Maria Sumnicht

Former: Urban Technology Architect
New York City Cyber Command

CEO: OT Governance

GSO 2025
Global Security Operations

Blank

SLATE

PROBLEM STATEMENT

Agencies deploying massive quantities of unvetted IoT Endpoint Technology and connecting them to New York City networks increasing the threat landscape while addressing legacy along the way.

END GOAL

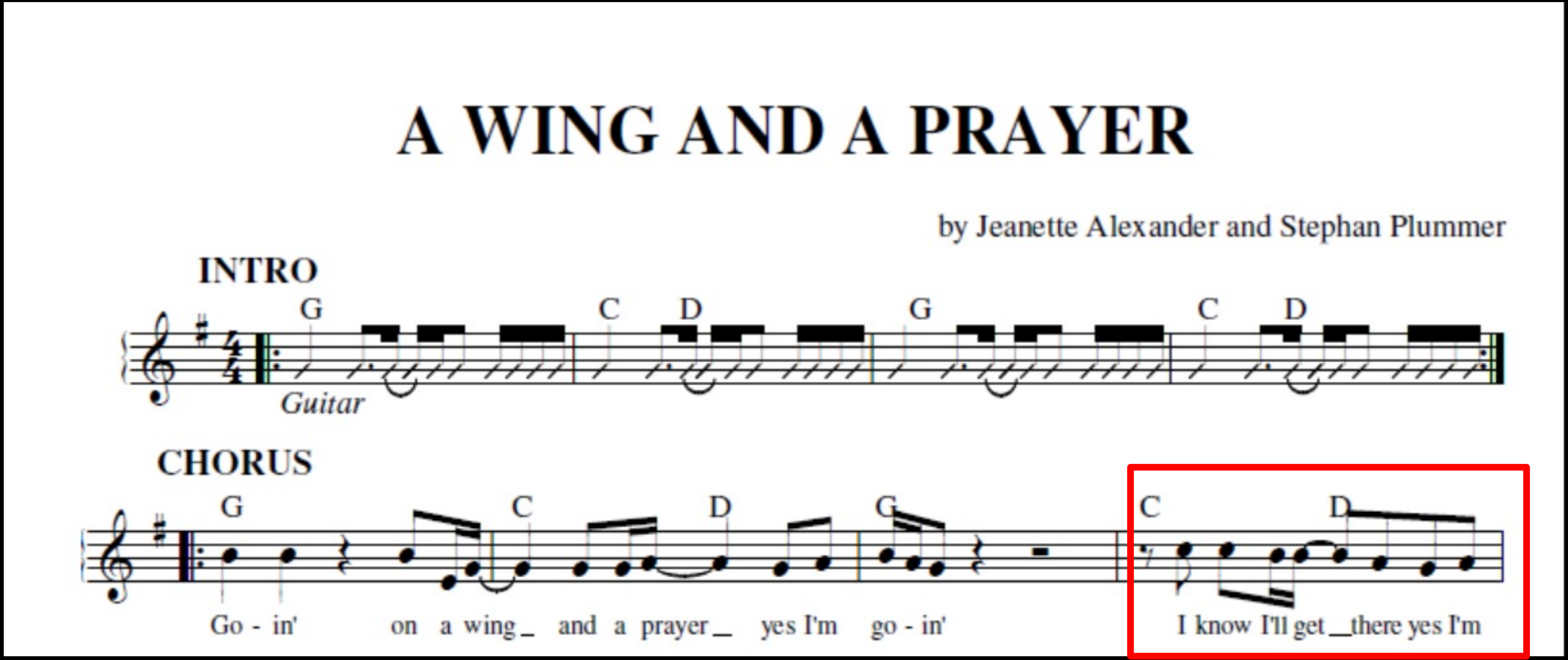
To ***PROACTIVELY*** secure & protect Endpoint Technology prior to their deployment on New York City networks.

Big Apple Challenges

- There was nothing done like this before on such a massive scale. It's NYC!
- Headcount -> hiring talent in highly competitive job market.
- Having a 'catch mechanism' for procurement of new & renewed IoT technology.
- Agencies thinking the program is a roadblock to their rapid deployment of technology.
- Inconsistent legal agreements for the purchasing of technologies – almost each agency had their own legal agreements/contracts.
- Educating Agencies on what exactly is IoT.
- The GREAT unknown – the existing IoT footprint:
  - What exactly is out there, how many and is it being supported contractually(legally)?
  - How to capture existing technologies and bring them into the process.
- How to automate inventory and monitoring IoT footprint in NYC.
- How to automate upgrades and certificate management of IoT networks.

Biggest Challenge

Budget Only $150,000.00



A WING AND A PRAYER

by Jeanette Alexander and Stephan Plummer

INTRO
G
C
D
G
C
D
Guitar
CHORUS
G
C
D
G
C
D
Go - in' on a wing_ and a prayer_ yes I'm go - in'
I know I'll get__there yes I'm

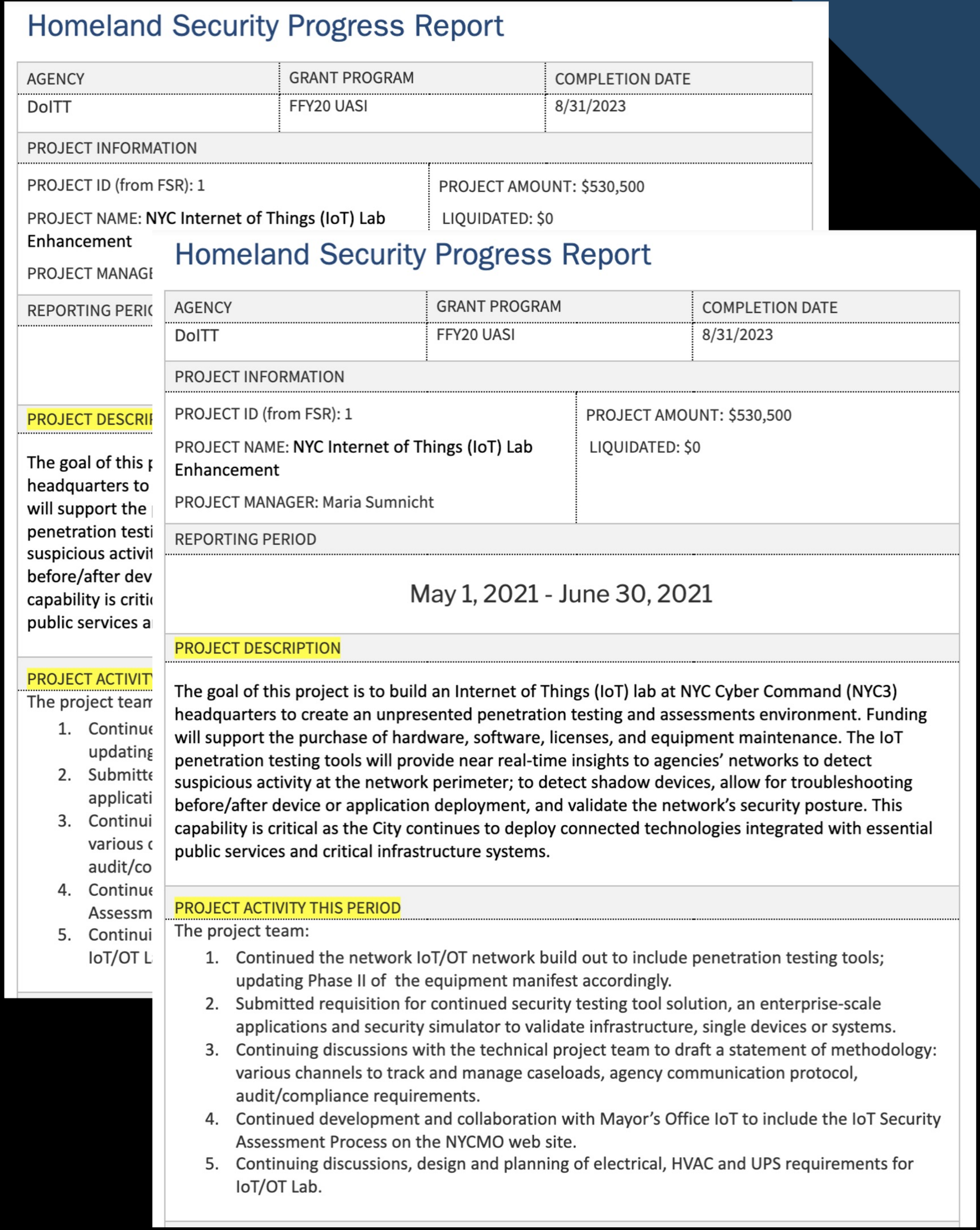
I Needed to FIND Money ASAP!

UASI GRANT

The Grant Writer for the City of New York was my new best friend!

IoT & ICS UASI Grant

IoT Total Grant Fund	$530,500.00
Phase I Lab Infrastructure	
Phase II Servers & Build Services	$155,000.00
Phase III Software & Pen Test Tools	$130,000.00
Phase IV Lab Interior Decorating	
ICS Total Grant Fund	$2.2M
Pen Testing of Critical Infrastructure	$1M
Procurement of Logging & Monitoring Tool	$1.2M



Homeland Security Progress Report

AGENCY	GRANT PROGRAM	COMPLETION DATE
DoITT	FFY20 UASI	8/31/2023

PROJECT INFORMATION

PROJECT ID (from FSR): 1

PROJECT AMOUNT: $530,500

PROJECT NAME: NYC Internet of Things (IoT) Lab Enhancement

LIQUIDATED: $0

Homeland Security Progress Report

AGENCY	GRANT PROGRAM	COMPLETION DATE
DoITT	FFY20 UASI	8/31/2023

PROJECT INFORMATION

PROJECT ID (from FSR): 1

PROJECT NAME: NYC Internet of Things (IoT) Lab Enhancement

PROJECT MANAGER: Maria Sumnicht

PROJECT AMOUNT: $530,500

LIQUIDATED: $0

REPORTING PERIOD

May 1, 2021 - June 30, 2021

PROJECT DESCRIPTION

The goal of this project is to build an Internet of Things (IoT) lab at NYC Cyber Command (NYC3) headquarters to create an unpresented penetration testing and assessments environment. Funding will support the purchase of hardware, software, licenses, and equipment maintenance. The IoT penetration testing tools will provide near real-time insights to agencies' networks to detect suspicious activity at the network perimeter; to detect shadow devices, allow for troubleshooting before/after device or application deployment, and validate the network's security posture. This capability is critical as the City continues to deploy connected technologies integrated with essential public services and critical infrastructure systems.

PROJECT ACTIVITY THIS PERIOD

The project team:

1. Continued the network IoT/OT network build out to include penetration testing tools; updating Phase II of the equipment manifest accordingly.
2. Submitted requisition for continued security testing tool solution, an enterprise-scale applications and security simulator to validate infrastructure, single devices or systems.
3. Continuing discussions with the technical project team to draft a statement of methodology: various channels to track and manage caseloads, agency communication protocol, audit/compliance requirements.
4. Continued development and collaboration with Mayor's Office IoT to include the IoT Security Assessment Process on the NYCMO web site.
5. Continuing discussions, design and planning of electrical, HVAC and UPS requirements for IoT/OT Lab.

National Urban Area Security Initiative Association

GSO 2025 Global Security Operations

Governance

- Developed "The Pillars" that would be the City of New York's IoT Cyber Resiliency Program.
- The directive existed, the 67 Mayoral Agencies through Executive Order No. 28, executed on July 11, 2017 established NYC Cyber Command.
  - Section 6. All agency and office heads are directed to cooperate with New York City Cyber Command.

LEGAL POLICY PROCUREMENT METRICS

The Pillars of
New York City’s IoT Cyber Resiliency Program

Governance

Challenge

- Co-operation from City Agencies and Offices who did not report to you.
- NYC is compromised of kingdoms within an empire. Many unique and colorful personalities.

Key Objectives

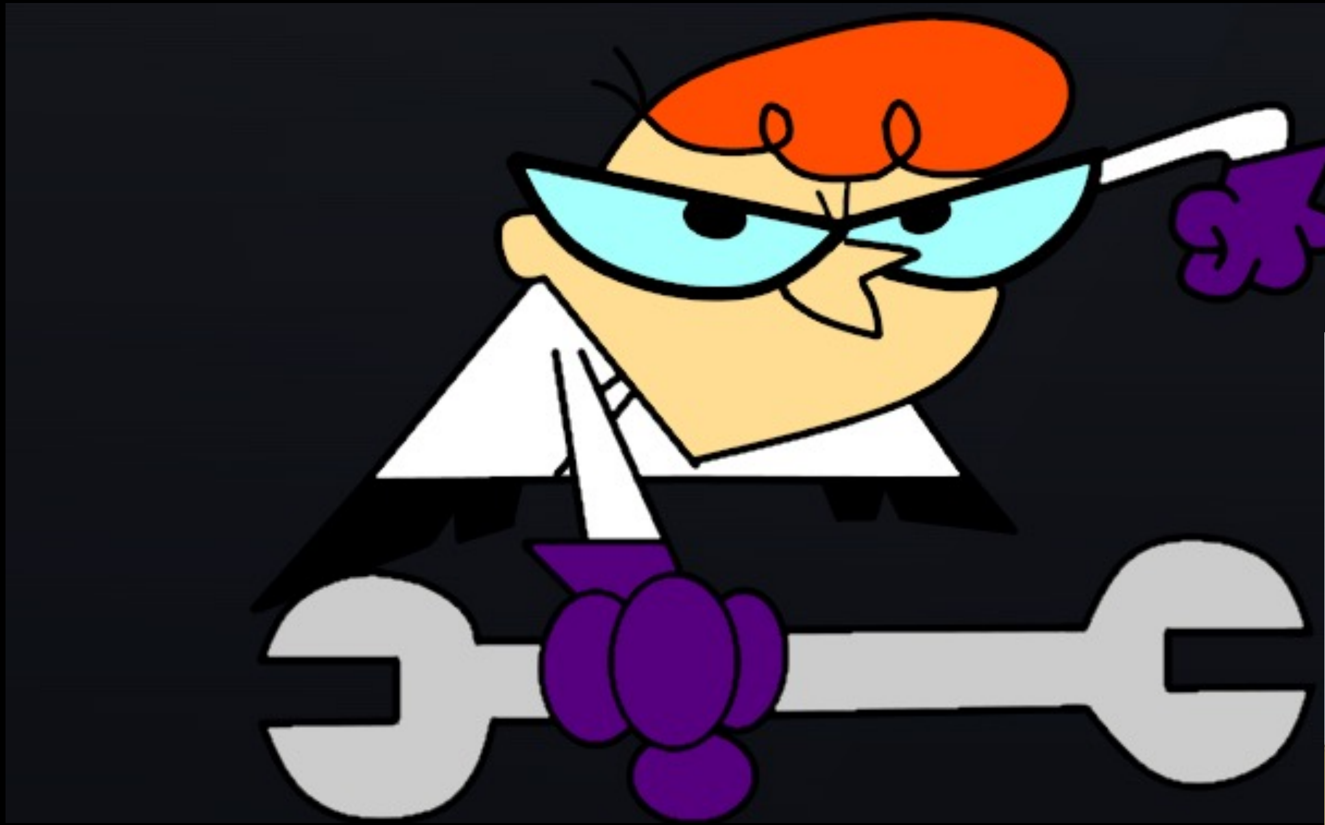
- Finding a reasonable and prudent path in order to get maximum agency buy in.
- Make and sustain reasonable and prudent governance decisions at all levels.
- Staying the course over time and adapting where and when necessary.
- End Game: Measuring and sustaining governance across NYC.

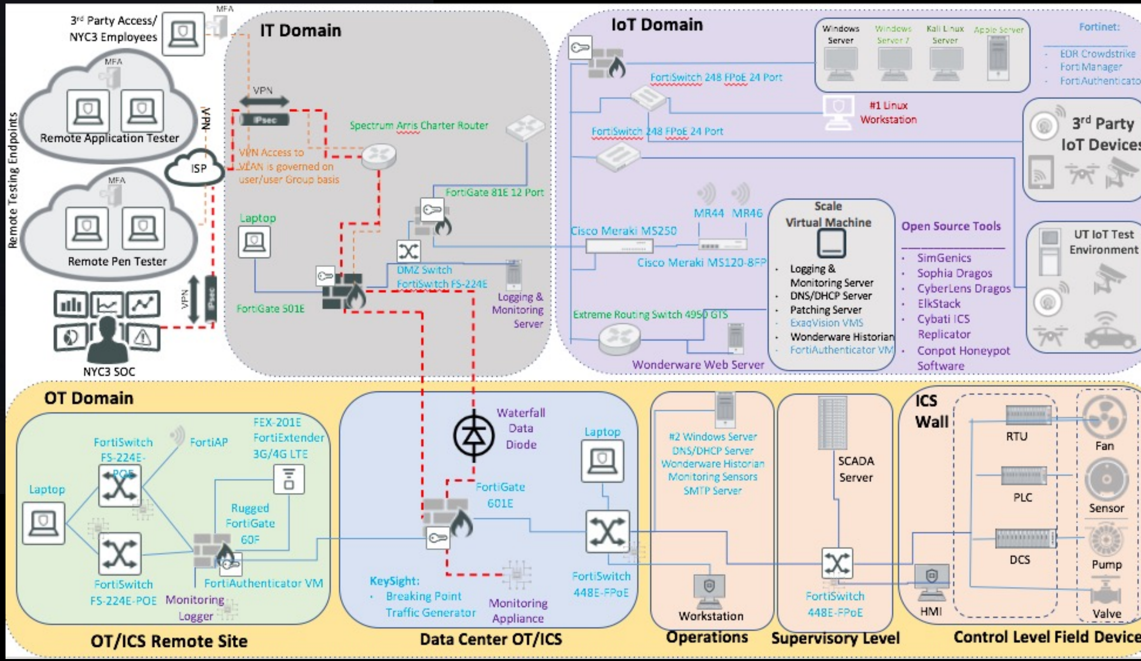
Pillar #1 - Legal

Established Consistent Legal Purchasing Agreements Across All Agencies for Technology Procurement

- End User License Agreement (EULA)
  - The EULA covers on-premise software, firmware, hardware (including connected devices).
- Cloud Services Agreement(CSA)
  - The CSA covers hosted services including, but not limited to, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). Both the EULA and the CSA are the City's licensing terms for purchasing these types of products.
- Penetration Testing Agreement (PTA)
  - The PTA is the City's terms for pen testing of connected devices and their management platforms. All Critical, High and Medium vulnerabilities must be remediated prior to deployment.
- Agency Risk Acceptance Agreement (ARAA)
  - Agency can accept risk of deploying IoT solutions without cyber security assessment. Agency accepts full responsibility.

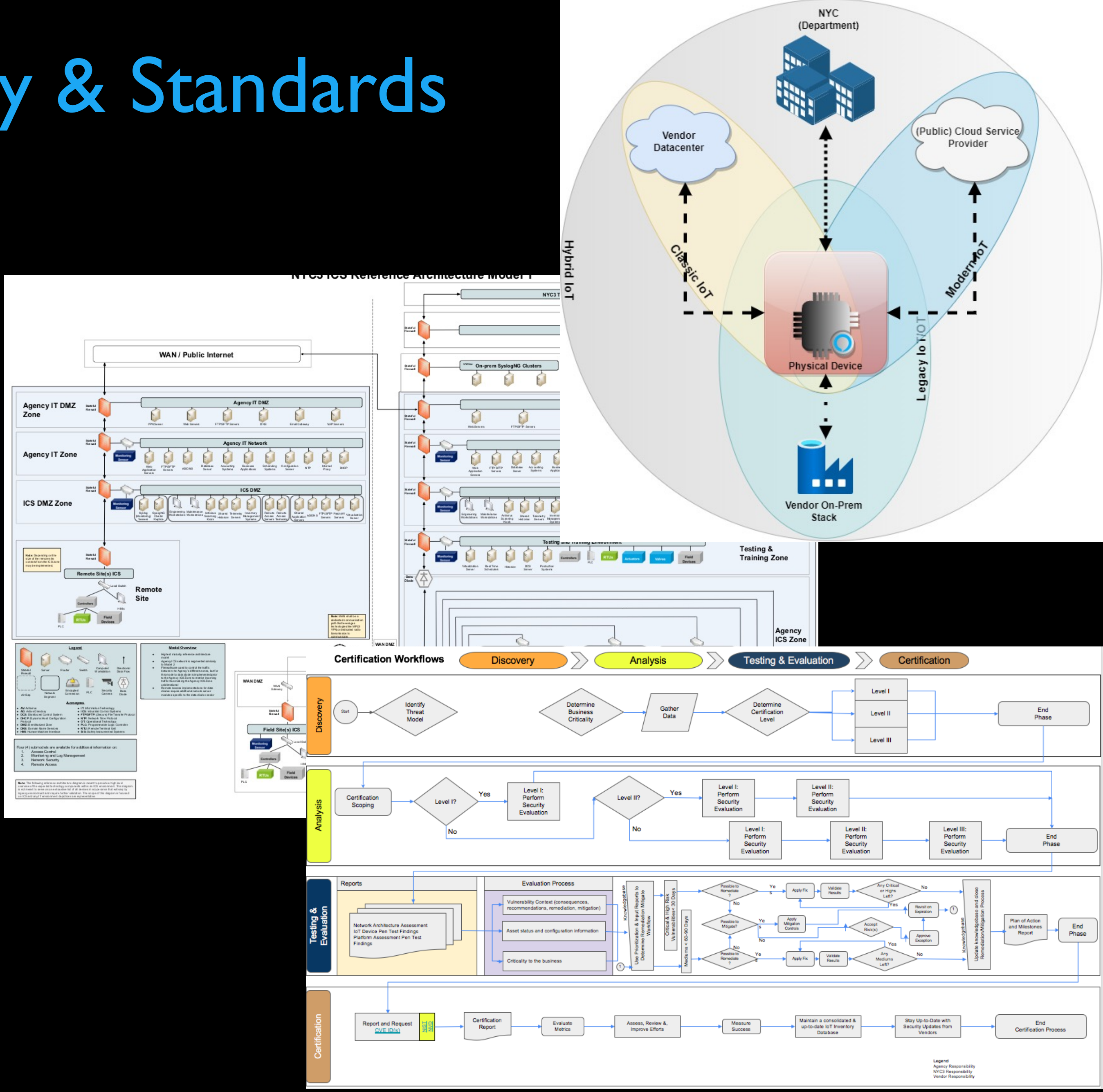
Design a IoT/ICS Red Team Cyber Resiliency Laboratory





Pillar #2 – Policy & Standards

- IoT & ICS Policy
- IoT & ICS Standards
- IoT Program Charter and Process
- IoT Threat Models
- IoT & ICS Reference Architecture(s)
- IoT Guidance
- IoT Citywide Strategy


NYC3 ICS Reference Architecture Model 1
WAN / Public Internet
Agency IT DMZ Zone
Agency IT DMZ
Agency IT Zone
Agency IT Network
ICS DMZ Zone
ICS DMZ
On-prem SyslogNG Clusters
Remote Site(s) ICS
Remote Site
Testing & Training Zone
Agency ICS Zone
WAN DMZ
Field Site(s) ICS
Field Devices
Legend
Model Overview
NYC (Department)
Vendor Datacenter
(Public) Cloud Service Provider
Hybrid IoT
Classic IoT
Modern IoT
Legacy IoT/OT
Physical Device
Vendor On-Prem Stack
Certification Workflows
Discovery
Analysis
Testing & Evaluation
Certification
Start
Identify Threat Model
Determine Business Criticality
Gather Data
Determine Certification Level
Level I
Level II
Level III
End Phase
Certification Scoping
Level I?
Yes
No
Level I: Perform Security Evaluation
Level II?
Level II: Perform Security Evaluation
Level III: Perform Security Evaluation
Reports
Network Architecture Assessment
IoT Device Pen Test Findings
Platform Assessment Pen Test Findings
Evaluation Process
Vulnerability Context (consequences, recommendations, remediation, mitigation)
Asset status and configuration information
Criticality to the business
Knowledgebase
Use Prioritization & Input Reports to Determine Remediation Mitigate Workflow
Critical & High Risk Vulnerabilities< 30 Days
Mediums < 60-90 Days
Possible to Remediate?
Possible to Mitigate?
Apply Fix
Validate Results
Apply Mitigation Controls
Any Critical or Highs Left?
Any Mediums Left?
Accept Risk(s)
Revisit on Expiration
Approve Exception
Update knowledgebase and close Remediation/Mitigation Process
Plan of Action and Milestones Report
Report and Request CVE ID(s)
NIST NVD
Certification Report
Evaluate Metrics
Assess, Review & Improve Efforts
Measure Success
Maintain a consolidated & up-to-date IoT Inventory Database
Stay Up-to-Date with Security Updates from Vendors
End Certification Process
Legend
Agency Responsibility
NYC3 Responsibility
Vendor Responsibility

Pillar #3 - Procurement

- Worked with Office of Management and Budget (OMB) to integrate new & renewal technology procurement into the IoT cyber security process.
- Worked with OMB to integrate existing technology upgrades, contracts and license renewals into the IoT/OT cyber security process.
- Developed a portfolio of IoT tested solutions which were shared with City Agencies.
- Integrate IoT cybersecurity process into existing Technology Review In-take process.
- Established checkpoint when cybersecurity process was completed OMB is notified, a release certificate is issued and vendors funds are released.

Pillar #4 - Metrics

- The UASI Grant kept us honest - had to document *EVERYTHING* spent and justify the spend down.
- Kept the metrics simple:
  - Number of vulnerabilities found.
  - Number of vulnerabilities remediated.
  - Number of IoT/OT devices tested.
  - Quantity of each IoT/OT device(s) deployed by Agency.
  - Number of IoT/OT management platforms tested.
  - Number of IoT/OT network security assessments performed.
  - Which agencies came through the program and tracked the trends in technologies being procured.

QUANTIFYABLE KEY SUCCESSES

Discovered

Performed 67 IoT Penetration Tests

- **54** of these were *Critical/High*
- **59** Medium
- **28** Low
- **18** Informational

Remediated

Verified and Remediated Vulnerabilities

- **54** of these were *Critical/High*
- **59** Medium
- **28** Low
- **17** Informational

159

IoT "**Zero-Day**" Vulnerabilities Found & Remediated Feb 2019 - Mar 2022

QUALITATIVE

The Value Proposition

Risk to NYC Agencies and their infrastructure.

REDUCED

Visibility into vulnerabilities and possible threats across IoT technology for all city agencies.

TIMELY

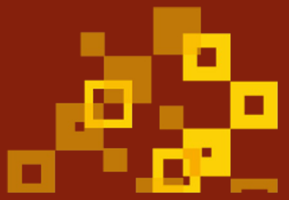
Monitoring, scanning and reporting on vulnerabilities for IoT network connected assets.

CONSISTENT

Ability to direct, inspect and measure compliance as recommended by industry best practices with NIST, CISA.

ENHANCED

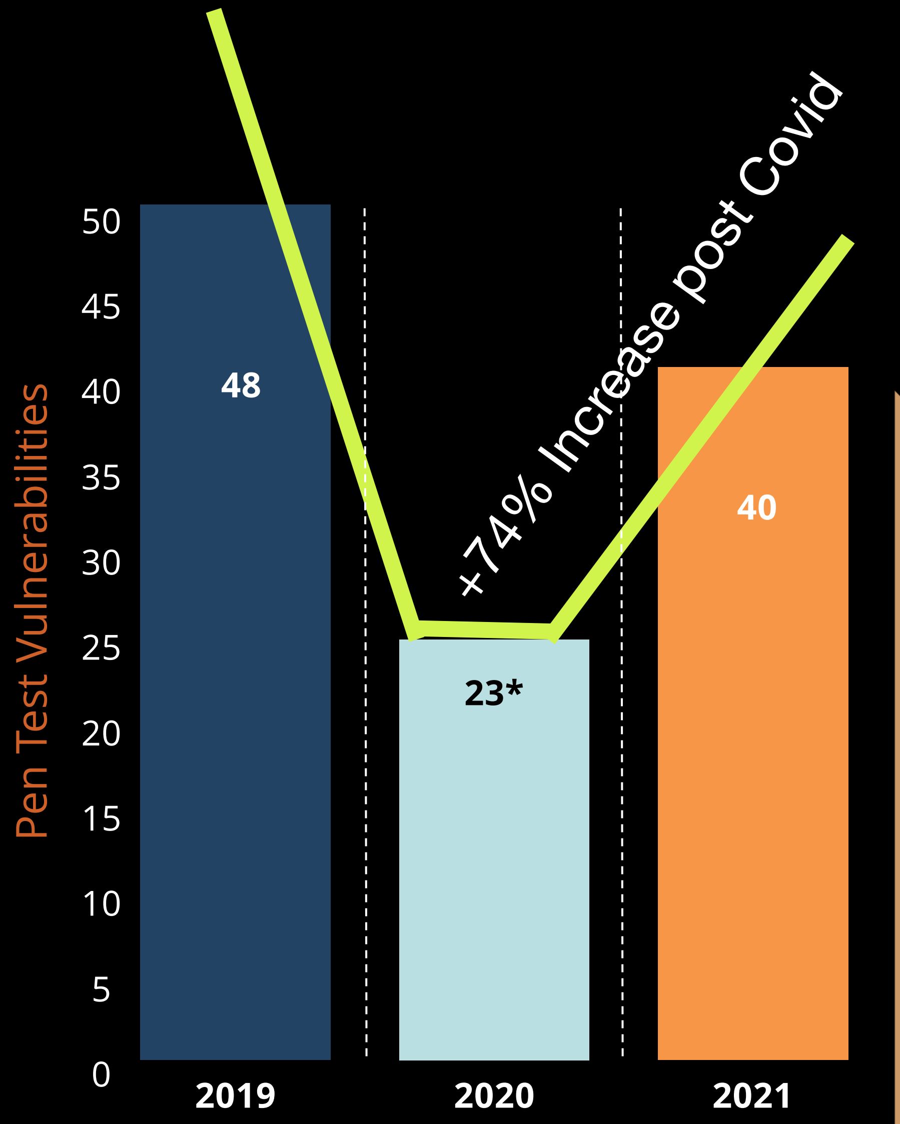
Deeper understanding of agency IoT footprints, workflows and priorities.



ALIGNMENT

Why ‘is’ the IoT Cyber Resiliency Program Important to NYC?

The Program Made NYC More Resilient?

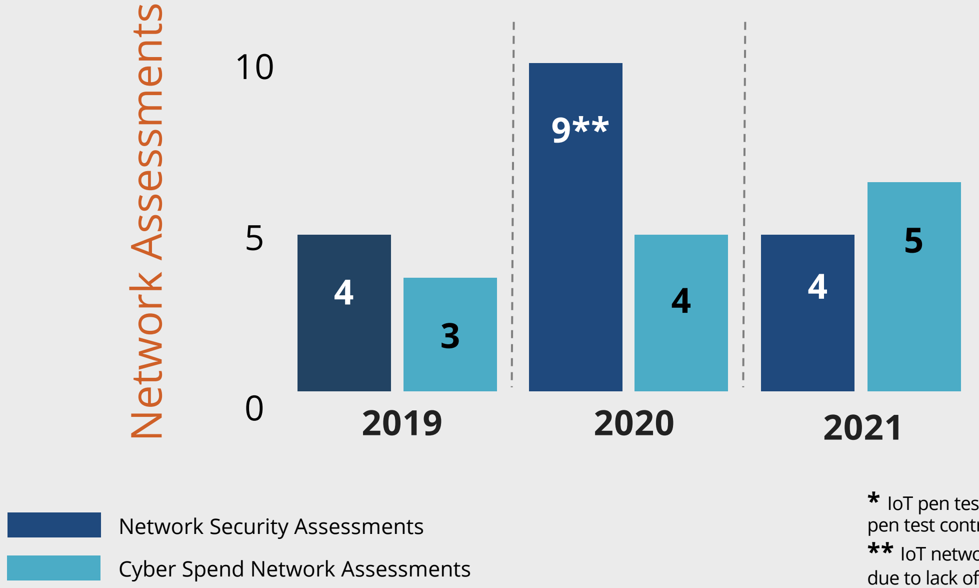


Enhanced Programs reputation across City Agencies and **Transformed** the way Agencies view IoT security & buy IoT.

Proactive security **testing** of IoT devices, their cloud-based management platforms & assessing their network end-to-end ***decreased*** *attack surfaces* on a '***massive scale.'***

Increased security posture of IoT by performing Threat Modeling and End-to-End network security assessments, measuring cyber resiliency against NIST Cybersecurity Framework 800.213.

METRICS



* IoT pen test decreased due to lack of pen test contract with 3rd party firm.

** IoT network assessments increased due to lack of a pen test contract in place with 3rd Party firm.

GSO 2025 Global Security Operations

PROACTIVELY SECURED

Massive Deployments of IoT

- **Board of Elections** over **50,000+** router/modems for remote voting locations.
- **DoP/MOCJ** over **10,000+** prisoner ankle monitors.
- **FDNY** over **20,000+** router/modem for vehicles and stations houses/HQ.
- **FDNY** over **15,000+** Phase 2 Channel 16 Radio Upgrade.
- **FDNY** over **15,000+** GPS Transponders/Locators for entire vehicle fleet.
- **NYPD** over 65,000 Motorola NextGen Apex radios.
- **NYPD/TLC** over 65,000 body worn cameras
- **DoT** over **14,500+** NYC parking meters.
- **DoT** over **15,000+** NYC traffic light controller router/modems.
- **DoE** over **30,000+** school bus & student GPS transponders/locators and tracking.
- **DSNY** over **20,500+** switches/routers/modems/Wi-Fi for sanitation/snow removal vehicle fleet.

Wins!

- Agencies began to include Cyber Command in the RFP/RFI process.
- Agencies coming to Cyber as SME's asking 'we are looking at solutions to do X, have you already tested a solution that we could look at?'
- Continuous Education: Created a quarterly forum where Agency CISO's and staff and presented their solutions, legal presented agreements and educated Agencies on their usage, procurement presented, and Cyber brought Agencies up to date on any known vulnerabilities and solutions.
- Considerably reduced the IoT threat landscape across NYC on a massive scale.

Links

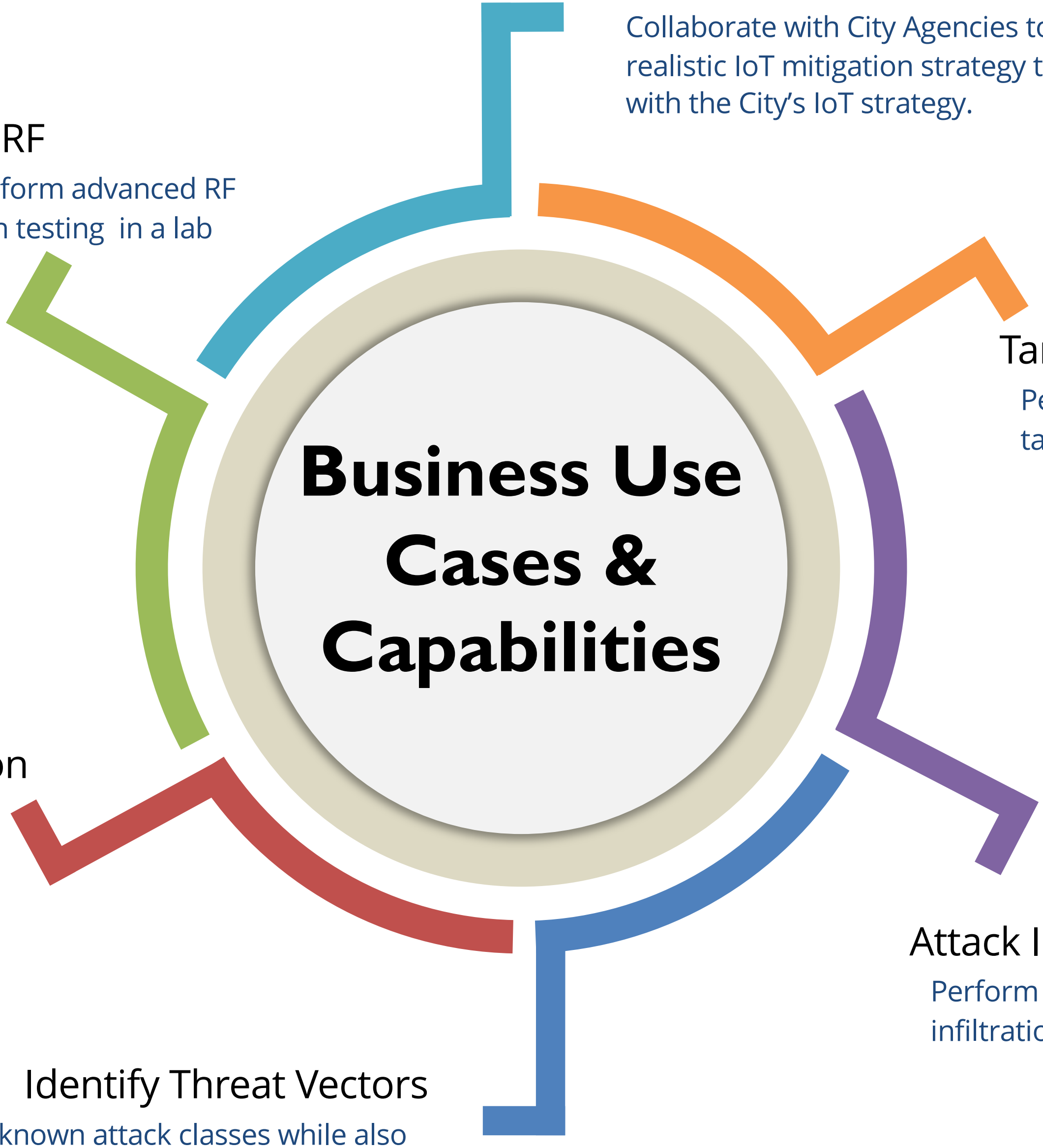
- IoT Process - https://blueprint.cityofnewyork.us/process/iot-network-security-assessment-process/
- IoT Guidelines - https://iot.cityofnewyork.us/#guidelines
- City of New York IoT Strategy - https://www1.nyc.gov/assets/cto/downloads/iot-strategy/nyc_iot_strategy.pdf

THANK YOU.

maria@otgovernance.com
(408) 914-1309
otgovernance.com

QUESTIONS?

maria@otgovernance.com
(408) 914-1309
otgovernance.com



Business Use Cases & Capabilities

Agency Collaboration

Collaborate with City Agencies to develop a realistic IoT mitigation strategy that is aligned with the City's IoT strategy.

Targeted Exfiltration Attacks

Perform exfiltration testing and targeted attack scenarios.

Attack Infiltration Attacks & Simulations

Perform goal-based attack simulation and infiltration.

Identify Threat Vectors

Identifying known attack classes while also finding new zero-day vulnerabilities.

Real World Attack Simulation

To perform real-world attack scenarios and develop advanced vulnerability research techniques.

Simulate & Test RF

To simulate and perform advanced RF network penetration testing in a lab environment.

New York City’s IoT Landscape 2018-2023

Trends in IoT Solutions

- Wireless Communications
- Sensors
- GPS Transponders
- Cameras
- Building Automation

IoT Footprint

~Number of IoT deployed in 3 yrs.

- FDNY ~70,000+
- DoT ~60,000+
- DoE ~30,000+
- DSNY ~20,000+
- DRP ~ 20,000+
- NYPD ~ 50,000+

Top IoT Consumers

- New York Police Department
- Department of Transportation
- New York Fire Department
- Parks & Recreation
- Department of Sanitation
- Office of Coroner/Medical Examiner