Regulatory Impact Statement for the Proposed Second Amendment to 23 NYCRR Part 500 ("Part 500")

1. Statutory Authority: Financial Services Law ("FSL") §§ 102, 201, 202, 301, 302, and 408; Banking Law ("BL") §§ 10, 14, 37(3), 37(4), and 44; and Insurance Law ("IL") §§ 109, 301, 308, 309, 316, 1109, 1119, 1503(b), 1717(b), 2110, and 2127 and Articles 21 and 47.

FSL § 102 states that the goals for the Department of Financial Services ("DFS") include the establishment of "a modern system of regulation, rulemaking and adjudication that is responsive to the needs of the banking and insurance industries and to the needs of the state's consumers and residents", and "to promote the reduction and elimination of fraud, criminal abuse and unethical conduct by, and with respect to, banking, insurance and other financial services institutions and their customers."

FSL § 201 grants DFS broad authority to take such actions as are necessary to: ensure the continued solvency, safety, soundness, and prudent conduct of the providers of financial products and services; protect users of financial products and services from financially impaired or insolvent providers of such services; and eliminate financial fraud, other criminal abuse and unethical conduct in the industry.

FSL § 202 establishes the Office of the Superintendent.

FSL § 301 gives DFS broad power "to protect users of financial products and services."

FSL § 302 provides DFS with broad authority to adopt regulations relating to "financial products and services."

FSL § 408 grants DFS authority to levy civil penalties after notice and hearing in addition to any civil or criminal liability provided by law.

BL § 10 gives DFS the authority to supervise and regulate all banking organizations in such manner as to ensure the safe and sound conduct of such business and to maintain public confidence in such business and protect the public interest and the interests of depositors, creditors, shareholders and stockholders.

BL § 14 allows DFS to determine what is an unsafe manner of conducting the business of banking organizations and what is an unsafe condition of a banking organization.

BL § 37(3) allows DFS to require special reports from banking organizations and other organizations subject to BL § 37(3).

BL § 37(4) authorizes DFS to prescribe the form and content of all periodic and special reports except as expressly provided by BL § 37.

BL § 44 gives DFS the ability to issue fines for violations of the BL by entities subject to the BL.

IL § 109 grants DFS the authority to levy fines against persons and entities subject to the IL for violations of the IL and regulations promulgated thereunder.

IL § 301 gives DFS the authority to prescribe, withdraw, or amend regulations that are consistent with the IL.

IL § 308 provides DFS with the authority to make inquiries of entities subject to the IL or mandate the submission of statements in the form and manner of its choosing.

IL § 309 gives DFS the ability to examine insurers, pension funds, retirement systems, and any other organization required by law to make reports to, or that is subject to examination by, DFS.

IL § 316 grants DFS the authority to require filings be made electronically and grant exemptions to the electronic filing upon request.

IL § 1109 provides DFS the authority to promulgate regulations in effectuating the purposes and provisions of the IL and Article 44 of the Public Health Law and may modify the requirements applicable to the contracts between a health maintenance organization and its subscribers.

IL § 1119 gives DFS the authority to promulgate regulations in effectuating the purposes and provisions of the IL and Article 46 of the Public Health Law, which includes the contracts between a continuing care retirement community and its residents.

IL § 1503(b) requires that holding companies that directly or indirectly control an insurer adopt a formal enterprise risk management function and file an enterprise risk report with DFS annually.

IL § 1604(b) requires that authorized domestic property/casualty insurers adopt a formal enterprise risk management function and file an enterprise risk report with DFS annually.

IL § 1717(b) requires that life and accident and health insurance parent corporations adopt a formal enterprise risk management function and file an enterprise risk report with DFS annually.

IL Article 21 sets forth requirements for all insurance producers, adjusters, life settlement brokers, excess line brokers, reinsurance intermediaries, and insurance consultants.

IL § 2110 authorizes DFS to refuse to renew, revoke, or suspend the license of any insurance producer, insurance consultant, adjuster, or life settlement broker if they have, among other things, violated any insurance laws or regulations.

IL § 2127 grants DFS the authority to fine an Article 21 licensee in lieu of revoking or suspending the licensee's license.

IL Article 47 sets forth requirements for municipal cooperative health benefit plans.

2. Legislative Objectives: This amendment is intended to ensure that all financial services providers regulated by DFS continue to have and maintain cybersecurity programs that meet certain minimum cybersecurity standards in order to protect consumers, continue operating in a safe and sound manner, and protect the stability of our financial system.

3. Needs and Benefits: This amendment is necessary to ensure that DFS-regulated entities address new and evolving cybersecurity threats with the most effective cybersecurity controls and best practices to protect consumers' nonpublic information ("NPI"), prevent and mitigate cyberattacks, and ensure DFS-regulated entities continue to operate in a safe and sound manner. DFS consulted with cybersecurity experts and industry

groups, considered cybersecurity events reported to DFS, and reviewed cybersecurity treatises, standards, rules, and regulations when drafting this amendment.

This amendment clarifies some definitions, including covered entity, penetration testing, person, risk assessment, and third party service provider, and adds definitions for the terms "class A companies," "independent audit," "privileged account," and "senior governing body." Class A companies are a new category of covered entities that are larger, more complex, and have more resources. The definitions and clarifications were established by reviewing accepted standards and guidance from the National Institute of Standards and Technology ("NIST"), the Center for Internet Security ("CIS"), the Federal Reserve Board, the Federal Financial Institutions Examination Council ("FFIEC"), and the Federal Deposit Insurance Corporation ("FDIC").

This amendment requires class A companies to implement additional cybersecurity controls, such as conducting independent audits of their cybersecurity programs at least annually, monitoring privileged access activity, and using external experts to conduct a risk assessment at least once every three years.

This amendment clarifies that covered entities adopting the cybersecurity program of their affiliates must provide the superintendent, upon request, all documentation related to that program regardless of whether the affiliate is regulated by DFS.

This amendment requires the board of directors or equivalent governing body to approve written cybersecurity policies and procedures at least annually and that those policies address data retention, end of life management, remote access controls, systems monitoring, security awareness and training, application security, incident notification, and vulnerability management. These changes are necessary because cybercriminals have been able to access NPI maintained by DFS-regulated entities that have failed to: replace systems that are no longer supported; secure ports that allow remote access; monitor abnormal system activity; secure applications; properly implement MFA for remote access by authorized users; and remediate vulnerabilities in a timely

manner. As cyber threats change rapidly, policies and procedures must be reviewed at least annually to ensure current threats are being addressed effectively.

This amendment adds requirements regarding cybersecurity governance, including requiring that the chief information security officer ("CISO") has adequate authority to ensure cybersecurity risks are appropriately managed, the CISO's annual written report to the covered entity's senior governing body include plans for remediating material deficiencies, the CISO timely report to the covered entity's senior governing body material cybersecurity issues, and the governing body has, or avails itself of, sufficient expertise and knowledge to exercise effective oversight of cybersecurity risk management. Provisions requiring board members to understand cyber activities and risks, oversee major projects related to cybersecurity, review and approve a strategic plan for cybersecurity, and receive appropriate information from sources both internal and external to the entity are supported by guidance from the FFIEC.

This amendment changes the requisite timing of penetration testing to be at least annually and adds requirements for automated scans or manual reviews periodically and promptly after major system changes, a monitoring process to ensure covered entities are promptly informed of new security vulnerabilities, covered entities to timely remediate vulnerabilities and give priority to remediation based on risk, documentation of material issues found during testing, and reporting of those issues to the covered entity's senior governing body.

This amendment adds required controls regarding user and privileged accounts, including limiting the number of them and their functions, to reduce and mitigate the threat of successful ransomware and other cyberattacks. For the same reasons, it also requires covered entities to disable or securely configure all protocols that permit remote control of devices. Class A companies are further required to monitor privileged access activity and implement a privileged access management solution and an automated method of blocking commonly used passwords.

This amendment adds requirements to update risk assessments at least annually and whenever a change in the business or technology causes a material change to the covered entity's cyber risk.

This amendment requires covered entities to incorporate the requirements of section 500.4 in addition to section 500.11 when relying on an affiliate or third party to assist in complying with Part 500.

This amendment requires the use of multi-factor authentication ("MFA"), except where equivalent or more secure compensating controls have been implemented and approved by the CISO in writing, for all privileged accounts and for remote access to the covered entity's information systems and third party applications from which NPI is accessible. In addition, this amendment requires the CISO to periodically, but at a minimum annually, review approvals of compensating controls. These requirements are based on recommendations and guidance on ransomware from many cybersecurity experts and agencies including CIS and the Cybersecurity and Infrastructure Security Agency ("CISA").

This amendment adds requirements regarding the implementation of written policies and procedures regarding asset inventory management and maintenance.

This amendment adds a requirement to implement controls that protect against malicious code and provide cybersecurity awareness training that includes social engineering exercises at least annually. These requirements are in accordance with guidance from CIS, CISA, and the Conference of State Bank Supervisors, among others. Class A companies are further required to implement, unless the CISO has approved in writing the use of reasonably equivalent or more secure access controls, an endpoint detection and monitoring solution and a solution that centralizes logging and security event monitoring,

This amendment eliminates a CISO's ability to review and approve compensating controls for encryption of NPI in transit as DFS has not seen an acceptable, effective compensating control that replaces encryption for data in transit. The CISO's ability to review and approve compensating controls for encryption of data at rest remains but this amendment requires such approval to be in writing.

This amendment requires written plans that contain proactive measures to investigate and mitigate disruptive events and ensure operational resilience, including incident response and business continuity and disaster recovery ("BCDR") plans. Copies of these plans must be made accessible to relevant employees, who are required to be trained on how to implement these plans. The amendment also requires covered entities to test the plans with senior management and staff critical to a response as well as to test the ability to restore systems from backups which must be adequately protected from unauthorized alterations or destruction. Tests must be conducted at least annually and be updated as necessary. These requirements are based on recommendations from CISA, other agencies, and many other cybersecurity experts.

This amendment provides for electronic filing of the forms required to be submitted pursuant to Part 500 and adds a section permitting entities to request an exemption to electronic filing as required by IL § 316. The amendment also eliminates Appendices A and B, which are forms for Certifications of Compliance and Notices of Exemption. Covered entities have been submitting these forms electronically through the department's website so these amendments reflect current practice.

This amendment also allows covered entities to file, instead of a Certification of Compliance, an acknowledgement of noncompliance, which requires a description of the nature and extent of noncompliance and the identification of all areas, systems, and processes that require material improvement, updating, or redesign. Further, it requires that the certification or acknowledgement be signed by the highest-ranking executive at the covered entity and the CISO or, if the covered entity does not have a CISO, the senior officer in charge of cybersecurity. This change is being made to enable covered entities who cannot certify compliance with all sections of Part 500 to submit their reasons for not being able to certify as well as their timelines and plans to come into compliance with Part 500. It also eliminates the need for DFS to follow-up with every covered entity that has not submitted a certification.

This amendment adds a requirement that covered entities notify the superintendent of cybersecurity events where a privileged account has been accessed by an unauthorized user or where the cybersecurity event resulted in the deployment of ransomware within a material part of a covered entity's information systems. Further, covered entities affected by a cybersecurity event at a third party service provider are required to notify the superintendent no later than 72 hours from the time the covered entity becomes aware of such cybersecurity event. Covered entities must also provide updates and supplemental information for cybersecurity events reported.

This amendment adds a requirement to notify the superintendent if an extortion payment is made and to provide an explanation of why the payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment, and all diligence performed to ensure compliance with applicable rules and regulations including those of the Office of Foreign Assets Control. Such reporting requirements are consistent with the reporting framework established by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), which was passed on March 15, 2022.

This amendment expands those that fall within the small business exemption under § 500.19(a) and eliminates § 500.12 from the list of exempted sections. This amendment also extends the list of entities exempted from the requirements of Part 500 to include accredited reciprocal jurisdiction reinsurers pursuant to 11 NYCRR Part 125, individual insurance agents who are placed in inactive status under IL § 2103, and individual licensees placed on inactive status under BL § 599-i. This amendment also exempts individual insurance brokers subject to IL § 2104 who do not otherwise qualify as a covered entity and do not operate, maintain, utilize or control any information systems, and do not own, access, generate, receive or possess NPI and have not for any compensation, commission or other thing of value acted or aided in any manner in soliciting, negotiating or selling any insurance or annuity contract or in placing risks or taking out insurance on

behalf of another for at least one year. It also decreases the time permitted to come into compliance with Part 500 to 120 days if a covered entity no longer qualifies for an exemption.

This amendment defines what constitutes a violation of Part 500 and lists the factors the superintendent considers when assessing penalties pursuant to Part 500 in order to improve transparency. These factors include those listed in BL § 44(a).

This amendment eliminates Appendices A and B, which are forms for Certifications of Compliance and Notices of Exemption, and adds a section regarding exemptions from electronic filing and submission requirements since this amendment requires the aforementioned forms to be submitted electronically.

4. Costs: This amendment may increase costs for some DFS-regulated entities because, if they are not already doing so, they may have to: maintain policies for data retention, end of life management, remote access controls, systems monitoring, security awareness and training, application security, incident notification, and vulnerability management; conduct automated scans or manual reviews periodically and promptly after major system changes; establish a monitoring process for new security vulnerabilities; timely remediate vulnerabilities; utilize MFA for remote access to information systems, third party applications and all privileged accounts except where equivalent or more secure compensating controls have been implemented and approved by the CISO in writing; maintain an asset inventory; implement controls that protect against malicious code; provide cybersecurity awareness training that includes social engineering exercises; test incident response and BCDR plans with senior management including the most senior executive at the covered entity; test the ability to restore systems from backups; and maintain backups that are that are adequately protected from unauthorized alterations or destruction. Costs may increase for covered entities that pay a ransom as they will be required to provide notice and explanation of the payment to the superintendent.

For certain larger companies that are covered entities, costs may further increase. Class A companies must conduct: an independent audit of their cybersecurity programs; systematic scans or reviews of information

systems reasonably designed to identify publicly known cybersecurity vulnerabilities at least weekly; and use external experts to conduct a risk assessment at least once every three years. Such companies also need to: monitor privileged access activity; implement an endpoint detection and response solution to monitor anomalous activity and a centralized logging and security event alerting solution unless the CISO approves in writing the use of reasonably equivalent or more secure controls or tools; and implement a privileged access management solution and an automated method of blocking commonly used passwords unless the CISO approves in writing at least annually the use of reasonably equivalent or more secure compensating controls . These requirements may increase costs for Class A companies that are not already implementing the security measures contained in this amendment. These larger entities have more data to protect, can afford to implement more expensive and stringent controls, and a cyberattack at one of these entities is likely to affect more NYS companies and consumers.

At the same time, this amendment may decrease costs for certain covered entities that will be exempt from the requirements of Part 500, including reciprocal jurisdiction reinsurers, certain inactive insurance agents and brokers, and certain inactive individual banking licensees, provided they do not otherwise qualify as a covered entity. Further, this amendment increases the number of smaller DFS-regulated entities that will qualify for a limited exemption.

It is also anticipated that the costs of compliance will be offset when the required controls prevent or mitigate cyberattacks.

Local governments should not incur additional costs from this amendment. DFS may incur costs to review new filings regarding extortion payments. However, any additional costs incurred should be minimal and DFS should be able to absorb such costs in its ordinary budget. Moreover, DFS's costs should decrease because the new option to file an acknowledgment of noncompliance in lieu of a certification of compliance will eliminate time spent following up with entities that were not qualified to file certifications of compliance.

5. Local government mandates: This amendment does not impose any new programs, services, duties, or responsibilities on local government.

6. Paperwork: This amendment adds a requirement that covered entities provide the superintendent with notice when an extortion payment is made, along with a written description of the reasons for, and alternatives to, payment among other things. This amendment will also permit covered entities to submit an acknowledgement of noncompliance instead of a certification of compliance.

7. Duplication: There may be duplicative requirements for some DFS-regulated entities that are subject to the requirements of 11 NYCRR Part 421 ("Part 421") which requires persons "licensed, or required to be licensed, or authorized, or required to be authorized, or registered, or required to be registered pursuant to the Insurance Law of this State; a health maintenance organization holding, or required to hold, a certificate of authority pursuant to article 44 of the Public Health Law; or an unauthorized insurer in regard to the excess line business conducted pursuant to section 2118 of the Insurance Law and Part 27 of Regulation 41" to implement a comprehensive written information security program. Part 421 also requires such persons and entities to identify reasonably foreseeable threats leading to disclosure of consumer information, design an information security program to control the identified risks, train staff, and test key controls regularly. The provisions in this amendment are much more specific than those in Part 421 and are necessary to ensure that those DFS-regulated entities not subject to the Part 421 also implement an effective cybersecurity program to protect consumers, continue operating in a safe and sound manner, and protect the stability of our financial system.

There may be duplicative requirements for some DFS-regulated entities that are subject to the requirements of 23 NYCRR Part 200, which only applies to those engaging in virtual currency business. To reduce the duplication of requirements, this amendment incorporates some of the requirements of Part 200.

There may be duplicative requirements for some DFS-regulated entities that are subject to the requirements of the Gramm-Leach-Bliley Act ("GLBA"). The Act requires the Federal Trade Commission

("FTC"), the Securities Exchange Commission, and other federal agencies to implement regulations that safeguard the security and confidentiality of customer information, protect against anticipated threats or hazards to the integrity of such information, and protect against unauthorized access to such information which could result in substantial harm or inconvenience to any customer. Although the GLBA applies to "any [financial] institution the business of which is engaging in financial activities," and therefore applies to DFS-regulated entities, the provisions in this amendment are more specific than those in the GLBA and are necessary to ensure that those DFS-regulated entities not subject to the GLBA also implement an effective cybersecurity program to protect consumers, continue operating in a safe and sound manner, and protect the stability of our financial system.

There may be duplicative requirements for some DFS-regulated entities that are subject to the requirements of the Federal Trade Commission's Safeguards Rule ("Safeguards Rule"). The Safeguards Rule requires covered financial institutions designate a qualified individual to implement and supervise their information security program, conduct a risk assessment, maintain an asset inventory, design safeguards based on the risk assessment, implement MFA, create a written incident response plan, and provide a written annual report to the board of directors or equivalent governing body. The provisions in this amendment are more detailed than those in the Safeguards Rule and are necessary to ensure that those DFS-regulated entities not subject to the Safeguards Rule also implement an effective cybersecurity program to protect consumers, continue operating in a safe and sound manner, and protect the stability of our financial system.

There may be duplicative requirements for some DFS-regulated entities that are subject to the requirements of the Computer-security Incident Notification Requirements for Banking Organizations and their Bank Service Providers ("the Banking Organization Notification Rule") which was jointly published by the Officer of the Comptroller of the Currency ("OCC"), the Federal Reserve Board, and the FDIC. The rule applies to banking organizations which are national banks, federal savings associations, or federal branches or agencies

of foreign banks. Such banking organizations are required to notify the OCC no later than 36 hours after the bank determines a computer-security incident has occurred. The provisions in this amendment are broader than those in the Banking Organization Notification Rule and are necessary to ensure that those DFS-regulated entities not subject to the Banking Organization Notification Rule also implement an effective cybersecurity program to protect consumers, continue operating in a safe and sound manner, and protect the stability of our financial system.

There may be duplicative requirements for some DFS-regulated entities that will be subject to CIRCIA. CIRCIA will require covered entities to report cyberattacks to CISA within 72 hours and ransomware payments within 24 hours. However, there is currently no definition of what a covered entity is under the law, nor is there a definition for what constitutes a covered cyber incident. CISA is required to implement a final rule by March 15, 2024. The final definition of covered entity under CIRCIA must consider the consequences that compromise of such an entity could cause to national security, economic security, or public health and safety, the likelihood the entity will be targeted for a cyberattack, and if such an attack would enable disruption of critical infrastructure. The final definition of a covered cyber incident must require at least the occurrence of a cyber incident that leads to substantial loss of confidentiality, integrity, or availability of an information system or network, a disruption of business or industrial operations, unauthorized access or disruption of business caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise. In addition, attacks where the disruptive threat is extortion must be excluded from the definition of covered cyber event under the final rule. Such definitions may not include many entities covered by Part 500 or cyber events they experience, meaning the final rule may not impose reporting requirements deemed essential by DFS.

There may be duplicative requirements for some DFS-regulated entities that will be subject to the Security and Exchange Commission's proposed Cybersecurity Risk Management, Strategy, Governance, and

Incident Disclosure rule ("SEC's Proposed Rule"). That proposed rule, which is subject to change, would require public companies to disclose information regarding any material cybersecurity incidents within four business days of the determination that such an event occurred, and to publicly disclose information about their cybersecurity policies and procedures and the cybersecurity expertise of their board members. The provisions in this amendment are broader than those in the SEC's Proposed Rule and are necessary to ensure that those DFS-regulated entities not subject to the SEC's Proposed Rule also disclose information regarding material cybersecurity incidents.

8. Alternatives: DFS considered not amending the regulation, but this was determined to be an unacceptable alternative because of the rapidly evolving cyber threat landscape, including changing costs of cyber events, effectiveness and types of cybersecurity controls, and cybersecurity best practices. DFS posted a draft of the amendment on its website on July 29, 2022, for pre-proposed outreach and, in response to comments received, made changes to certain provisions such as the Class A companies definition, the requirements for vulnerability management and multi-factor authentication, transitional periods and adding an exemption for inactive individual insurance brokers. For the Class A companies definition, a requirement that these entities must have $20,000,000 in gross annual revenue in each of the last two fiscal years from business operations in New York was added. Some commenters had expressed concern regarding small and medium-sized New York branches of foreign banking organizations being classified as a Class A company. For the vulnerability management requirements, clarifying changes were made in response to questions from commenters regarding whether penetration testing could be performed by internal personnel by stating that penetration testing could be conducted by either internal or external independent parties, and the requirement that Class A companies must conduct weekly systematic scans or reviews was removed and replaced with a requirement that applies for all non-exempt covered entities to conduct scanning at a frequency determined by its risk assessment. For the muti-factor authentication requirements, in response to comments that it would be

technically infeasible to implement multi-factor authentication for all technologies and privileged accounts, changes were made to allow the CISO to approve reasonably equivalent or more secure compensating controls. In response to comments requesting additional time for the transitional periods beyond 12 months, additional transitional periods of 18 months and two years were added that apply for certain new requirements. Additionally, a new exemption for inactive individual insurance brokers was added in response to requests from several commenters.

9. Federal Standards: This amendment may exceed some minimum standards established by the GLBA. Section 6807(b) of the GLBA, however, allows states to implement a statute, regulation, order, or interpretation affording protections that are greater than those in the GLBA.

This amendment may exceed some minimum standards established by the Safeguards Rule.

This amendment may exceed some minimum standards set by the Banking Organization Notification Rule.

This amendment may exceed some minimum standards imposed by the final rule promulgated pursuant to CIRCIA and by the SEC's Proposed Rule.

10. Compliance Schedule: Covered entities will have 180 days from publication of the Notice of Adoption of this amendment in the State Register to comply with its requirements, except as otherwise specified in the amendment.

Regulatory Flexibility Analysis for Small Businesses and Local Governments for the Proposed Second Amendment to 23 NYCRR Part 500

1. Effect of rule: This amendment adds new requirements to ensure that entities regulated by the Department of Financial Services ("DFS") ("covered entities") have and maintain cybersecurity programs that meet certain minimum cybersecurity standards in order to protect consumers, continue operating in a safe and sound manner, and protect the stability of our financial system. Certain covered entities affected by this amendment, such as insurance producers, mortgage brokers, and mortgage bankers, fall within the definition of a "small business" as defined in State Administrative Procedure Act Section 102(8). There are approximately 30,000 business entities licensed as insurance producers, mortgage brokers, and mortgage bankers in New York. Many of these business entities may be small businesses. In addition, industry has asserted that certain insurers, such as mutual and co-op insurers, fall within the definition of a "small business" too.

This amendment does not affect local governments.

2. Compliance requirements: This amendment adds a requirement that covered entities, including covered entities that may be small businesses, provide DFS with notice when an extortion payment is made, along with a written description of the reasons for, and alternatives to, payment, among other things. This amendment will also permit covered entities to submit an acknowledgement of noncompliance instead of a certification of compliance.

This amendment also adds requirements that covered entities, including covered entities that may be small businesses, if they are not already doing so: maintain policies for end of life management, remote access controls, and vulnerability management; conduct vulnerability scans; update risk assessments if a change in the business or technology causes a material change to its cyber risk; utilize multi-factor authentication for all privileged accounts; maintain an asset inventory that tracks certain specified information; monitor and filter emails to block malicious content; provide cybersecurity training and exercises; test incident response plans

with senior management, including the highest-ranking executive at the covered entity; test the ability to restore systems from backups; and maintain backups that are isolated from network connections. This amendment does not impose any additional reporting, recordkeeping, or other compliance requirements on any local governments because local governments are not affected by this amendment.

3. Professional services: No local government will need professional services to comply with this amendment because the amendment does not apply to any local government. A covered entity that may be a small business may need professional services to comply with this amendment.

4. Compliance costs: This amendment may increase costs for some covered entities that may be small businesses because, if they are not already doing so, they may have to: maintain policies for end of life management, remote access controls, and vulnerability management; conduct vulnerability scans; update risk assessments if a change in the business or technology causes a material change to its cyber risk; utilize multi-factor authentication for all privileged accounts; maintain an asset inventory that tracks certain specified information; monitor and filter emails to block malicious content; provide cybersecurity awareness training and exercises; test incident response plans with senior management, including the highest-ranking officer at the covered entity; test the ability to restore systems from backups; and maintain backups that are adequately protected from unauthorized alterations or destruction. Costs may increase for covered entities that may be small businesses and that pay a ransom as they will be required to provide notice and explanation of the payment to DFS.

At the same time, this amendment may decrease costs for certain covered entities that may be small businesses that will be exempt from the requirements of 23 NYCRR 500, provided they do not otherwise qualify as a covered entity, including reciprocal jurisdiction reinsurers, certain inactive insurance agents, and certain inactive individual banking licensees. Further, this amendment increases the number of smaller DFS-regulated entities that will qualify for a limited exemption.

It is also anticipated that the costs of compliance will be offset when the required controls prevent or mitigate cyberattacks.

Local governments will not incur additional costs as a result of this amendment because the amendment does not apply to local governments.

5. Economic and technological feasibility: This amendment does not apply to any local government; therefore, no local government should experience any economic or technological impact because of the amendment. A covered entity that may be a small business may incur economic and technological impacts as a result of this amendment.

6. Minimizing adverse impact: There will not be an adverse impact on any local government because the rulemaking does not apply to any local government. DFS attempted to minimize any adverse impact on covered entities that may be small businesses by providing for exemptions from certain requirements of 23 NYCRR 500.

7. Small business and local government participation: Prior to the July 29, 2022 publication of the pre-proposal amendments, DFS discussed Part 500 with industry and professional groups representing small business at industry conferences and in meetings. Feedback received in those discussions were considered when drafting the proposed amendments. DFS had posted a draft of the amendment on its website on July 29, 2022 for pre-proposed outreach and notified interested parties, including small businesses, of the posting. Interested parties, including small businesses and local governments, will be given another opportunity to review and comment on the amendment once it is posted on the DFS website and published in the State Register.

Rural Area Flexibility Analysis for the Proposed Second Amendment to 23 NYCRR 500

1. Types and estimated numbers of rural areas: Entities regulated by the Department of Financial Services ("DFS") ("covered entities") affected by this amendment do business in every county in this state, including rural areas as defined in State Administrative Procedure Act Section 102(10).

2. Reporting, recordkeeping, and other compliance requirements; and professional services: This amendment adds a requirement that covered entities, including covered entities that may be in rural areas, provide the superintendent with notice when an extortion payment is made, along with a written description of the reasons for, and alternatives to, payment, among other things. This amendment will also permit covered entities that may be in rural areas to submit an acknowledgement of noncompliance instead of a certification of compliance.

3. Costs: This amendment may increase costs for some covered entities that may be in rural areas because, if they are not already doing so, they may have to: maintain policies for end of life management, remote access controls, and vulnerability management; conduct vulnerability scans; update risk assessments if a change in the business or technology causes a material change to its cyber risk; use multi-factor authentication for all privileged accounts; maintain an asset inventory that tracks certain specified information; monitor and filter emails to block malicious content; provide cybersecurity awareness training and exercises; test incident response plans with senior management, including the highest-ranking officer at the covered entity; test the ability to restore systems from backups; and maintain backups that are adequately protected from unauthorized alterations or destruction. Costs may increase for covered entities that may be in rural areas and that pay a ransom as they will be required to provide notice and explanation of the payment to the superintendent.

For certain larger covered entities ("Class A companies") that may be in rural areas, costs may increase. Class A companies must conduct: an independent audit of their cybersecurity programs; systematic scans or reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities at

least weekly; and use external experts to conduct a risk assessment at least once every three years. Such companies also need to: monitor privileged access activity; implement an endpoint detection and response solution to monitor anomalous activity and a centralized logging and security event alerting solution unless the chief information security officer ("CISO") approves in writing the use of reasonably equivalent controls; and, if they are employing passwords as a method of authentication, implement a password vaulting solution for privileged accounts and an automated method of blocking commonly used passwords unless the CISO approves in writing the use of reasonably equivalent controls. These requirements may increase costs for Class A companies in rural areas that are not already implementing the security measures contained in this amendment. Class A companies have more data to protect, can afford to implement more expensive and stringent controls, and a cyberattack at one of these companies is likely to affect more New York residents.

At the same time, this amendment may decrease costs for certain covered entities that may be in rural areas that will be exempt from the requirements of 23 NYCRR 500, provided they do not otherwise qualify as a covered entity, including reciprocal jurisdiction reinsurers, certain inactive insurance agents, and certain inactive individual banking licensees. Further, this amendment increases the number of smaller DFS-regulated entities that may be in rural areas that will qualify for a limited exemption.

It is also anticipated that the costs of compliance will be offset when the required controls prevent or mitigate cyberattacks.

4. Minimizing adverse impact: This amendment uniformly affects covered entities throughout New York State. Therefore, it does not impose any adverse impact on rural areas.

5. Rural area participation: Prior to the July 29, 2022 publication of the pre-proposal amendments, DFS discussed Part 500 with industry and professional groups at industry conferences and in meetings. Feedback received in those discussions were considered when drafting the proposed amendments. Interested parties,

including those parties in rural areas, will be given an opportunity to review and comment on the amendment once it is posted on the DFS website and published in the State Register.

Statement Setting Forth the Basis for the Finding that the Proposed Second Amendment to 23 NYCRR Part 500 Will Not Have a Substantial Adverse Impact on Jobs and Employment Opportunities

The Department of Financial Services ("DFS") finds that this amendment will not have a substantial adverse impact on jobs and employment opportunities. This amendment is necessary to ensure that all entities regulated by DFS continue to have and maintain cybersecurity programs that meet certain minimum cybersecurity standards in order to protect consumers, continue operating in a safe and sound manner, protect the stability of our financial system, and address new and evolving cybersecurity threats with the most effective cybersecurity controls and best practices.