

# **New York City: Cyber Research**

# Table of Contents

## Portal 1: NYC Cyber Command

( <a href="https://www.nyc.gov/site/em/ready/cybersecurity.page">https://www.nyc.gov/site/em/ready/cybersecurity.page</a> ).....	3
Purpose: .....	4
Features:.....	5-7
Chatbot: Yes / No.....	7
Additional Pointers: .....	8

## Portal 1: NYC Cyber Command

(<https://www.nyc.gov/site/em/ready/cybersecurity.page>)

### Purpose:



- NYC Cyber Command was established to function as the City's centralized cyber-defines organization, tasked with coordinating cyber-security policies, standards, incident response and threat intelligence across New York City agencies.
- It aims to protect the City's information infrastructure, critical services and public welfare by managing city-wide cyber threats, leading investigations and liaising with federal, state and private sector partners.
- It serves to standardize cyber-security practices across municipal agencies and enforce compliance with security frameworks and procurement reviews, enhancing resilience of governmental operations.

Features:

1. Policy & Standards Setting

NYC

Services

Events

Office of the Mayor

Your government

Office of the Mayor

News

Contact the Mayor

Biography

Q Search

English

The Cyber Command Operations of the Office of Technology and Innovation

[Download Executive Order 10](#)

WHEREAS, government entities at the Federal, State and local levels have increasingly become the targets of sophisticated malicious cyber-attacks that compromise the security and integrity of government operations; and

WHEREAS, the City of New York is a prime target for cyber-threat actors; and

WHEREAS, protecting the City's information infrastructure is vital to its continued operations and to ensuring the health, safety and welfare of its residents; and

WHEREAS, pursuant to Executive Order No. 3, issued on January 19, 2022, the Mayor established the Office of Technology and Innovation, which incorporated the Office of Cyber Command, the City's centralized cyber response office; and

WHEREAS, collaboration and information sharing between government, law enforcement and private stakeholders will enable the City to better assess cyber threat levels and protect its residents from such threats; and

- NYC Cyber Command is mandated (via Executive Order 10) to set information security and policy standards for all City agencies, direct city-wide cyber defence and incident response, and coordinate with federal/state/private stakeholders.
- This includes reviewing cyber-related procurements, ensuring vendor compliance, and deploying administrative/technical controls across agencies.

2. Threat Intelligence & Incident Response

NEW ISSUE – BOOK-ENTRY ONLY

NEW YORK STATE

Environmental Facilities Corporation

RATINGS:

Fitch: AAA

Moody's: Aaa

S&P: AAA

\$717,295,000

NEW YORK STATE ENVIRONMENTAL FACILITIES CORPORATION

State Clean Water and Drinking Water Revolving Funds Revenue Bonds

(New York City Municipal Water Finance Authority Projects – Second Resolution Bonds) Series 2024 A Subordinated SRF Bonds

DATED: Date of Delivery

DUE: June 15, as shown on the inside cover

This cover page is only a brief general summary. You must read this entire official statement to obtain essential information for making an informed investment decision.

PURPOSES

We will use the proceeds of the State Clean Water and Drinking Water Revolving Funds Revenue Bonds (New York City Municipal Water Finance Authority Projects – Second Resolution Bonds) Series 2024 A Subordinated SRF Bonds (the “offered bonds”) to provide financial assistance to the New York City Municipal Water Finance Authority (the “Authority” or “NYCMWFA”) to finance or refinance water pollution control projects and drinking water projects and to refund certain bonds previously issued for water pollution control projects and drinking water projects.

THE OFFERED BONDS

Interest on the offered bonds is payable on June 15 and December 15 of each year commencing December 15, 2024. The offered bonds are issued in \$5,000 denominations. The DTC book-entry system will apply to all offered bonds, so you will not be registered as a bondowner. You will not receive physical delivery of certificates evidencing ownership of the offered bonds.

REDEMPTION

The offered bonds are subject to redemption prior to maturity as described herein.

SECURITY AND SOURCES OF PAYMENT

The offered bonds are our *special limited* obligations, payable *solely* from amounts pledged as security as described in this official statement. The offered bonds are issued as Subordinated SRF Bonds under the Master Trust Agreement. As security for the offered bonds, we have pledged: (i) repayments we receive on related bonds issued by the Authority; (ii) moneys available from time to time in the General Reserve Fund under the 2006 Indenture; and (iii) on a subordinated basis, moneys available from time to time in the De-allocated Reserve Account and the Deficiency Reserve Account after such moneys are applied, to the extent necessary, in connection with all Senior SRF Bonds secured by the Master Trust Agreement, as described in this official statement. The General Reserve Fund secures all bonds issued under the 2006 Indenture, including the offered bonds. Amounts available from the De-allocated Reserve Account and Deficiency Reserve Account secure the offered bonds on a parity basis with all other subordinated NYCMWFA bonds issued and outstanding and to be issued in the future, all as described herein.

TAX EXEMPTION

The offered bonds are not our general obligations and are not a charge against our general credit. The offered bonds are not a debt of the State of New York (the “State”), The City of New York (the “City”) or the Authority. We have no taxing power.

In the opinion of Ballard Spahr LLP and BurgherGray LLP, acting as our Co-Bond Counsel (“Co-Bond Counsel”), interest on the offered bonds is excludable from gross income for purposes of federal income tax, assuming continuing compliance with the requirements of federal tax law. Interest on the offered

- The organisation handles collection, ingestion and dissemination of cyber-threat intelligence for the city and coordinates incident response across agencies.
- It also monitors, investigates and responds to cyber-attacks affecting city infrastructure, prioritising remediation of vulnerabilities and unpatched systems.

### 3. Cross-Sector Collaboration & Partnerships

#### Cybersecurity

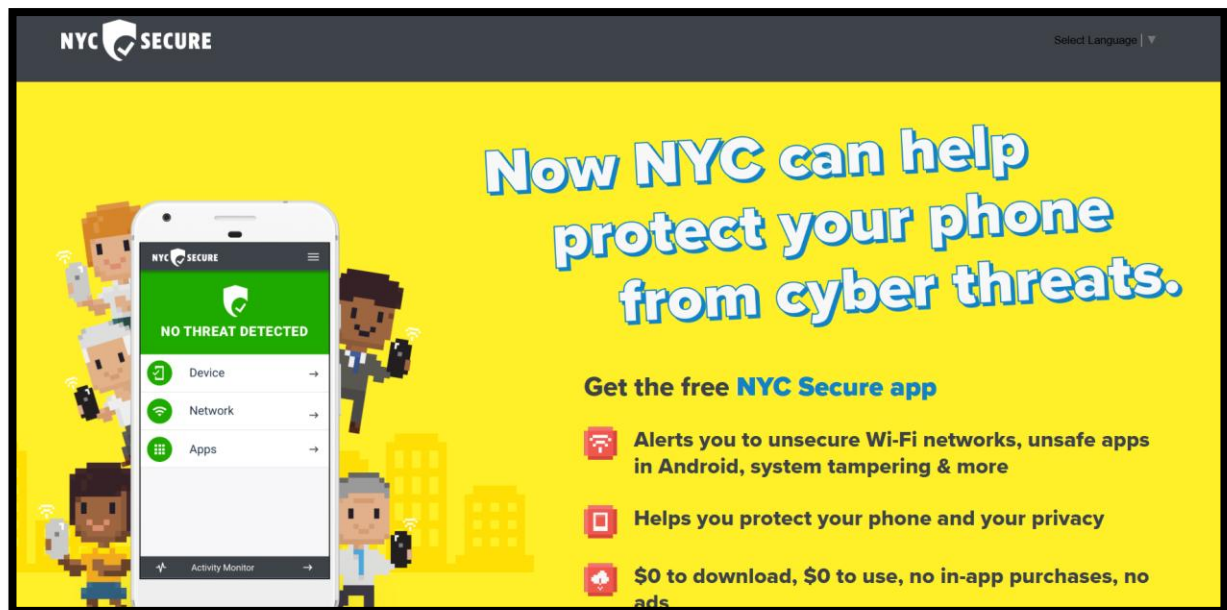
The System relies on a large and complex technological environment to conduct its operations. As a recipient and provider of personal, private or sensitive information, the System and the City, including DEP, face multiple cyber threats including, but not limited to, hacking, viruses, malware and other attacks on computers and other sensitive digital networks and systems. To protect the System from cyber-attacks, DEP, through its Bureau of Business Information Technology, works with a range of City, State, and federal law enforcement and technology agencies, including the City's Office of Technology and Innovation ("OTI") (formerly the Department of Information Technology and Telecommunications), the New York City Cyber Command ("NYC Cyber Command") and the Federal Bureau of Investigation's Joint Terrorism Task Force. NYC Cyber Command, which was created in 2017, is charged with setting information security policies and standards for the City for directing the City's citywide cyber defense and incident response, deploying defensive technical and administrative controls and providing guidance to the Mayor and City agencies, including DEP, on cyber defense. In January 2022, NYC Cyber Command became part of OTI. In addition, DEP works with other utilities around the country and is a member of various industry organizations, including the Water Information Sharing and Analysis Center (WaterISAC), the American Water Works Associations (AWWA), and the Water Environment Federation (WEF), to address cybersecurity risks and to share best practices surrounding cybersecurity.

NYC Cyber Command has over 100 full-time employees and works with designated cybersecurity contacts at each City agency as part of the Citywide Cybersecurity Program. The City's financial plan released in January 2024 reflects funding for Cyber Command of \$115.5 million in Fiscal Year 2024 and approximately \$105.5 million in each of Fiscal Years 2025 and 2026. Such funding does not account for cybersecurity funding at other City agencies, including DEP. NYC Cyber Command is built around two core cybersecurity functions: (1) threat management, which manages incident response and cyber threat intelligence and vulnerability management, which helps agencies prioritize remediation efforts on identified unpatched systems in the City's networks; and (2) security sciences, which manages strategic and tactical cyber defense technologies and initiatives.

In carrying out its functions, NYC Cyber Command works with a range of City, State, and federal law enforcement agencies, including the New York City Police Department and the Federal Bureau of Investigation's Joint Terrorism Task Force. In February 2022, the City and the State, along with the mayors of Albany, Buffalo, Rochester, Syracuse, and Yonkers, unveiled the Joint Security Operations Center. The center has enhanced coordination of cybersecurity efforts across the State, helping to foster collaboration among city, State, and federal entities. NYC Cyber Command also regularly works with other states and municipalities throughout the country to share cybersecurity threat intelligence and best practices, as well as with non-governmental entities such as utilities, telecommunications providers and financial services companies for the purpose of enhancing collective cyber defenses. The City has developed standard cybersecurity policies and standards for third party vendors of the City to follow, and security provisions for contracts with vendors, which help ensure that the City is notified of cyber breaches and suspected cyber breaches of a vendor's network environment. The City has also developed a Citywide Incident Response Policy, which requires City agencies to develop incident response plans in accordance with Cyber Command policies and standards.

- NYC Cyber Command liaises with federal, state and private partners (including law-enforcement agencies) to share intelligence, coordinate defence strategies, and unify response to large-scale threats.
- It also collaborates with other cities/states and municipal agencies to align standards, best practices and vendor oversight.

#### 4. Consumer-Facing Tools & Public Outreach



- Among its public-facing offerings is the “NYC Secure” mobile application, developed under the City’s cyber-strategy, which alerts users to device and network threats, contributing to citizen cyber-hygiene.
- Public outreach includes channels for tips and reports from the public regarding cybersecurity issues and avenues for non-agency stakeholders to engage with cyber-defence efforts

**Chatbot: No**

#### **Additional Pointers:**

- ☐ **Funding & Scale:** According to municipal documents, NYC Cyber Command employed over 100 full-time staff and had a fiscal plan budget of approximately USD \$115.5 million for FY 2024, and ~\$105.5 million for FY 2025-26.
- ☐ **Jurisdictional Scope:** While it serves City agencies primarily, its collaboration with state and federal partners means its remit extends beyond strictly municipal boundaries in coordinating cyber-defines for critical infrastructure.
- ☐ **Reporting Mechanisms:** Public tips can be submitted via the city website or through agency channels, although there is **no direct 311 public line** dedicated solely to Cyber Command.