projects in this proposal, we have included NYSTEC security engagements over the past 10 years, primarily those projects that focused exclusively on security.

In the Related Project Experience Section of this Appendix (B.2), we describe 15 recent projects in which we performed IT risk assessments for various clients, many of which were NYS entities. Over the past decade, we have participated in nearly 60 consulting engagements in which information or network security was the primary or sole focus of the client project. More than 80% of our client engagements that focused exclusively on security were conducted for large New York State agencies.

In addition, we have served clients on many dozens of other projects in which information or network security was a component of a more comprehensive consulting engagement. In many cases, assessing risks was the primary focus.

NYSTEC is a New York State business:

- Founded in April 1995, we officially filed with the New York State Department of State as a domestic not-for-profit corporation in October 1996.
- We are an independent company based in Rome, New York, with offices in Albany and New York City.

NYSTEC is an IT business:

- We help clients plan and manage the acquisition, implementation, and security of IT systems.
- Applying proven processes for project management and system integration, we bring engineering discipline to the formidable undertaking of developing or enhancing a technology system.

NYSTEC is focused on information security:

- Most of our information security professionals are Certified Information Systems Security Professionals (CISSPs). Those who are not CISSPs hold other equivalent certifications.
- Our standard risk-assessment methodology is based largely on the National Institute of Standards and Technology (NIST) Special Publications 800-30 Guide for Conducting Risk Assessments and the NIST SP 800-53 Recommended Security Controls for Federal

Information Systems. The 800-53 Recommended Security Controls provide an industry-accepted standard for security controls that we use as a foundation for assessments.

Our past cybersecurity risk assessment projects are many and varied, but they have typically required an analysis of the client's hardware, network, and applications; existing and potential vulnerabilities; mitigation options and costs; and the potential effects of threat agents acting on vulnerabilities. We are also experienced at using surveys and interviews with key stakeholders and documentation examinations as key steps in performing our risk assessments.

B.2 RELATED PROJECT EXPERIENCE

NYSTEC provides a broad spectrum of security testing and cybersecurity risk-analysis services that are generally tailored to the client's specific environment and requirements. Often, NYSTEC recommends the completion of a new risk assessment or review of an existing risk assessment prior to any testing activities to make sure that the testing targets systems and data that pose the greatest risk to the client.

NYSTEC has experience in performing the following types of security testing and evaluation services:

- Security program evaluations against industry standards
- Data classification
- General network and system vulnerability scanning
- General and application-specific penetration testing
- Technology-specific testing (i.e., wireless radio systems and electronic voting systems)
- Network, router, Intrusion Detection System (IDS) and firewall security analysis
- Wireless network assessments
- Business continuity and disaster recovery readiness assessments

NYSTEC subscribes to industry accepted best practices in security assessments (i.e., program review, risk analysis, and vulnerability testing), as espoused in the following documents:

- ISO/IEC 27001 Information Security Standard
- NIST SP 800-30 Risk Management Guide
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
- Open Web Application Security Project's (OWASP's) Testing Guide v3.0

These documents serve, in part, as NYSTEC's foundation for planning and conducting technical information-security testing and assessments, analyzing findings, and developing mitigation strategies.

In addition to industry best practices, we leverage our independence to perform security testing that is completely unbiased and client focused. Our experience enables us to be efficient when conducting analysis and reporting to translate technical findings into actionable recommendations for risk mitigation that will improve the client's security posture.

APPENDIX D: NYSTEC SECURITY TEAM BRIEF BIOS

Rob Zeglen leads the NYSTEC Security Practice. A Certified Information Security Systems Professional (CISSP), Rob is an information security principal consultant with more than 22 years of IT experience. His knowledge and skills include identity and access management, systems programming, performance computing, systems administration, information security architectures, web security, risk analysis, and security compliance and training.

Bruce Barnett is an information security consultant who assists clients with vulnerability testing and analysis. Bruce is knowledgeable in multiple technology areas, including security technologies, programming languages, numerous operating systems, networking and wireless systems and solutions, and system-administration platforms.

Todd Brasel is an information security principal consultant with 20 years of experience at technology companies ranging from startups to Fortune 400 organizations. He is a PMI-certified Project Manager, Lean Six Sigma Green Belt, Certified Scrum Master, and Systems Security Certified Practitioner (SSCP); he is also a certified Java Programmer, specializing in the areas of performance and security.

Jonas DiSorbo is an information security senior consultant with more than 16 years of experience with government information assurance and security, including administration and monitoring of networks and systems, vulnerability assessments, intrusion detection, and intelligence analysis. A Certified Information Security Systems Professional (CISSP), he is also trained or certified in seven other security disciplines.

Nicole Dombroski is an information security senior consultant. Previously, she served as a program lead with the company's Healthcare Technology Adoption Practice, assisting with subject-matter support, program operations, stakeholder outreach, educational development, workgroup development, data analysis, quality management, federal reporting requirements, process documentation, and process re-engineering.

Nils Ekberg is an information security principal consultant with more than 40 years of IT experience. His background includes 20-plus years in IT security and more than 25 years developing and managing IT organizations for a large international corporation. Nils, who has extensive experience in leading user groups, has delivered presentations at conferences around the world.

Mary Jeanne Gagan is an information security consultant with more than 20 years of experience in the computer science field. MJ's areas of concentration are in client server development and database relational design. She is well versed in the full project life cycle, from initial business analysis through implementation.

Mark Hammond is an information security consultant who joined NYSTEC after a distinguished 31-year career with New York State government. Through his extensive managerial experience and knowledge of IT systems, Mark has acquired strong analytical and problem-solving skills emphasizing root-cause discovery.

Vince Hannon is an information security principal consultant with more than 20 years of experience in IT. Vince's broad experience includes many areas of information security, ranging from network and application security architecture to risk analysis to incident response and investigation. He is a Certified Information Security Manager (CISM), Information Systems Audit and Control Association (ISACA), and a Six Sigma Green Belt.

Alan Kowlowitz is an information security consultant with more than 30 years of IT experience. He was the primary author of New York State's original Identity Trust Model. A Government Fellow with the Center for Technology in Government, Alan is a Certified Information Security Manager. He holds an ITIL Foundation Certificate in IT Service Management as well as an ITIL Practitioner's Certificate in IT Service Management – Security Management.

Yakov Leonov is an information security consultant with five years of experience providing a variety of technical services, including networking and configuration; data analysis; hardware repair, support and troubleshooting; and website development. Previously, he was the senior vice president for entertainment company Rhythm In Motion.

Slaw Marcinkowski is an information security principal consultant with more than 15 years of experience. He focuses on the information security aspects of projects, including the performance of vulnerability assessments and policy development. His certifications include Certified Information Systems Security Professional (CISSP), Global Information Assurance Certification (GIAC) Systems and Network Auditor (GSNA), GIAC Security Essentials, and GIAC Assessing Wireless Networks (GAWN).

John Mounteer is an information security principal consultant with more than 25 years of experience in diverse areas of information technology. He is a Cisco Certified Network Associate (CCNA) and Design Associate (CCDA), a Checkpoint Certified Security Administrator (CCSA), and a Convergence Technologies Professional (CTP), and he holds a Global Information Assurance Certification (GIAC) in Security Essentials.

Sean Murray is an information security principal consultant with more than 15 years of experience across a broad range of information security-related areas. He has worked in virtually all aspects of assessing and implementing network and application security and is accomplished at building security into the design, specification, coding, and documentation of software applications. Sean is a Certified Information Systems Security Professional (CISSP).

Beth Pritchett is an information security consultant with more than ten years of experience in legal compliance and litigation review. Previously, Beth worked as a senior client manager for high-profile litigation and multi-state litigation projects.

Paul Romeo, an information security senior consultant, has more than eight years of experience in various information security roles and an additional eight years of experience as an IT technician. Paul is a Certified Information Systems Auditor and a Certified Ethical Hacker, and he holds a Global Information Assurance Certification (GIAC) Security Essentials Certification.

Ron Stamp is an information security consultant with 23 years as manager of IT Systems with the New York State Department of Health (NYSDOH). Previously, Ron spent eight years developing and implementing circuit-board technologies in manufacturing environments to enhance production, testing, and repairs.

Michele Warner is an information security senior consultant with more than three years of experience in IT, focusing on quality assurance. Previously, she served in the company's Healthcare IT Practice. Before joining NYSTEC, she was a quality assurance analyst, a client manager, and an attorney.

Randy Wheeler is an information security senior consultant with 27 years of experience. He received the 2015 Superior Service Award from NYS Office of the Attorney General and is a past recipient of the NYS Digital Government Outstanding IT Service & Support Award and the NYS CIO Academy's Outstanding IT Manager Award.

Jeff Wilson is an information security principal consultant. He has nearly 30 years of IT experience, most recently serving for three years as Albany Medical Center's director of information services, during which he planned and oversaw comprehensive improvements to cybersecurity processes and systems. Jeff is a Certified Information Systems Security Professional (CISSP).