BIG I | NEW YORK

NEW YORK FINANCIAL SERVICES CYBERSECURITY REGULATION

FREQUENTLY ASKED QUESTIONS

Are unlicensed employees of an agency required to make the annual compliance filings?

Are licensed employees required to make the annual compliance filings?

My agency has a New York non-resident license. Do I have to comply with the regulation?

I'm a small agency. Do I have to make the annual compliance filing?

Do I have to make the compliance filing every year?

How do I get help completing the compliance filing?

When I make the compliance filing, how do I know which form to complete?

The compliance filing form is asking if I'm a Class A company. Am I?

How do I know if my agency qualifies for the limited exemption?

Does my agency have to submit the Notice of Exemption every year?

Do agency employees have to submit the Notice of Exemption every year?

I have a new licensed employee or a current employee who just obtained a license. What does that person need to do?

If my agency qualifies for the limited exemption, what requirements do we have to meet?

I don't know how to create a cybersecurity program. How do I make one?

What does the regulation mean by "nonpublic information"?

What is a cybersecurity risk assessment?

How often does the agency have to perform a risk assessment?

Do I have to send cybersecurity questionnaires to every business I work with?

Do I have to send cybersecurity questionnaires to every third-party service provider?

Do I have to send the completed questionnaires to DFS?

What happens if a third-party service provider does not respond to my questionnaire or if it doesn't meet my minimum cybersecurity requirements?

Will my agency get in trouble if a third-party service provider never responds to my questionnaire?

I received a third-party cybersecurity questionnaire from a carrier or wholesale broker with whom I do business. Am I required to complete and return it?

My agency qualifies for the limited exemption. Do I have to encrypt all my emails and stored data?

How do I create an inventory of all my agency's computer network devices?

If something happens, do I have to report it to DFS?

If my agency has a reportable cybersecurity incident, how do we report it?

Does the regulation require me to take a course on cybersecurity?

Does the regulation require the agency to buy cyber insurance?

I have a broker's license in my personal name, but I'm retired. Do I have to comply with the regulation?

The only license in my personal name is an agent's license, and the DFS website says that it is inactive because I don't have any carrier appointments. Do I have to comply with the regulation?

Is all this really necessary?

Where can I get a copy of the regulation?

Are unlicensed employees of an agency required to make the annual compliance filings?

No. The regulation's requirements apply to "covered entities." The regulation defines "covered entity" as any individual or entity "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the (New York) Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies." Back to beginning

Are licensed employees required to make the annual compliance filings?

No, not if the agency's cybersecurity program applies to them. Back to beginning

My agency has a New York non-resident license. Do I have to comply with the regulation?

Yes, the requirements apply to all holders of New York insurance licenses, both resident and non-resident. Back to beginning

I'm a small agency. Do I have to make the annual compliance filing?

Yes, agencies that qualify for the limited exemption must make the annual compliance filing. Back to beginning

Do I have to make the compliance filing every year?

Yes. Agencies of all sizes must complete a compliance filing each year between January 1 and April 15 for the prior calendar year. Back to beginning

How do I get help completing the compliance filing?

Visit the Filing Instructions page in the Cybersecurity section of our website. That page contains a link to a video demonstrating how to do it. It also has links to printed directions from the New York State Department of Financial Services (DFS.) Back to beginning

When I make the compliance filing, how do I know which form to complete?

Complete the checklist of the applicable requirements on the Filing Instructions page of the Cybersecurity section of our website. If the answer to all questions is "yes," submit the Certification of Material Compliance; otherwise, submit the Acknowledgement of Non-Compliance. Back to beginning

The compliance filing form is asking if I'm a Class A company. Am I?

No, unless the agency has at least $20 million in gross annual revenue and either more than 2,000 employees or more than $1 billion in gross annual revenue.

Back to beginning

How do I know if my agency qualifies for the limited exemption?

An agency qualifies for the limited exemption if any one of the following statements about the agency are true:

- It has fewer than 20 employees and independent contractors, including those of its affiliates (any individuals or entities that the agency controls, is controlled by, or is under common control with another individual or entity.)
- It has less than $7,500,000 in gross annual revenue in each of the last three fiscal years from all its business operations and the New York business operations of its affiliates.
- It has less than $15,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates.

Back to beginning

Does my agency have to submit the Notice of Exemption every year?

No, not unless the agency no longer meets one of the criteria listed above.

Back to beginning

Do agency employees have to submit the Notice of Exemption every year?

No. However, if a licensed person changes employers or names, they must submit an amended Notice of Exemption within 30 days. Back to beginning

I have a new licensed employee or a current employee who just obtained a license. What does that person need to do?

Complete and submit the Notice of Exemption within 30 days. There are instructions for completing and submitting it on the Filing Instructions page in the Cybersecurity section of our website. Where the form asks for the reason for the exemption, the employee should check only the box for Section 500.19(b). Where it asks for the name of the covered entity whose cybersecurity program covers the employee, they should enter your agency's name. Back to beginning

If my agency qualifies for the limited exemption, what requirements do we have to meet?

You can find them in the checklist of the applicable requirements on the Filing Instructions page of the Cybersecurity section of our website. Compliance with additional requirements regarding limiting access to your information systems is required by May 1, 2025. Compliance with a requirement to keep an inventory of all information system assets is required by November 1, 2025. Back to beginning

I don't know how to create a cybersecurity program. How do I make one?

Start with the template the DFS created in 2024. Modify it as necessary to reflect your agency's cybersecurity risk assessment. Back to beginning

What does the regulation mean by "nonpublic information"?

Refer to this flow chart linked to the Compliance Resources page in the Cybersecurity section of our website. Back to beginning

What is a cybersecurity risk assessment?

It is the process of identifying, estimating, and prioritizing the cybersecurity risks your agency faces. Think of it as a loss control survey of your information systems.

Back to beginning

How often does the agency have to perform a risk assessment?

At least once a year, more often if a technological or operational change causes a material change in the agency's cybersecurity risks. Back to beginning

Do I have to send cybersecurity questionnaires to every business I work with?

No. The regulation requires covered entities to perform due diligence on the cybersecurity practices of "third-party service providers." This flowchart will help you identify which of your business relationships are third-party service providers.

Back to beginning

Do I have to send cybersecurity questionnaires to every third-party service provider?

No. The regulation requires covered entities to perform "due diligence" on the cybersecurity practices of their third-party service providers. It does not specify what form the due diligence must take. A questionnaire such as the one in our Cybersecurity Bundle is one way to do it. Another way is to check what publicly traded companies have reported to the U.S. Securities and Exchange Commission. Other ways include having documented conversations with the providers' cybersecurity personnel, monitoring the media for reports of security breaches, or any other way to gather information.

Back to beginning

Do I have to send the completed questionnaires to DFS?

No. The information you gather during your due diligence is for your agency's use only. The regulation requires all covered entities to set minimum cybersecurity practices they will expect third-party service providers to meet before they will do business with those providers. The covered entity should compare the information gathered through due diligence to those minimum practices. Back to beginning

What happens if a third-party service provider does not respond to my questionnaire or if it doesn't meet my minimum cybersecurity requirements?

Your agency must decide whether to do business with that provider. The regulation leaves that decision up to you. Be prepared to justify that decision to the DFS should the provider later suffer a cybersecurity incident that impacts your agency.

Back to beginning

Will my agency get in trouble if a third-party service provider never responds to my questionnaire?

If you made a good faith effort to perform due diligence on that provider, you are unlikely to be subject to disciplinary action. See the answer to the previous question regarding how to respond in this situation. Back to beginning

I received a third-party cybersecurity questionnaire from a carrier or wholesale broker with whom I do business. Am I required to complete and return it?

No. The regulation requires the other entity to perform due diligence on your cybersecurity practices, but it does not mandate that you respond to a questionnaire. However, a potential consequence if you choose not to complete it is that they may decide to stop doing business with you.Back to beginning

My agency qualifies for the limited exemption. Do I have to encrypt all my emails and stored data?

No, but it's still a good idea. Back to beginning

How do I create an inventory of all my agency's computer network devices?

Use the information system asset inventory workbook posted under step two on the Compliance Resources page in the Cybersecurity section of our website.

Back to beginning

If something happens, do I have to report it to DFS?

It depends on what happens. The regulation requires a covered entity to report a successful or unsuccessful act or attempt to gain unauthorized access to, disrupt, or misuse its information or the data stored in it. However, the entity must report it only if it occurs at the entity, one of its affiliates, or a third-party service provider, and only if it:

- Impacts the entity and requires it to notify law enforcement or some other regulatory body.
- Has a reasonable likelihood of materially harming any material party of the entity's normal operations.
- Results in the deployment of ransomware with a material part of the entity's information systems.

Back to beginning

If my agency has a reportable cybersecurity incident, how do we report it?

Report it within 72 hours of determining that it has occurred on the same DFS portal you use to submit the annual compliance filing.

Back to beginning

Does the regulation require me to take a course on cybersecurity?

No, but more knowledge about any subject is always a good thing. Also, a course on the cybersecurity regulation may meet the continuing education requirement that licensees take at least one hour of instruction on insurance law.

Back to beginning

Does the regulation require the agency to buy cyber insurance?

No, but buying cyber insurance is just as much a good idea for your agency as it is for your clients. Back to beginning

I have a broker's license in my personal name, but I'm retired. Do I have to comply with the regulation?

You are completely exempt from the regulation if all the following are true:

- You do not directly or indirectly "operate, maintain, utilize or control any information systems."
- You do not, and are not required to, "directly or indirectly control, own, access, generate, receive or possess nonpublic information."
- You have not, "for any compensation, commission or other thing of value, acted or aided in any manner in soliciting, negotiating or selling any policy or contract or in placing risks or taking out insurance on behalf of another person for at least one year."
- You do not otherwise qualify as a covered entity under the regulation.

Back to beginning

The only license in my personal name is an agent's license, and the DFS website says that it is inactive because I don't have any carrier appointments. Do I have to comply with the regulation?

No, you are completely exempt. Back to beginning

Is all this really necessary?

It would be necessary even if there were no regulation because:

- Even a relatively minor cybersecurity incident can disrupt the agency's operations.
- A ransomware attack could shut down the agency, perhaps permanently.
- Clients and business partners may decide to sue the agency following a data breach.
- Clients may lose trust in the agency after a data breach and take their business elsewhere.
- The agency may have difficulty obtaining cyber insurance if it has not implemented the controls the regulation requires.

Back to beginning

Where can I get a copy of the regulation?

The Cornell Law School Legal Information Institute has the current text on its website.

Back to beginning