CDSystems

New York State Department of Financial Services (DFS) Security Assessment

WHO IS IT FOR?

- **NYS Department of Financial Services Covered Entities…**
  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 of New York State.

WHY IS IT IMPORTANT?

- **It's not optional** – Organizations who must comply with the 23 NYCRR 500 DFS cybersecurity regulation must, by law, perform the prescribed actions within the regulation.
- **Things change** – Addressing risk is not a one-time ordeal. As business objectives change, employees come and go, and technology advances, the need for cybersecurity risk assessment services is constant.
- **Keep your license** – If you are not compliant with the 23 NYCRR 500 DFS cybersecurity regulation, you may lose your license to operate in New York State.

HOW CAN WE HELP?

The DFS security assessment is designed to:

- **Identify gaps** in DFS compliance.
- **Develop a roadmap** for remediating gaps in DFS compliance.
- **Pass an audit** – Find problem areas so you can make adjustments before DFS sends auditors.

WHAT IS INCLUDED?

The DFS security assessment includes:

- **Internal & External Vulnerability Assessment** – Identifies vulnerabilities in the technical environment and develops a prioritized remediation report with recommendations for how to remediate vulnerabilities.
- **What-If Threat Simulation** – We work with the Covered Entity to go over various attack scenarios. The goal is to ask "what would happen if…?" and identify areas in procedural security where the Covered Entity needs to bolster their controls.
- **Policy and Controls Review** – We review existing policies and controls and looks for gaps that would result in failing DFS compliance. A roadmap for compliance will be provided and presented.
- **Risk Evaluation** – We gather information about the business and how it operates. Workflows, data, and systems are mapped out and risk values and statements are assigned. An information security plan will be created to document initiatives for the upcoming year.
- **Security Plan** – Based on the Risk Evaluation, we create a custom security plan designed to meet § 500.02 "Cybersecurity Program". The document will serve as a roadmap built according to your unique risk, resources, and business environment.