



Let's Talk MFA

February 26, 2026

Agenda

- 1 Introductions
- 2 Multi-Factor Authentication (MFA) Requirements
- 3 Supervisory Expectations
- 4 Questions



A background image showing a business meeting. In the center, two people in business attire are shaking hands. To the left, a person is holding a tablet and pointing at the screen. In the foreground, there are several documents on a desk, some with charts and graphs. The lighting is bright and professional.

1 Introductions



Speaker Introductions

Sarah Rugnetta

Executive Deputy Superintendent
Cybersecurity Division

Will Peterson

Deputy Superintendent
Cybersecurity Supervision

Sebastian Fischer

Deputy Superintendent
Cybersecurity Operations



The Department of Financial Services

Established with the goal of creating a more comprehensive regulator to oversee the financial services industry, better protect consumers, and encourage economic growth

We regulate the activities of over 3,000 financial institutions with nearly \$10 trillion in assets. This includes more than 1,300 banking and non-depository entities, and more than 1,900 insurance companies

DFS was the first State Department of Banking or Insurance to institute comprehensive cybersecurity regulations



Cybersecurity Division



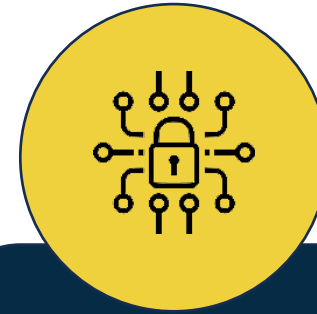
Issues guidance to help clarify requirements of the Cybersecurity Regulation



Enforces the Department's Cybersecurity Regulation, Part 500



Issues alerts to covered entities about emerging and persistent cyber threats



Conducts cybersecurity and IT examinations of covered entities



Monitors cybersecurity incidents reported to DFS

Who has to comply with Part 500?

Covered Entities

23 NYCRR § 500.1

Any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies.



Tailored Requirements Based on Size and Revenue*

Small Businesses (§500.19(a) Exemption)

Must comply with only specific requirements.

Non-Class A, Non-Exempt ("Standard") Companies

Must comply with most requirements.

Large ("Class A") Companies

Must comply with all requirements.

*Part 500 includes other full and limited exempt categories of Covered Entities.



Nonpublic Information (§500.1(k))



**Sensitive
Business
Information**



**Personally
Identifiable
Information
(PII)**



**Protected
Health
Information
(PHI)**



2 MFA Requirements



Authentication Primer

What does “Authentication” mean?

- Verifying the identity of a user or account to authorize access to specific resources in an Information System, including potentially Nonpublic Information (NPI).

Why is it important?

- Authentication measures are designed to protect Information Systems against unauthorized or fraudulent access.
 - Authenticating users builds confidence that actions taken on Information Systems (*e.g.*, deleting data, sharing information) are done by specific, known users.

How is it done?

- Authentication involves checking measurable characteristics of identity – commonly called factors – against the Information System's digital record.



What is Multi-Factor Authentication (MFA)?

Multi-factor authentication (MFA) is a security control that provides an enhanced means of verifying the identity of a user. Specifically, Section 500.1(j) defines MFA as authentication through verification of **at least two** of the following types of authentication factors:



Knowledge
(Something you know)
Such as a password,
passphrase, or personal
identification number (PIN)



Possession
(Something you have)
Such as a token, app, or
smartcard



Inherence
(Something you are)
Such as a biometric
characteristic like a
fingerprint or face scan



Regulatory Requirements


Where can I find the MFA requirements?

- Section 500.12 of the Cybersecurity Regulation (Part 500)
- Guidance on the Cybersecurity Resource Center


MFA Requirements

MFA is generally required to be utilized for any individual accessing any information systems of the covered entity.


For Small Businesses:



Remote access
to the covered
entity's
information
systems



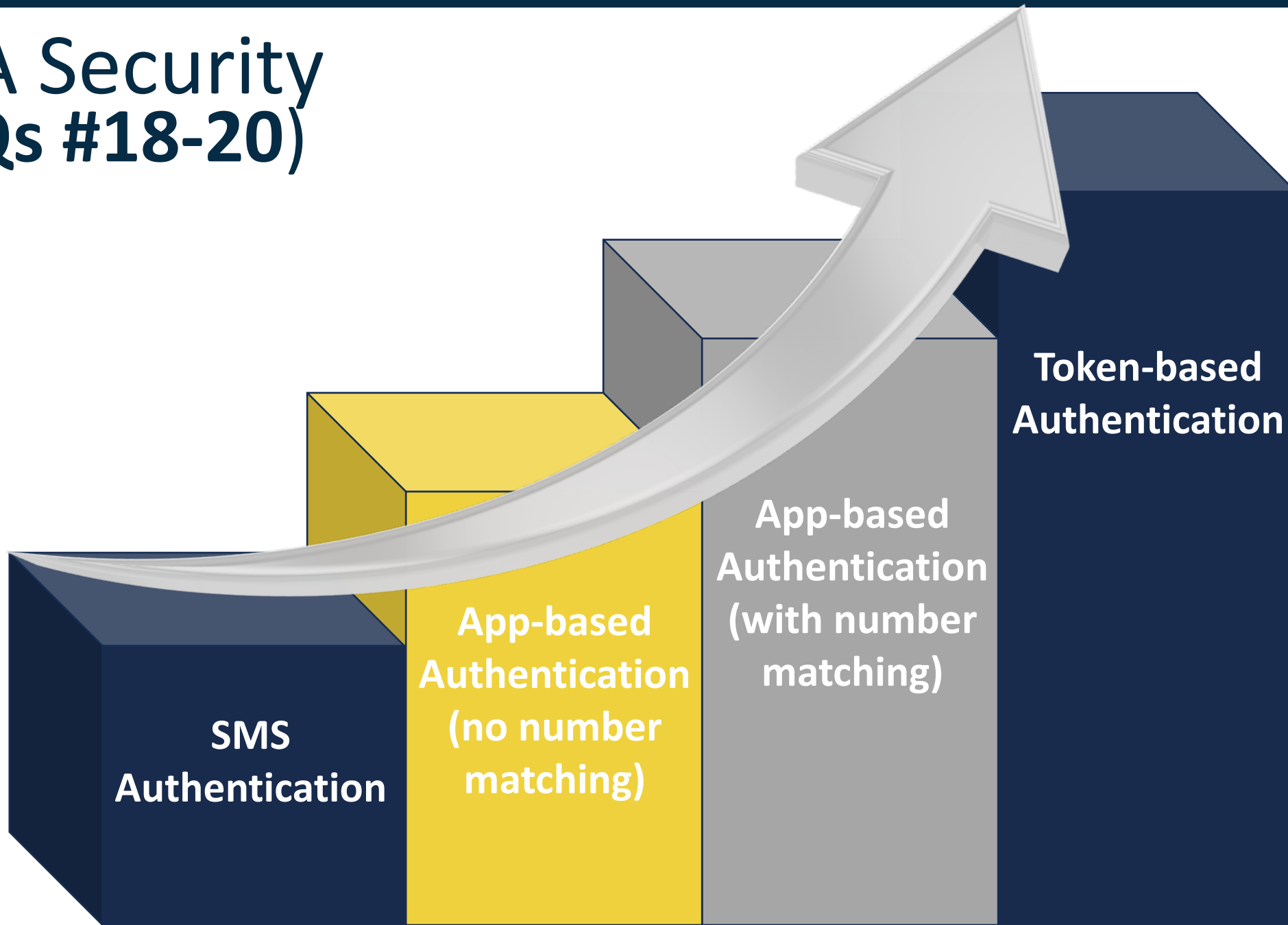
Remote access to
third-party
applications



Privileged accounts
(except non-
interactive service
accounts)



MFA Security (FAQs #18-20)



Possession Factors (FAQ #19 Continued)

Key Concept

A possession factor requires cryptographic or technical proof that the user controls a specific device, token, or authenticator at the time of authentication.

Hardware tokens or security keys

Authenticator applications generating one-time codes

Push authentication with protections such as number matching or user interaction

Device or credential-based mechanisms that provide cryptographic proof of possession



MFA Through Single Sign-On (FAQ #21)

Single Sign-On (SSO)

May be used; however,
MFA must be enforced
as part of the
authentication process

SSO alone does
not satisfy MFA
requirements



Cloud-Based Email and Document Hosting Services (FAQ #22)

Among other things, MFA is required for Covered Entities accessing:

Cloud-based
email services

Cloud-based
document storage
and collaborative
platforms

Cloud-based business
applications or systems



External-Facing Information Systems (FAQ #23)

Most external-facing information systems (e.g., website home, marketing, contact pages) do not require MFA.

unless:

Other Information Systems can be accessed from the external-facing system without authentication

The Information System otherwise poses a material cybersecurity risk to the Covered Entity, its customers, other Information Systems, or NPI



3 Supervisory Expectations

COMPLIANCE



Governance Requirements for MFA Compensating Controls

Multi Factor Authentication

23 NYCRR § 500.12(b)

- Non-exempt Covered Entities* must implement MFA or reasonably equivalent or more secure compensating controls.
- The CISO must approve, in writing, the compensating controls.
- The compensating controls must be reviewed periodically, but at a minimum, annually.

*Small Businesses may rely on Section 500.12(b) only if they have a CISO.



DFS Supervision



Status and sufficiency of implementation



Risk-based decisions, exceptions, and compensating controls



Scope of implementation (e.g., has MFA been implemented with third-party platforms?)



Governance & Oversight Practices



Documentation and reasonableness of risk-based determinations



Supervisory Expectations for MFA



MFA Control
Strength



MFA with SSO



Cloud-Based
Email &
Document
Hosting



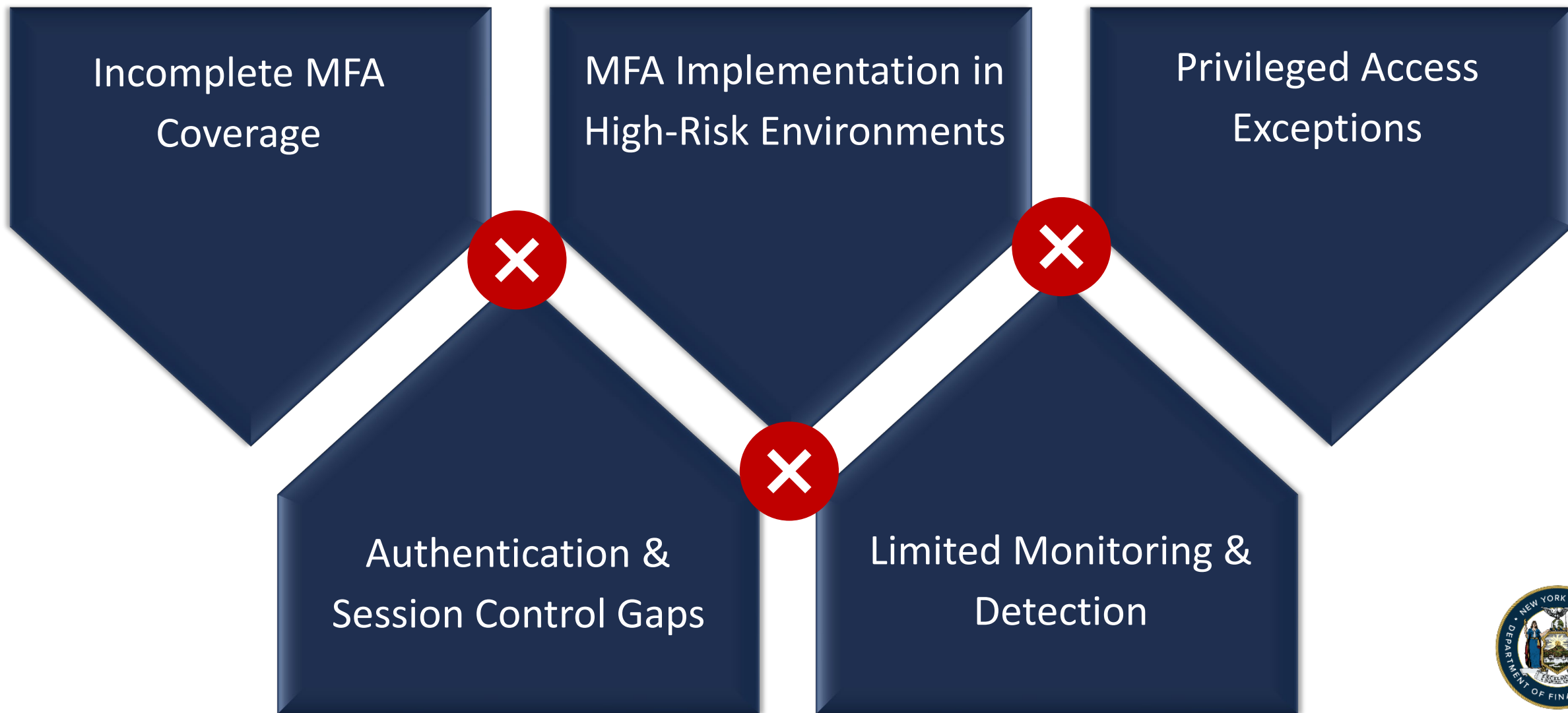
External-
Facing
Information
Systems



Supervisory Considerations for Compensating Controls



Common Themes on MFA Examinations



4 Audience Questions

COMPLIANCE



Thank You!

For more information: dfs.ny.gov/cyber

