

KATHY HOCHUL  
Governor



ADRIENNE A. HARRIS  
Superintendent

*Electronically Submitted Via Email*

June 13, 2024

[REDACTED]  
President  
[REDACTED]

Re: Information Technology – Cybersecurity Examination

Dear Registrant:

Institution Number:

Pursuant to Section 596 of the New York Banking Law, the New York State Department of Financial Services (the “Department”) will commence a Limited Scope Examination of your institution. Our examination will focus on your institution’s policies, procedures and controls designed to safeguard confidential borrower information, including Information Technology infrastructure, Cybersecurity practices and enterprise-wide risk assessment. The examination will cover the period April 1, 2020, through December 31, 2023.

To facilitate our limited scope examination, the Department request that you submit the information detailed on Appendix A through the Department’s secured Portal (mySend) no later than July 5, 2024. For Access to the examination component of the Department’s secured Portal, email [Ninad.Shah@dfs.ny.gov](mailto:Ninad.Shah@dfs.ny.gov) and provide Ninad Shah with the name and email address of the individual who will be responsible for uploading the requested documents and data.

Kindly note, each question detailed on Appendix A requires a response. If the question is not applicable to your institution, respond by stating “none or NA.” To eliminate potential confusion, please cross-reference your response to the appropriate questions.

Additionally, an original signature of the Attestation must be mailed to the Department no later than June 21, 2024.

Should you have any questions regarding Appendix A or the pending limited scope contact the undersigned at [helen.hodge.dfs.ny.gov](mailto:helen.hodge.dfs.ny.gov). In my absence, please contact Karim Thomas at [karim.thomas@dfs.ny.gov](mailto:karim.thomas@dfs.ny.gov).

Very truly yours,

/s/

Helen Hodge  
Assistant Deputy Superintendent

Enclosure

Institution Name: \_\_\_\_\_  
Institution No.: \_\_\_\_\_

Date:

---

**EXAMINATION AFFIDAVIT**

---

STATE OF,

COUNTY OF,

In connection with the examination of \_\_\_\_\_

I, \_\_\_\_\_, being duly sworn depose and say:

That I am the owner or authorized principal officer of the above name registered \_\_\_\_\_ I complied with all the information in response to Attachment A and attest that the information provided there in is accurate.

\_\_\_\_\_

Subscribed and sworn to before me this

\_\_\_\_\_ day of

at

\_\_\_\_\_  
Examiner duly appointed

by the **Superintendent of the New York State Department of Financial Services**  
to examine the above-named \_\_\_\_\_

---

## SECTION F – INFORMATION TECHNOLOGY

Please provide electronic copies of the following items as of **December 31, 2023**, unless otherwise indicated. File submissions should be labeled using the appropriate number corresponding to the request list "Item #" below (i.e., CYBER.6 - Qualifications of the CISO –). Preferred file types include Word, Excel, or Adobe PDF documents. All documentation and responses are due by **June 28, 2024**. If an item is not applicable, place an "X" in the right column and explain why it's not applicable.

Failure to provide complete and timely responses could hinder the overall examination process and result in the citation of violations of law or regulation. For example, management is reminded of its obligations to make available all documentation and information relevant to the entity's cybersecurity program to the superintendent upon request (Part 500.2(e)) and maintain for examination by the Department all records, schedules and data supporting annual certificate of compliance for a period of five years and make such documentation available for inspection by the superintendent (Part 500.17(b)(3)).

Item #	Item Description	N/A
<b>CYBERSECURITY - Provide the following:</b>		
CYBER.1	If the entity is considered a Class A company, provide copies of the two (2) most recent audited financial statements and an employee roster or audited company statement (such as an annual report) that includes number of employees for the Covered Entity and its affiliates.	
CYBER.2	If the entity has filed a Notice of Exemption pursuant to 23 NYCRR 500.19, provide a statement indicating the exemption(s) claimed and the analysis used to support such claim(s), including: <ol style="list-style-type: none"> <li>a. the number of employees and independent contractors at all the entity's Affiliates;</li> <li>b. the gross annual revenue of those Affiliates' New York business from the last three fiscal years; and/or</li> <li>c. the year-end total assets of those Affiliates corresponding to each subsection of the exemption(s) claimed by the entity</li> </ol>	
CYBER.3	If the entity has adopted all, or a portion of the Cybersecurity Program of an Affiliate <sup>21</sup> , as defined in 23 NYCRR § 500.1(a), or utilizes information systems maintained by an Affiliate, provide copies of any Service Level Agreements or Intercompany Agreements describing	

<sup>21</sup> Affiliate means any person that controls, is controlled by or is under common control with another person. For purposes of this subdivision, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of stock of such person or otherwise.

Letter 6/13/2024

Item #	Item Description	N/A
	such arrangements. For each adopted provision of the Affiliate’s cybersecurity program, provide any relevant documentation necessary to demonstrate compliance with such adopted provisions.	
CYBER.4	Policies and procedures that demonstrate compliance with the relevant sections of Part 500.3: a) information security, b) data governance, classification, and retention including data disposal, c) asset inventory, device, and end of life management, d) access controls, including physical control, remote access and identity management, e) business continuity and disaster recovery planning and resources, f) systems operations and availability concerns, g) systems and network security and monitoring, h) security awareness and training, i) systems and application security and development and quality assurance, j) physical security and environmental controls, k) customer data privacy, l) vendor and Third-Party Service Provider management, including any security policies and procedures, m) risk assessment, n) incident response and notification, o) vulnerability management.	
CYBER.5	The organizational chart detailing the organizational hierarchy, as well as the individuals involved in governance and oversight of Information Security and Cybersecurity, their names, titles, positions, and roles	
CYBER.6	The curriculum vitae or resume and job descriptions for key Cybersecurity personnel (e.g., CISO). If the CISO function is outsourced to a third party or affiliate, provide copies of any agreement describing the cybersecurity-related services to be provided.	
CYBER.7	To the extent that the entity has met the requirement set forth in 23 NYCRR 500.4 to designate a Chief Information Security Officer (CISO) by using an employee of an Affiliate or a Third-Party Service Provider, identify the senior member(s) of the entity’s personnel responsible for direction and oversight of the CISO and provide supporting documents to evidence such oversight.	
CYBER.8	Identify the individual(s) responsible for the duties of the CISO in the event of a short or long term absence (or outage) (alternate/backup for CISO).	

Letter 6/13/2024


Item #	Item Description	N/A
CYBER.9	A copy of the most recent specialized cybersecurity training provided to cybersecurity personnel, including training materials, attendance logs, and certificates of the training. Also provide a schedule of such training planned for the coming calendar year.	
CYBER.10	Describe any threat intelligence feeds or security advisories (e.g., CISA, US Cert, InfraGard) the Company subscribes to, and any memberships in intelligence sharing programs or communities (e.g., FS-ISAC, MS-ISAC) (i.e. what resources are used to monitor changes in cybersecurity threats and how is the information disseminated).	
CYBER.11	List of all committees or groups (Board, management, department, and other) that are responsible for IT-related discussions, including information security and cybersecurity. For each committee (group), describe the primary functions (e.g., development and approval of the cybersecurity program), member names and titles, charters, and frequency of meetings.	
CYBER.12	Copies of the CISO's written annual reports to the senior governing body (e.g., Board) or senior officer, for the last two (2) years, and any other reports and/or presentations on material cybersecurity issues, such as significant cybersecurity events, extortion or ransomware payments made, and/or significant changes to the entity's cybersecurity program (if submitted at a more frequent cadence).	
CYBER.13	Minutes for any IT/IS-related Board and/or Management committee meetings since the previous examination. For example, IT Steering, Information Security, Project Management, Change Management, etc.	
CYBER.14	Evidence of the Board members' expertise and knowledge (e.g., experience, education, and training) to exercise effective oversight of cybersecurity risk. If advisors or experts are utilized, provide copies of the consulting agreements.	
CYBER.15	A list of IT-related plans (including cyber) for the short term (next 12 months) and long term (12 – 48 months), including the status of such plans (e.g., project tracker) and associated budgets for last year and this year.	
CYBER.16	In addition to policies and procedures relating to penetration testing and vulnerability management provide the following: a) Two samples of penetration testing reports for the last two (2) years of the information systems from both inside and outside the	

Item #	Item Description	N/A
	<p>systems’ boundaries, including a copy of the risk assessment used to support the frequency and scope of penetration testing activities.</p> <p>b) The last four (4) vulnerability scans and the report of any manual review of systems not covered by the scans.</p> <p>c) Patch management reporting including (1) Most recent Patch Installation report and (2) Patch Aging report.</p> <p>d) A description of the process for being promptly informed of new security vulnerabilities, including details of any monitoring processes in place.</p> <p>e) Copies of reports and documentation that demonstrate how vulnerabilities, including those reported in audits, and penetration tests are prioritized and remediated in a timely manner, based on the risk they pose to the covered entity.</p> <p>f) If testing is performed by external parties, provide copies of any agreements.</p>	
<p>CYBER.17</p>	<p>Indicate and provide the technical products and controls used to address the 23 NYCRR 500.6 (a)(1) &amp; (a)(2) audit trail requirements. Describe the controls used to protect the integrity of audit trails and log data from alteration or tampering and provide copies of any enterprise-wide data retention and/or back-up procedures.</p>	
<p>CYBER.18</p>	<p>For Access privileges and management,</p> <p>a) Provide policies and procedures that limit access privileges to information systems including those with Nonpublic information that ensure:</p> <ul style="list-style-type: none"> <li>• User access privileges necessary for user’s job performance.</li> <li>• Privilege accounts are minimized and solely used for performing functions that require such access.</li> <li>• Removing or disabling accounts and access as no longer necessary.</li> <li>• Standards that ensure secure configuration of protocols to remote devices.</li> <li>• Evidence of electronic mail authentications controls such as DMARC or that prevent spam, and phishing attacks.</li> </ul> <p>b) Provide a detailed list of access privileges for all personnel, including those with elevated access levels, remote access capabilities, and multi-factor authentication for employees as requested by examiners.</p> <p>c) Provide sample reports used for auditing individual system access rights periodically but at minimum annually. These reports</p>	

Letter 6/13/2024



Item #	Item Description	N/A
	<p>should demonstrate the organization's compliance with periodic reviews and account management protocols.</p> <p>d) Provide written standards for password parameter for all applications, including requirements for minimum length, complexity, prohibition on repeat use, frequency of change, restrictions on similarity, and repeating characters. Include configurations and screenshots showing these standards implemented on critical systems and applications.</p> <p>e) If applicable, detail any Privileged Access Management (PAM) and/or Privileged Identity Management (PIM) policies, procedures, standards, and describe any tools or solutions in current development or in use.</p>	
CYBER.19	<p>Any procedures, guidelines, or standards addressing secure in-house application development practices, and requirements for evaluating, assessment, or testing the security of externally developed applications. Copies of sample configuration and change management documentation.</p>	
CYBER.20	<p>Complete copies of the most recently approved risk assessment(s) that form the basis of the Cybersecurity Program, which includes criteria for evaluation and categorization of cybersecurity risks and threats, assessment of confidentiality, integrity, and availability of information systems and nonpublic information, and risk mitigation and acceptance of (residual) risks.</p> <p>Additionally, please provide any summaries or analysis used to report the results of these assessment to the entity's senior management, board of directors, a committee of the board, or an equivalent governing body.</p>	
CYBER.21	<p>Please provide the policy and standards or a detailed description of the risk assessment methodology indicating how it relates to protecting information systems including nonpublic information (NPI) as outlined in Part 500.9(b)(1),(2),(3). Additionally, include the name(s) of the parties responsible for maintaining the risk assessment policy and standards.</p>	
CYBER.22	<p>A copy of any policy or procedure relating to the types of events or circumstances that would trigger an update to the Risk Assessment, such as the development of new products or services, new geographies of operation, or evolving cyber threats.</p>	
CYBER.23	<p>A list of any new products and/or services that are being implemented, or have been implemented, since DFS's previous examination including a description of any significant changes in IT/IS management</p>	

Letter 6/13/2024

Item #	Item Description	N/A
	personnel, software, hardware, or operating procedures which have occurred or are planned.	
CYBER.24	Copies of any self-assessments, and/or controls gap analyses, performed by the CISO, internal audit function, or external consultant to monitor, manage, and determine the adequacy of the overall cybersecurity program.	
CYBER.25	To the extent that the entity has identified areas, systems or processes that require material improvements, updating or redesign, provide the schedule identifying such items and the remedial efforts underway to address such areas, systems, or processes.	
CYBER.26	Documentation evidencing management’s efforts to address IT/IS Findings, Matters Requiring Immediate Attention (MRIA), Matters Requiring Attention (MRA), and/or violations of laws or regulation identified during previous examinations. The documentation should support corrective measures to address all the issues and independent validation of any completed measures. In addition, provide all internal tracking and validation reports for the Findings/MRIA/MRAs.	
CYBER.27	A statement or other documentation of the risk appetite that the Board has created for management, and a description of how identified risks will be mitigated or accepted.	
CYBER.28	<p><b>Complete the attached spreadsheet.</b> Additionally, prepare for review, a list of all Third-Party Service providers, vendors, and independent contractors and include the following details regarding each one: name, service provided, contract date, vendor risk rating, and date of last due diligence review. Be prepared to provide samples of due diligence and system security reviews for critical service providers, including any periodic analysis of financial condition and control environment.</p> <div style="text-align: center;">  <p>Critical 3rd Party Service Providers.xlsx</p> </div>	
CYBER.29	<p>Information concerning cloud computing, including:</p> <ol style="list-style-type: none"> <li>a) the type of cloud service (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS),</li> <li>b) how the service is used, and</li> <li>c) the name of the cloud provider and a copy of the contract,</li> <li>d) Multi-Factor Authentication controls.</li> </ol>	



Letter 6/13/2024

Item #	Item Description	N/A
	e) Encryption controls used for data at rest and data in motion.	
CYBER.30	Identify any applications, if any that is used to manage and support in the entity's Third-Party Risk Management Program.	
CYBER.31	<p>Be prepared to provide examiners with:</p> <p>(a) The third party risk assessments conducted on critical or high-risk third-party service providers.</p> <p>(b) Copies of all agreements with Third-Party Service Providers regarding the entity's Cybersecurity Program and the Risk Assessments.</p> <p>(c) Due diligence and system security reviews for critical service providers and new critical vendors. Include any cybersecurity questionnaires or periodic analysis of the financial condition and control environment.</p> <p>(d) The most recent third party service provider reporting to the Board (risk rating, financial review, service level agreement review, exceptions, etc.).</p>	
CYBER.32	If applicable, make any necessary preparations to allow examiners to perform a physical walkthrough to inspection physical and environmental security controls at onsite telecommunications or server rooms and/or offsite datacenters or co-locations (within reasonably commutable distance from the primary examination site).	
CYBER.33	Policies, procedures, standards and guidelines on the use of multifactor authentication (MFA). Detail the MFA methodologies used to authorize customer and employee access (e.g., passwords, tokens, certificates, etc.)	
CYBER.34	If MFA is not in use, provide evidence of the written CISO's annual review and approval of MFA exceptions, including a consideration of the use of reasonably equivalent or more secure controls.	
CYBER.35	<p><b>Complete the applicable Platform Data Sheet (Depository or Non-Depository)</b></p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">             Platform Datasheet            - Depository.doc         </div> <div style="text-align: center;">             Platform Datasheet            - Non-Depository.dc         </div> </div>	
CYBER.36	A comprehensive listing of the entity's assets and infrastructure including those provided by third-party service providers.	

Item #	Item Description	N/A
	<p>(a) Indicate the owner, location, criticality of assets, end-of-life status and support expiration dates;</p> <p>(b) List the tools used to ensure that management has an up-to-date asset inventory (hardware and software) and the tools used to scan assets;</p> <p>(c) Describe tools used to monitor and detect changes or anomalies in the IT environment.</p> <p>(d) For critical vendor software that is used in-house, describe any source code agreements and related applicable escrow audit confirmations.</p>	
CYBER.37	Policies, procedures, or standards addressing methods for secure disposal of nonpublic information, stored on various mediums or storage types (e.g., disks, tapes, cloud), that is no longer necessary for business operations.	
CYBER.38	<p>A comprehensive list of technical controls including samples of monitoring reports (e.g., security violations, failed access attempts, changes to security profiles, alerts) the Company utilizes to monitor user and system activities, protect against malicious code, detect unauthorized access of information systems and non-public information.:</p> <p>a. If applicable, describe any centralized log management solution(s) and security event alerting mechanisms in place.</p> <p>b. Describe controls that are designed to protect against malicious code, including those that monitor web traffic and electronic mail.</p> <p>c. If applicable, describe any deployed Enhanced Detection and Response (EDR) tools used to monitor and detect anomalous activities and malicious code across your network.</p>	
CYBER.39	Copies of any information security, cybersecurity (including social engineering and phishing testing), and/or privacy training materials, provided to all employees since the last examination. Indicate the method of delivery, dates training was offered, and evidence of employee completion (e.g., attendance records).	
CYBER.40	Policies, procedures, standards, and guidelines for encryption of data at rest and in-transit, along with diagrams, screenshots, and configurations evidencing the implementation of encryption, in accordance with industry standards. If encryption of NPI at rest is deemed infeasible, provide evidence that the CISO reviews and approves the feasibility of encryption and effectiveness of alternative compensating controls at least annually.	

Letter 6/13/2024

Item #	Item Description	N/A
CYBER.41	Copies of any incident response plans, for responding to, and recovering from, cybersecurity events affecting the confidentiality, integrity or availability of information systems or non-public information maintained by the Company or its service providers. Include all procedures (e.g., runbooks, playbooks) addressing specific steps for responding to different incident types (e.g., Ransomware, DOS/DDOS, Data exfiltration and data leakage or loss, social engineering and phishing) and processes for ensuring timely notification of external parties (as required by law or regulation).	
CYBER.42	Business Continuity and Disaster Recovery (BCDR) plans, including any Business Impact Analyses used to identify, assess, and prioritize recovery of critical business processes and establish key recovery metrics to guide recovery and testing activities. Such plans should address documents, data, facilities, infrastructure, external DR services, personnel, training, internal and external communications, and periodic testing.	
CYBER.43	Reports of any tests (including tabletop exercises), relevant to incident response and BCDR plans since DFS's last examination, including tests evidencing the Company's ability to restore critical data and information systems from backups. Also provide copies of any reports to the Board (or senior governing body), including the dates, scope of testing, results, and action plans.	
CYBER.44	Provide a list of any cybersecurity attacks, significant security events, and/or operational disruptions, experienced by the Company, or third-party service providers since the previous examination, that have not been reported to DFS. Include a brief description of the events, and other relevant information such as dates and reporting to any government body, self-regulatory agency, or other supervisory body.	
<b>IT AUDIT / INDEPENDENT TESTING PROGRAM - Provide the following:</b>		
ITAUDIT.1	<ul style="list-style-type: none"> <li>a) Organizational chart for the Information Technology (IT) Audit Department, and</li> <li>b) Job descriptions for employees in the IT Audit Department and/or a list of all duties (audit and other) performed by them.</li> </ul>	
ITAUDIT.2	<ul style="list-style-type: none"> <li>a) The most recent resumes or biographies for the IT Auditor(s), and</li> <li>b) A list of any training received by the IT Auditor(s) since the last examination.</li> </ul>	

Letter 6/13/2024

Item #	Item Description	N/A
ITAUDIT.3	a) The Audit Committee Charter b) Minutes and reports for any Audit Committee(s) meetings held since the prior examination	
ITAUDIT.4	a) The Internal Audit Charter, and b) The Audit Manual or Policy	
ITAUDIT.5	The most recent IT audit risk assessment, that details audit priorities (e.g., IT Audit Universe), and corresponding IT audit plan/schedule (current and/or next year).	
ITAUDIT.6	All IT-related internal and external audit reports and reviews completed since the previous examination, including those regarding the Information Security Program. Include engagement letters for any outsourced audits and reviews.	
ITAUDIT.7	Copies of any audit and regulatory findings/exception tracking reports	
ITAUDIT.8	Make available for examiners to review: a) Audit tasks outlines (work programs), if any; and b) Workpapers for examiner selected audits.	
ITAUDIT.9	Describe audit involvement in major application development, acquisition, conversion, and testing activities, including continuous monitoring activities.	
<b>IT MANAGEMENT - Provide the following:</b>		
ITMGT.1	Describe management succession plans for key IT personnel.	
ITMGT.2	Provide a listing, with examples, of management information system reports (including, but not limited to, system availability and resource utilization reports) and other management reports that are used by senior level management (e.g., on dashboards) to monitor the IT operations.	
ITMGT.3	Provide a summary of insurance coverage related to computer processing, electronic transaction activities, business interruption, and/or cybersecurity risks, including coverage in a stand-alone cyber insurance policy or as an endorsement to another type of policy.	
ITMGT.4	Provide a list of reports management and the Board of Directors (or designated committee) used to monitor the entity's compliance with Section 501(b) of the Gramm-Leach-Bliley Act ("GLBA").	

Letter 6/13/2024

Item #	Item Description	N/A
<b>DEVELOPMENT AND ACQUISITION</b>		
DA.1	Project, and change management policies, manuals, standards, and guidelines, if not already provided. Include: <ul style="list-style-type: none"> <li>• Information regarding software updates</li> <li>• Emergency program changes</li> <li>• System development life-cycle processes.</li> </ul>	
DA.2	Description any custom software used (report development, bridging/middleware, ancillary applications, applicable programming interfaces (APIs)). Indicate whether they are maintained, developed, or supported internally or externally. Provide documentation of periodic tests of the security controls over internally developed software and independent reviews of software integrity prior to placing into production.	
<b>ARCHITECTURE, INFRASTRUCTURE, AND OPERATIONS (formerly IT Operations)</b>		
AIO.1	Network topologies, diagrams, or schematics depicting physical and logical operating environment(s), including network devices, firewall, IDS/IPS, and connectivity to hosts, branches, and recovery sites. Do not include IP addresses.	
AIO.2	Provide all capacity management reports used to ensure the entity's computing infrastructure has adequate resources to handle current and future data processing requirements. Such reports include those used for IT monitoring, administration and planning actions.	
AIO.3	Provide a sample of the report(s) used to track and resolve reported Helpdesk and IT operational incidents and problems.	
AIO.4	Provide a list of configuration standards and policies to harden servers, laptops, workstations, firewalls, and mobile devices. Provide samples of device hardening checklists (as appropriate).	
AIO.5	For each major system and application, provide the name(s) of the administrator(s) and a brief description of his or her responsibilities.	