

A Report for the City of New York



NYCWiN Incident Assessment

April 30, 2019

This report has been redacted to remove information which, if disclosed, would jeopardize the City's capacity to guarantee the security of its information technology assets, such assets encompassing both electronic information systems and infrastructures.

This Report may contain information that is confidential, proprietary or otherwise legally protected. The contents of this report are the result of a rapid assessment conducted by Gartner that was based on the findings from interviews and documentation provided by the City of New York. Gartner makes no representation that it conducted a forensic technical assessment of NYCWiN nor a legal analysis of related contracts. The City of New York recognizes that the services are not a substitute for its own independent evaluation and analysis and do not constitute a recommendation to pursue a specific course of action. Gartner shall not be liable for any actions or decisions that the City of New York may take based on the services and/or any information or data contained herein.

Table of Contents

1.0 Executive Summary	1
2.0 Assessment Scope	5
3.0 Background	6
3.1 NYCWiN.....	6
3.2 Week Number Rollover	12
4.0 Timeline.....	15
5.0 Impact Summary	17
6.0 WNRO Incident Analysis	19
7.0 Incident Preparedness and Response	23
8.0 Conclusion.....	29
9.0 Appendix.....	30
9.1 Interviews Conducted.....	30
9.2 Glossary.....	32

1.0 Executive Summary

Overview

On April 6, 2019, the New York City Wireless Network (NYCWiN) experienced a networkwide service interruption. NYCWiN was not fully restored until April 17, 2019. NYCWiN supports public safety and other essential City operations with highly secure, real-time access to high-speed voice, video and data communications. This was the first NYCWiN-wide service interruption since the network became fully operational in 2009. Approximately 10 City agencies, including those responsible for public safety, regulatory and administrative functions, were impacted during the NYCWiN incident.

The incident was reportedly due to a GPS technology failure caused by the GPS Week Number Rollover (WNRO) event. GPS employs a week counter that enables receivers to calculate the appropriate date, which must be reset to zero every 1,024 weeks, or approximately once every 20 years (i.e., a WNRO event).¹ The WNRO event is similar in nature to the Y2K event.² The April 6 WNRO event was widely known and communicated, including notification by the U.S. Department of Homeland Security (DHS) in a memorandum published in April 2018.

Once NYCWiN was fully restored the City immediately recognized that the event warranted a detailed review by an independent third party. Gartner, Inc. was engaged to perform a rapid assessment of the NYCWiN incident. The core objectives of the assessment include:

- Providing a clear understanding of what transpired before and after the incident
- Identifying how City agencies were affected
- Providing recommendations to reduce the risk of an incident of this nature happening in the future

In the time allotted, Gartner conducted 51 interviews with City staff and NYCWiN vendors and reviewed documents provided by the City. Gartner also supplemented its review with publicly available information, specific research and best practices.

WNRO Incident Analysis

Based on the analysis, the NYCWiN incident could have been prevented by the timely update of the GPS component firmware at each of the NYCWiN Radio Access Network (RAN) sites. The fundamental question of how the WNRO event was overlooked, given the vital role GPS plays in the operation of NYCWiN, is not answered by a single factor but rather by the following key findings:

- **Finding 1.** Failure to replace NYCWiN in a timely manner resulted in a high degree of risk associated with end of life technology.

¹ U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, *GPS Week Number Roll Over (WNRO)*, <https://www.dhs.gov/cisa/gps-week-number-roll-over> (last accessed April 28, 2019).

² U.S. Library of Congress Business Reference Services, “The Year 2000:Y2K,” September 28, 2018, <http://www.loc.gov/rr/business/businesshistory/January/y2k.html> (last accessed April 28, 2019).

- **Finding 2.** The heavy reliance on the long-standing outsourced maintenance and support model was not counterbalanced by a consistent, well-executed vendor management discipline within DoITT.
- **Finding 3.** [REDACTED]
- **Finding 4.** The WNRO event was known by multiple agencies.

Incident Preparedness and Response

While multiple agencies use NYCWiN, the Department of Information Technology and Telecommunications (DoITT) is the designated responsible agency for NYCWiN. DoITT manages the City's long-standing contractual agreement with Northrop Grumman (NG) to operate, support and maintain the network. The following findings provide insight into NYCWiN preparedness and the incident response:

- **Finding 5.** DoITT devoted limited attention to NYCWiN continuity of operations and emergency planning.
- **Finding 6.** [REDACTED]
- **Finding 7.** Joint engagement among DoITT, NYC3, NYCEM and NG was limited and unstructured as it relates to NYCWiN incident preparedness.
- **Finding 8.** NG did not promptly notify DoITT when it first detected the NYCWiN service interruption.
- **Finding 9.** [REDACTED]
- **Finding 10.** A clear decision-making and communication structure was not promptly established during incident response.
- **Finding 11.** Limited data analytics in the early stages of the incident hindered response effectiveness and decision-making.
- **Finding 12.** [REDACTED]
- **Finding 13.** DoITT has yet to issue a formal post-incident report.

Recommendations

While this review was limited in scope and timing, its findings indicate that the City may be exposed to more risk than necessary regarding technology-related incidents and the disposition of critical infrastructure. The following recommendations serve as a starting point to address many of the findings:

- **Recommendation 1.** Finalize the decommissioning of NYCWiN as soon as possible by mandating that all remaining agencies migrate either to CCEWiN or an alternative by a firm, established deadline.
- **Recommendation 2.** Develop a comprehensive Citywide inventory of all end of life hardware and software assets associated with critical infrastructure in the next 30 days and create a risk based assessment for asset risk mitigation, contingency planning and asset upgrade.

- **Recommendation 3.** Institute an ongoing process for identifying, classifying and prioritizing end of life assets that provide critical NYC capabilities and issue regular reports on progress to City Hall.
- **Recommendation 4.** All vendors maintaining systems that provide critical NYC capabilities (or “critical functions”³ as defined by DHS) must provide periodic attestation to the City that all patches and configuration changes are current, along with a forecast for upcoming required changes in the next 12 months.
- **Recommendation 5.** [REDACTED]
- **Recommendation 6.** Require regular, structured engagement on preparedness between parties operating critical technologies, including DoITT, NYC3, NYCEM and any involved vendors.
- **Recommendation 7.** The City should evaluate the circumstances and thresholds where NYCEM is put in charge, or takes over, an incident response.
- **Recommendation 8.** Require all necessary capabilities and equipment potentially required to service critical technology in the event of an incident, to be locally available whether the provider is the City or a vendor.
- **Recommendation 9.** [REDACTED]
- **Recommendation 10.** Require standardized incident response procedures across City agencies and vendors that are consistent with Citywide Incident Management System (CIMS) protocols and enforce their use in response to incidents.
- **Recommendation 11.** [REDACTED]
- **Recommendation 12.** Perform a detailed business impact analysis on all identified critical City technology infrastructure to understand the consequences of a disruption and gather the requisite information needed to develop robust recovery strategies.
- **Recommendation 13.** Establish a critical technology task force to update all emergency and continuity of operations plans, as well as to evaluate preparedness in detail.

The recommendations provided in this report serve as a starting point. Beyond the initial recommendations, it is essential that the City take immediate action to examine preparedness regarding all its critical technology infrastructure, in-process projects and any related assets, including those that may be operated in whole or part by vendors on behalf of the City. Moreover, it is recommended that any technologies critical to public safety, such as

³ DHS CISA, “National Critical Functions Initiative,” Definition of National Critical Functions, <https://www.dhs.gov/cisa/national-critical-functions-initiative> (last accessed April 29, 2019).

NextGeneration 911,⁴ be among those prioritized for review. This incident serves as a signal to increase focus on critical technology infrastructure preparedness and response.

Finally, while this report identifies several issues regarding the NYCWiN incident, it is important to note that many City agencies and personnel actively worked together to restore NYCWiN as quickly as possible for the benefit of all New Yorkers.

⁴ DoITT, “Department of Information Technology and Telecommunications Commences NextGeneration 911 Project,” DoITT Press Releases, July 13, 2017, <https://www1.nyc.gov/site/doitt/about/press-releases/nextgeneration-911-project.page> (last accessed April 29, 2019).

2.0 Assessment Scope

The scope of this assessment is focused on the NYCWiN incident. The incident was reportedly due to the expected WNRO event of the U.S. Federal government Global Positioning System (GPS) (to which devices and computer networks of both commercial and public sector entities connect to around the world). Following the beginning of the incident on Saturday, April 6, the City worked to restore NYCWiN and full pre-incident connectivity was restored on Wednesday, April 17. The assessment is based on the WNRO event, the preparations and awareness of the WNRO event, and the immediate recovery period thereafter.

The objectives of this assessment are to provide a clear understanding of what transpired before and after the incident, identify how City agencies were affected and provide recommendations to significantly reduce the risk of an incident of this nature happening in the future.

Between Friday, April 19, and Monday, April 29, 51 interviews were conducted. Agencies and entities interviewed include the following in alphabetical order:

- Fire Department of the City of New York (FDNY)
- General Dynamics (GD)
- New York City Cyber Command (NYC3)
- New York City Department of Citywide Administrative Services (DCAS)
- New York City Department of Environmental Protection (DEP)
- New York City Department of Information Technology and Telecommunications (DoITT)
- New York City Department of Parks and Recreation (Parks)
- New York City Department of Sanitation (DSNY)
- New York City Department of Transportation (DOT)
- New York City Emergency Management (NYCEM)
- New York City Police Department (NYPD)
- Northrop Grumman (NG)
- Office of the Mayor of New York City

This assessment, including the findings and recommendations, are based on these interviews, as well as available documentation that was requested and provided during the assessment.

3.0 Background

This section provides context for analysis of the NYCWiN incident, including the history and current state of NYCWiN, and a description of the WNRO event issue.

3.1 NYCWiN

NYCWIn Origins (2001-2006)

After 9/11, NYC government assessed and determined opportunities for improvement of emergency operations — including increasing inter- and intra-agency communications capabilities. These and other assessments after storms and blackouts⁵ led to DoITT's March 2004 issuance of a Request for Proposals (RFP) for a Citywide Mobile Wireless Network. It was “aimed at addressing the City’s critical need for a high-speed network to provide advanced, interoperable data communications among and across key agencies.”⁶ The RFP effort included “a collaborative process of developing robust technical requirements and network specifications that included the Police Department, Fire Department, Office of Emergency Management, the Department of Transportation and DoITT.”⁷ The contract resulting from the RFP was entered into with Northrop Grumman Information Technology, Inc. in January of 2006.⁸

NYCWIn Launch (2007-2009)

Known as NYCWiN, the New York City wireless network began to be rolled out in lower Manhattan in January 2007, with testing related to “public safety and public service applications on the network.” On February 25, 2008 in testimony to City Council committees, the DoITT

⁵ The initial RFP was not available, though there has been reporting connecting NYCWiN to 9/11 and other significant City events. See, for example, Matthew Furman, “StateTech Interview With New York City CIO Carole Post,” *StateTech Magazine*, January 23, 2012, <https://statetechmagazine.com/article/2012/01/statetech-interview-new-york-city-cio-carole-post> (last accessed April 28, 2019); Matthew Harwood, “Rough Waters, Smooth Response,” *Security Management*, October 2010, <https://sm.asisonline.org/Pages/Rough-Waters-Smooth-Response.aspx> (last accessed April 28, 2019); Urgent Communications Administrator, “NYC operates government-only mobile broadband network,” *IWCE’s Urgent Communications*, February 15, 2011, <https://urgentcomm.com/2011/02/15/nyc-operates-government-only-mobile-broadband-network/> (last accessed April 28, 2019).

⁶ Paul Cosgrave, “Department of Information Technology and Telecommunications Testimony Before the City Council Committees on Fire and Criminal Justice Services, Public Safety, and Technology in Government Oversight — Implementation Status of the New York City Wireless Network,” New York City Council Committee Testimony, February 25, 2008, page 1, <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=448008&GUID=211DCE27-9A1A-420E-A77F-F706E3739073&Options=&Search=> (last accessed April 28, 2019).

⁷ Ibid.

⁸ Citywide Mobile Wireless Network Agreement by and between the City of New York Department of Information Technology and Telecommunications and Northrop Grumman Information Technology, Inc. (CT85820070008229).

Commissioner Paul Cosgrave described NYCWiN as “the most aggressive commitment by any municipality in the country to provide a next-generation public safety network.”⁹

Commissioner Cosgrave said NYCWiN “will give first responders high-speed data access to support large file transfers, including federal and state anti-crime and anti-terrorism databases, fingerprints, mug shots, city maps, automatic vehicle location, and full-motion streaming video” and “will enhance coordination by linking first responder personnel, on-scene, with incident managers at remote sites through real-time data and video feeds.” Commissioner Cosgrave went on to say that NYCWiN’s “role in improving the daily delivery of non-emergency City services will also be transformative” and “will support a range of additional public service applications, providing substantial improvements over existing technologies for the City’s mobile workforce by automating and streamlining time-consuming transactions and processes.”¹⁰

At the same hearing, Northrop Grumman Information Technology Vice President Sam Abbate testified. In addition to benefits discussed by Commissioner Cosgrave which Mr. Abbate generally referred to as the first “transformational impact,” Mr. Abbate also noted that NYCWiN would have a second transformational impact: “[I]t will extend the reach and capabilities of the City’s existing infrastructure.” Mr. Abbate stated, “This means that the City can wirelessly enable its existing infrastructure to better leverage its capital investments,” and “that as new challenges result in new infrastructure, that infrastructure can be remotely monitored and managed through NYCWiN.”¹¹

Commissioner Cosgrave noted that the initial launch of the network throughout the City would occur in April 2008, covering 70% of the City’s police precincts and fire houses, with 95% of the City to be covered by the end of the summer, and the rest by the end of 2008. He said, “NYCWiN will consist of 400 network sites throughout the five boroughs, managed from two fully-redundant network operation centers, which have already been completed, protected with 24-hour generation backup power, linked via multiple diverse fiber circuits, and staffed around the clock with technical support from the vendor.” He also noted, “DoITT will be dedicating nine staff members to full-time operational support of City agencies running applications on the network,” and said “unlike commercial networks, NYCWiN is designed for greater reliability, resiliency and redundancy.”¹²

Commissioner Cosgrave noted that “some 53 applications across 19 agencies are planned or in trial on NYCWiN,” providing examples of how City agencies such as NYPD and FDNY would use NYCWiN to gain “real-time access to vital information” and how data from the field could be coordinated with operations centers for agencies. The beginning of deployment of wireless vehicle modems, wireless traffic control modems, “handheld units for agencies conducting

⁹ Cosgrave, “Department of Information Technology and Telecommunications Testimony Before the City Council Committees on Fire and Criminal Justice Services, Public Safety, and Technology in Government Oversight — Implementation Status of the New York City Wireless Network,” pages 1-2.

¹⁰ Ibid.

¹¹ Sam Abbate, “Northrop Grumman Information Technology Vice President Sam Abbate, New York City Council Testimony on: The New York City Wireless Network (NYCWiN),” New York City Council Committee Testimony, February 25, 2008, pages 1-2, <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=448008&GUID=211DCE27-9A1A-420E-A77F-F706E3739073&Options=&Search=> (last accessed April 28, 2019).

¹² Cosgrave, “Department of Information Technology and Telecommunications Testimony Before the City Council Committees on Fire and Criminal Justice Services, Public Safety, and Technology in Government Oversight — Implementation Status of the New York City Wireless Network,” page 2.

enforcement and inspection activities in the field” and wireless cards for City agencies’ mobile staff would occur soon after the April 2008 initial launch, according to the testimony.¹³

The City formally announced NYCWiN was “operational citywide” in May 2009, noting that Northrop Grumman and IPWireless had worked to deploy the network.¹⁴ The press release stated, “The development of NYCWiN represents a major accomplishment and opportunity to transform the way New York City government operates, by improving the capabilities and efficiency of public safety and service agencies’ said Tom Shelman, vice president and general manager of Northrop Grumman Information Systems’ Civil Systems Division. ‘NYCWiN is a model for how states, cities, and counties can deploy and manage their own mission-critical communications infrastructure.’”¹⁵

As launched, NYCWiN was — and still is — a wireless network providing coverage throughout the five boroughs using “a cellular based architecture with radio access nodes [REDACTED]

[REDACTED] NYCWiN provides voice, video and data communications to support public safety and other public service City agencies, including enabling field operations on both laptops and handheld devices and secure transmission of data.¹⁹ It provides “street level” wireless communications and connects through CityNet to back-end City systems.²⁰

NYCWiN Growth (2009–2015)

The City continued to increase usage of NYCWiN, identifying agency needs and allocating applicable funding (for example, capital funding for DOT traffic signals).²¹ By May 2010, 20 agencies were using NYCWiN.²²

¹³ Id., pages 2-3.

¹⁴ DoITT, “Department of Information Technology and Telecommunications and Northrop Grumman Corporation Announce the New York City Wireless Network is Operational Citywide,” DoITT Press Releases, May 19, 2009, <https://www1.nyc.gov/site/doitt/about/pr-090519.page> (last accessed April 28, 2019). Note that IPWireless, “a San Francisco-based provider of 3G and 4G LTE wireless broadband network equipment and solutions for public safety and military customers,” was acquired in 2012 by General Dynamics. General Dynamics, “General Dynamics Completes Acquisition of IPWireless,” General Dynamics Press Releases, <https://www.gd.com/news/press-releases/2012/06/general-dynamics-completes-acquisition-ipwireless> (last accessed April 28, 2019).

¹⁵ DoITT, “Department of Information Technology and Telecommunications and Northrop Grumman Corporation Announce the New York City Wireless Network is Operational Citywide.”

¹⁶ DoITT, “Request for Expressions of Interest and Information (RFEI) on New York City Wireless Network (NYCWiN) Operations and Maintenance Services,” March 4, 2015, page 3, <https://www1.nyc.gov/assets/doitt/downloads/pdf/rfei/nycwin-ops-maint.pdf> (last accessed April 28, 2019).

¹⁷ However, the number of active transmitters is currently approximately [REDACTED] based on interviews with the City and Northrop Grumman.

¹⁸ DoITT, “NYCWiN.”

¹⁹ Ibid.

²⁰ DoITT, “Request for Expressions of Interest and Information (RFEI) on New York City Wireless Network (NYCWiN) Operations and Maintenance Services,” page 3.

²¹ New York City Council Finance Division, “Hearing on the Mayor’s Fiscal Year 2011 Executive Budget Department of Information Technology & Telecommunications,” New York City Council Finance Division

On March 8, 2012, DoITT Commissioner Carole Post, who succeeded Commissioner Cosgrave, testified to City Council committees:

Use of NYCWiN has increased by 40% each year since its launch. Over the next two years, another 60,000 devices and 10,000 users are planned to be added to the network, including 500 personal radiation detectors for the NYPD and at least 1,000 more mobile modems for the NYPD and FDNY. Today, there are nearly 800,000 devices and 10,000 users powering more than 300 applications across 29 City agencies on NYCWiN, running millions of wireless transactions over the network daily.²³

However, during this period,²⁴ the City reportedly began to evaluate the benefits²⁵ and costs of operating NYCWiN, including negotiating for savings in the first renewal contract for support of the network²⁶ and considering whether selling the network was a viable option.²⁷

Defining NYCWiN's Future (2015–2018)

In March 2015, the City made official that it had begun to consider the future of NYCWiN; it released a Request for Expressions of Interest and Information (RFEI) on NYCWiN Operations and Maintenance Services. The RFEI noted:

The operational models currently being considered are:

- 1) A City owned and vendor managed NYCWiN operational model for operations and maintenance (O&M) services. This is the current operational model in place.

Briefing Paper, May 25, 2010, pages 1, 7, 11 and 12, https://council.nyc.gov/budget/wp-content/uploads/sites/54/2017/01/fy2011-doitt_exec_rpt_2011.pdf (last accessed April 28, 2019).

²² Id., page 7.

²³ Carole Post, "Department of Information Technology and Telecommunications Testimony Before the City Council Committees on Land Use and Technology Fiscal Year 2013 Preliminary Budget," New York City Council Testimony, March 8, 2012, page 2, https://www1.nyc.gov/assets/doitt/downloads/pdf/testimony_fiscal_2013_prelim_budget_3_8_12.pdf (last accessed April 28, 2019).

²⁴ Interviews with the City and Northrop Grumman conducted in preparation of this report included discussion that the City was concerned about the cost of NYCWiN and considering decommissioning it as early as 2010.

²⁵ The New York Times suggested that Commissioner Post left her position in part due to challenges with IT projects and programs including "a shortage of users for NYCWiN [sic]." David M. Halbfinger and Michael M. Grynbaum, "City's Top Technology Official Resigns Amid Clashes Over Troubled Projects," *The New York Times*, April 13, 2012, <https://www.nytimes.com/2012/04/14/nyregion/new-yorks-top-technology-official-carole-post-resigns.html?searchResultPosition=3> (last accessed April 28, 2019).

²⁶ For example, compare Citywide Mobile Wireless Network Agreement by and between the City of New York Department of Information Technology and Telecommunications and Northrop Grumman Information Technology, Inc., Attachment PRC (CT85820070008229), to First Renewal Agreement by and between the City of New York Department of Information Technology and Telecommunications and Northrop Grumman Systems Corporation, Attachment PRC (CT85820111445466).

²⁷ Juan Gonzalez, "City to Contractor: Pretty Please, Could You Take Back This Great \$549 Million Wireless Network?," *New York Daily News*, February 15, 2012, <https://www.nydailynews.com/news/city-contractor-pretty-back-great-549-million-wireless-network-article-1.1022853> (last accessed April 28, 2019).

- 2) A transfer of ownership of the current NYCWiN infrastructure and operations to a third party. The third party would provide a lease or charge back model to the City.
- 3) A complete transfer of users and services from the current NYCWiN network to a carrier network or carrier-like network/service.

Additionally, the City of New York is interested in recommendations to develop and expand upon the citywide broadband infrastructure and to improve access to high-speed Internet for residents and visitors.²⁸

While the RFEI generated responses, “none were deemed suitable,” and DoITT continued to review options, including possibly “sun setting’ of this system.”²⁹

In 2017, DoITT decided to move forward with transitioning agencies off of NYCWiN largely to commercial carriers, as described by DoITT Commissioner Anne Roest in her FY 2018 Executive Budget testimony:

In future fiscal years, there will also be tens of millions in annual savings through the decommissioning of the New York City Wireless Network (NYCWiN). NYCWiN is our government-dedicated broadband wireless infrastructure, which was created to support essential City operations. As you know, we’ve been trying to find savings for NYCWiN since I became Commissioner, which costs the City over \$40 million a year in operations and maintenance costs. To that end, DoITT released an [RFEI] to gather ideas on ways to more efficiently use the network, but none of the responses offered a cost-effective solution. At this point, NYCWiN will only get more expensive, requiring hundreds of millions in upgrades in the near future simply to maintain the existing network. Therefore, as a matter of financial prudence we have decided to transition agencies from NYCWiN to commercial carriers. This should reduce the cost to less than \$10 million a year, saving the City more than \$30 million annually in future fiscal years. We are actively working with all agencies to ensure a smooth and seamless transition.³⁰

To support the announced decommissioning of NYCWiN, funding began to be allocated to DoITT and City agencies in order to help meet their specific needs.³¹

²⁸ DoITT, “Request for Expressions of Interest and Information (RFEI) on New York City Wireless Network (NYCWiN) Operations and Maintenance Services,” March 4, 2015, page 1. Interviews performed in preparation of this report indicated that the City had been considering what to do with NYCWiN, including perhaps decommissioning it, as early as 2010.

²⁹ New York City Council Finance Division, “Report on the Fiscal 2017 Executive Budget Department of Information Technology & Telecommunications,” New York City Council Finance Division Briefing Paper, May 19, 2016, page 6, <https://council.nyc.gov/budget/wp-content/uploads/sites/54/2016/06/doitt.pdf> (last accessed April 28, 2019).

³⁰ Anne Roest, “Testimony of Anne Roest Commissioner, New York City Department of Information Technology & Telecommunications Before the New York City Council Committees on Finance, Technology and Land Use Concerning the FY 2018 Executive Budget,” New York City Council Committee Testimony, May 18, 2017, page 2, <https://www1.nyc.gov/assets/doitt/downloads/pdf/FINAL%20DoITT%20FY18%20Exec%20Budget%20Testimony.pdf> (last accessed April 28, 2019).

³¹ See for example, New York City Council Finance Division, “Report to the Committee on Finance and the Committee on Technology on the Fiscal 2019 Executive Budget for the Department of Information Technology and Telecommunications,” Finance Division Briefing Paper, May 8, 2018, pages 1, 3, 4, 5 and 9, <https://council.nyc.gov/budget/wp-content/uploads/sites/54/2019/02/858-DoITT.pdf> (last accessed April 28, 2019); and New York City Council Finance Division, “Report of the Finance Division on the Fiscal

NYCWiN Today (2018-Present Day)

Under DoITT Commissioner Samir Saini, NYCWiN remains as a City-owned broadband wireless network providing coverage throughout the five boroughs. In 2019, City agencies still use NYCWiN for many purposes, including, but not limited to, the following examples:

- The Department of Transportation (DOT) remotely monitors and manages traffic lights and adjusts them in chosen locations based on changing traffic conditions and for specific events, including emergencies and public transit prioritization.
- Department of Parks and Recreation (Parks) employees have “access to email, Internet and intra-agency applications” at approximately 100 remote locations.³²
- The Department of Environmental Protection (DEP) transmits Automated Meter Reading (AMR) system data from the receivers collecting data from individual water meter sensors.³³
- The Police Department (NYPD) is able to connect in the field to their license plate readers, and transmit data securely.

While these agencies continue to rely on NYCWiN, other City agencies have begun to pilot and convert over to other network options, including commercial carriers [REDACTED]

From its initial launch to the present day, Northrop Grumman (as Northrop Grumman Systems Corporation) and its subcontractor General Dynamics (which acquired IPWireless) have been contracted to provide NYCWiN support, including network maintenance and site management services.³⁵ The City signed two renewal agreements with Northrop Grumman, one in 2011 and another in 2016; each included amendments that provide cost savings to the City.³⁶

2020 Preliminary Plan and the Fiscal 2019 Preliminary Mayor’s Management Report for the Department of Transportation,” Finance Division Briefing Paper, March 14, 2019, pages 4, 13 and 43, <https://council.nyc.gov/budget/wp-content/uploads/sites/54/2019/03/841-DOT-2020.pdf> (last accessed April 28, 2019).

³² DoITT, “NYCWiN.”

³³ NYC Department of Environmental Protection, *About Automated Meter Reading (AMR)*, https://www1.nyc.gov/html/dep/html/customer_services/amr_about.shtml (last accessed April 28, 2019).

³⁵ The ongoing involvement of General Dynamic in providing technical support was confirmed as part of interviews with the City and Northrop Grumman completed in preparation of this report.

³⁶ First Renewal Agreement by and between the City of New York Department of Information Technology and Telecommunications and Northrop Grumman Systems Corporation (CT85820111445466) and Second Renewal Agreement by and between the City of New York Department of Information Technology and Telecommunications and Northrop Grumman Systems Corporation (CT185820170003271). The first renewal agreement included lower fixed operations and maintenance costs and lower estimated pass-through costs than in the original agreement for the first renewal period, which is consistent with discussion during interviews with the City and Northrop Grumman completed in preparation of this report that indicated that the City was looking for cost savings in both of the renewal agreement negotiations.

3.2 Week Number Rollover

The Global Positioning System (GPS) is a U.S. government-operated utility that provides positioning, navigation, and timing services. In addition to delivering longitude, latitude and altitude, the 24 GPS satellites contain atomic clocks that provide precise time data. GPS receivers decode signals from the constellation of satellites to synchronize each receiver to the GPS atomic clocks, allowing users to determine the time to within 100 billionths of a second. Precise time is critical to a number of important systems all over the world, including electrical power grids, financial networks, and wireless telephone and data networks.³⁷

In 3G Universal Mobile Telecommunications Systems (UMTS), such as NYCWiN, the interconnected nodes only communicate correctly if the signals they exchange meet certain frequency and time synchronization requirements. Frequency and time (also known as phase) synchronization ensure that hand-offs between nodes are successful, bandwidth is optimized and network capacity is optimal. If frequency and time synchronization do not meet UMTS requirements, the stability and performance of the network erodes or fails entirely.³⁸

GPS receivers can play an important role in network synchronization and thus, the stability of a UMTS network. GPS receivers “lock” onto four or more satellites simultaneously so they can solve complex equations to compute their position and the current time.³⁹ This calculation of time allows the GPS receivers and network nodes to maintain synchronization across the network.

In order to accurately provide the current time, GPS satellites transmit time as a week number (WN) and the number of seconds elapsed in that week.⁴⁰ The WN associated with GPS time uses a ten (10) bit parameter with 1024 valid sequential values, meaning that “[a]t the end of the 1024th week, the counter experiences a rollover (resets) to 0.”⁴¹ The date from which the counters began was January 6, 1980, leading to the first rollover event in August 1999 and the second rollover event at 18 seconds before midnight UTC on April 6, 2019.⁴² The 2019 WNRO event was expected to be experienced by any GPS device unless it “conform[ed] to the latest

³⁷ National Coordination Office for Space-Based Positioning, Navigation, and Timing, *GPS.gov*, <https://www.gps.gov/> (last accessed April 28, 2019).

³⁸ Symmetricom, Inc., “Timing and Synchronization in Next-Generation Wireless Networks,” Technical Documentation, 2006, https://www.microsemi.com/document-portal/doc_download/133222-timing-and-synchronization-in-next-generation-wireless-networks (last accessed April 28, 2019).

³⁹ Paul Ducklin, “Serious Security: GPS Week Rollover and the Other Sort of ‘Zero Day,’” *Naked Security by Sophos*, April 5, 2019, <https://nakedsecurity.sophos.com/2019/04/05/serious-security-gps-week-rollover-and-the-other-sort-of-zero-day/> (last accessed April 28, 2019).

⁴⁰ Septentrio N.V., “All You Need to Know about the GPS / GNSS Week Number Rollover,” Insights, <https://www.septentrio.com/en/insights/all-you-need-know-about-gps-gnss-week-number-rollover> (last accessed April 28, 2019).

⁴¹ U.S. Department of Homeland Security National Cybersecurity & Communications Integration Center and National Coordinating Center for Communications, “Memorandum for U.S. Owners and Operators Using GPS to Obtain UTC Time.”

⁴² U.S. Department of Homeland Security, U.S. Coast Guard, “Local Notice to Mariners, District: 5, Week: 14/19,” Fifth District LNMs for 2019, April 2, 2019, pages 2-3, <https://www.navcen.uscg.gov/pdf/lnms/lnm05142019.pdf> (last accessed April 28, 2019). Note: UTC is the abbreviation for Coordinated Universal Time and is four hours ahead of Eastern Daylight Time.

IS-GPS-200 and provides UTC⁴³ or was otherwise configured to handle the date differently, for example was already receiving the 13-bit-based week number from modernized civil navigation (CNAV) signals.⁴⁴ Devices conforming to contemporary standards — whether recently manufactured or updated — were not expected to be affected.

In April 2018, the U.S. Department of Homeland Security (DHS) issued its “Memorandum for U.S. Owners and Operators Using GPS to Obtain UTC Time,” which was “intended to provide an understanding of the possible effects of the April 6, 2019 GPS Week Number Rollover on Coordinated Universal Time derived from GPS devices.”⁴⁵ The DHS’s Cybersecurity and Infrastructure Security Agency (CISA) also created a publicly available webpage related to the event.⁴⁶

In the 2018 memorandum discussing the 2019 WNRO event, DHS made specific recommendations:

Critical Infrastructure and other owners and operators are strongly encouraged:

1. to investigate and understand their possible dependencies on GPS for obtaining UTC,
2. to contact the GPS manufacturers of devices they use to obtain UTC
 - a. to understand the manufacturers’ preparedness for the April 6, 2019 WN rollover,
 - b. to understand actions required by CI and other owners and operators to ensure proper operation through the April 6, 2019 WN rollover, and
3. to ensure that the firmware of such devices is up-to-date.⁴⁷

Various agencies within DHS and other federal government agencies also published information about the WNRO event periodically prior to its occurrence.⁴⁸ For example, the Office of

⁴³ U.S. Department of Homeland Security National Cybersecurity & Communications Integration Center and National Coordinating Center for Communications, “Memorandum for U.S. Owners and Operators Using GPS to Obtain UTC Time.”

⁴⁴ Department of Defense, Department of the Air Force, “2017 Public Interface Control Working Group and Forum for the NAVSTAR GPS Public Documents,” *Federal Register* 84, no. 17 (January 25, 2019): 368, <https://www.federalregister.gov/documents/2019/01/25/2019-00111/2017-public-interface-control-working-group-and-forum-for-the-navstar-gps-public-documents> (last accessed April 28, 2019).

⁴⁵ U.S. Department of Homeland Security National Cybersecurity & Communications Integration Center and National Coordinating Center for Communications, “Memorandum for U.S. Owners and Operators Using GPS to Obtain UTC Time.”

⁴⁶ U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, *GPS Week Number Roll Over (WNRO)*.

⁴⁷ U.S. Department of Homeland Security National Cybersecurity & Communications Integration Center and National Coordinating Center for Communications, “Memorandum for U.S. Owners and Operators Using GPS to Obtain UTC Time.”

⁴⁸ U.S. Department of Homeland Security, U.S. Coast Guard, “Local Notice to Mariners, District: 5, Week: 14/19,” pages 2-3; Department of Defense, Department of the Air Force, “2017 Public Interface Control Working Group and Forum for the NAVSTAR GPS Public Documents”; Edward Powers, “CGSIC GPS Week Roll Over Issue,” U.S. Naval Observatory, September 26, 2017, <https://www.gps.gov/cgsic/meetings/2017/powers.pdf> (last accessed April 28, 2019); and Edward Powers, “Timing Criticality & GPS 1024 Week Rollover,” U.S. Naval Observatory, November 15, 2017, <https://www.gps.gov/governance/advisory/meetings/2017-11/powers.pdf> (last accessed April 28, 2019).

Electricity of the Department of Energy published a blog entry on February 7, 2019, and the Air Transportation Division of the Federal Aviation Administration of the Department of Transportation issued an Information for Operators (InFO) on April 3, 2019.⁴⁹

Despite the availability of information about the WNRO event, steps were not taken to prevent NYCWiN from being affected by the WNRO event. When the GPS receivers in NYCWiN rolled over on April 6, 2019, the NYCWiN NOC began receiving alerts that nodes were in “GPS unlock,” meaning they did not have the requisite connection with the GPS satellites. At that point, the nodes remained operational using cached locational and time data, but as the cached data expired, the nodes lost synchronization with the other nodes in the network. Without time and frequency synchronization, the nodes went down one by one the night of April 6 into April 7.

⁴⁹ Michael Pesin, OE-10, “The April 2019 Global Positioning System (GPS) Week Number Rollover,” U.S. Department of Energy Office of Electricity, February 7, 2019, <https://www.energy.gov/oe/articles/april-2019-global-positioning-system-gps-week-number-rollover> (last accessed April 28, 2019); and U.S. Department of Transportation Federal Aviation Administration, Air Transportation Division, “InFO 19005, Global Positioning System (GPS) Week Number Rollover Event,” Information for Operators, April 3, 2019, https://www.faa.gov/other_visit/aviation_industry/airline_operators/airline_safety/info/all_infos/media/2019/InFO19005.pdf (last accessed April 28, 2019).

4.0 Timeline

This timeline is an overview of the key milestones and activities related to the NYCWiN incident.⁵⁰ All times are considered approximate and are in Eastern Time.

- **April 2018** — U.S. Department of Homeland Security (DHS) releases a memorandum about the WNRO event coming in April 2019.
- **Saturday, April 6, 2019** — At 8 pm, GPS week number rolls over to zero.
- **Saturday, April 6, 2019** — At 8pm, Northrop Grumman’s Network Operations Center (NOC) identifies issues with NYCWiN network connectivity and initiates an investigation.
- **Saturday, April 6, 2019** — Throughout the night, NYCWiN connectivity issues expand across the network as NYCWiN node sites begin to go down. Between 10pm and 11pm, Northrop Grumman notifies DoITT, who begins to contact some of the City agencies on NYCWiN.
- **Sunday, April 7, 2019** — At 1:24am, Citywide Service Desk sends out initial notification to impacted City agencies concerning NYCWiN. Citywide Service Desk continues to send out regular updates through Tuesday, April 9.
- **Sunday, April 7, 2019** — At 6:30am, Northrop Grumman technicians have been able to replicate the issue in their U.K. lab and have determined the root cause and resolution.
- **Sunday, April 7, 2019** — [REDACTED]
- **Sunday, April 7, 2019** — In the morning, DoITT sets up an Incident Bridge for key stakeholders across agencies that provides regular updates through Thursday, April 11.
- **Sunday, April 7, 2019** — During the afternoon, DoITT and Northrop Grumman begin a harvesting process for infrastructure that require updates to the [REDACTED]. DoITT requests and receives assistance from field technicians, including other City agencies and Motorola, who have experience working with similar networks for the City.
- **Monday, April 8, 2019** — By 12pm, all [REDACTED] are down. A recovery strategy is developed that prioritizes testing and recovery at [REDACTED] NYCWiN priority sites prior to full restoration.
- **Monday, April 8, 2019** — By 6pm, Northrop Grumman technicians [REDACTED] with connector that is required to update the infrastructure that is being harvested from each NYCWiN site.
- **Tuesday, April 9, 2019** — By 10am, regression testing of updated infrastructure is still underway [REDACTED]
- **Tuesday, April 9, 2019** — Throughout the day, City agencies continue to harvest infrastructure from NYCWiN sites. City agencies, along with Northrop Grumman and Motorola, will continue to harvest and redeploy infrastructure throughout the rest of the week.

⁵⁰ This section is based on Citywide Service Desk Notifications from April 7 to April 9, and interviews conducted in preparation of this report, except as noted below.

- **Wednesday, April 10, 2019** — [REDACTED]
- **Thursday, April 11, 2019** [REDACTED]
- **Friday, April 12, 2019** — [REDACTED]
- **Saturday, April 13, 2019** — By 4pm, 69 NYCWiN sites are live on NYCWiN. As they are brought online, DOT technicians are sent to monitor traffic signals to ensure there are no adverse effects. Additional sites are brought up on Sunday, Monday, Tuesday and Wednesday.
- **Wednesday, April 17, 2019** — By 9pm, DoITT reports that NYCWiN has been restored to pre-incident connectivity.⁵¹

⁵¹ DoITT NYCWIN Agency Service Restoration Notice, April 18, 2019.

5.0 Impact Summary

Multiple City agencies, including those responsible for public safety, regulatory and administrative functions, rely on NYCWiN to conduct their normal business operations. Table 1 summarizes how individual agencies were impacted, based on Citywide Service Desk Notifications from April 7 to April 9, and interviews conducted in preparation of this report.

Table 1. Impact Summary

NYC Agency	Impact
Department of Buildings (DOB)	<ul style="list-style-type: none"> ▪ DOB inspectors were not able to access Buildings Information System (BIS) for their remote inspections. DOB continued to perform inspections without the ability to reference building information in the field.
Department of Citywide Administrative Services (DCAS)	<ul style="list-style-type: none"> ▪ DCAS fueling stations at approximately 100 sites across the City lost the ability to transmit data related to fueling station usage, fuel transactions and fuel tank capacity. DCAS could not provide its daily reporting on fuel information and transactions, limiting its insight into optimizing fuel distribution. ▪ Fueling stations did not lose the ability to dispense fuel during the NYCWiN incident. ▪ Several DCAS personnel were redirected from the course of normal operations to assist with NYCWiN restoration activities.
Department of Environment Protection (DEP)	<ul style="list-style-type: none"> ▪ DEP ESP systems for monitoring air quality throughout the City lost the ability to transmit data. DEP staff were forced to monitor these manually during the NYCWiN incident. ▪ DEP wireless devices affixed to water meters lost the ability to transmit data. DEP staff were forced to monitor these manually during the NYCWiN incident. ▪ 15-16 DEP personnel were redirected from the course of normal operations to assist with NYCWiN restoration activities.
Department of Health and Mental Hygiene (DOHMH)	<ul style="list-style-type: none"> ▪ Restaurant/pest inspection applications were impacted. Inspections continued to be performed without the ability to sync from the field.
Department of Sanitation (DSNY)	<ul style="list-style-type: none"> ▪ Approximately 70 remote sites lost backup connectivity. DSNY was still able to perform normal operations through their primary connectivity. ▪ Several DSNY personnel were redirected from the course of normal operations to assist with NYCWiN restoration activities.
Department of Transportation (DOT)	<ul style="list-style-type: none"> ▪ Approximately DOT 12,500 traffic signal controllers lost connectivity to NYCWiN. Impacted traffic signals continued to function despite loss of signal controller connectivity. ▪ DOT's ability to dynamically control impacted traffic signal controllers was lost, affecting DOT programs to monitor and optimize the flow of traffic and public transit throughout the City. ▪ Approximately 200 DOT traffic cameras used to monitor traffic conditions lost the ability to transmit images. As a result, DOT could not provide the public with real-time updates on traffic

NYC Agency	Impact
	<p>conditions in some areas of the City.</p> <ul style="list-style-type: none"> ▪ Approximately 50% of Real-Time Passenger Information Signs at New York City Bus Stops stopped functioning. ▪ 10-15 DOT personnel were redirected from the course of normal operations to assist with NYCWiN restoration activities.
Financial Information Services Agency (FISA)	<ul style="list-style-type: none"> ▪ 50 CityTime locations lost connectivity, preventing City staff from being able to submit their time remotely. City staff could still submit time at City offices during the NYCWiN incident.
Fire Department (FDNY)	<ul style="list-style-type: none"> ▪ FDNY’s supervisor ability to track EMS vehicles in its MobileMaps application was lost. As a result, FDNY used backup procedures to communicate locations. ▪ Several FDNY personnel were redirected from the course of normal operations to assist with NYCWiN restoration activities.
Parks and Recreation (Parks)	<ul style="list-style-type: none"> ▪ Parks devices and applications at approximately 100 remote sites lost connectivity to NYCWiN, including district offices, recreation centers and comfort stations. ▪ Parks lost the ability to remotely track workforce operations via workstations and handheld devices at impacted sites. ▪ Parks lost the ability to collect, record and transmit employee time and attendance data at impacted sites. ▪ Parks-administered locations lost the ability to electronically scan identification cards at impacted sites (e.g., recreation centers). ▪ Several Parks personnel were redirected from the course of normal operations to assist with NYCWiN restoration activities.
Police Department (NYPD)	<ul style="list-style-type: none"> ▪ Approximately 38 NYPD License Plate Readers (LPRs) lost the ability to transmit collected data. ▪ Mobile LPRs were deployed to impacted areas. ▪ Several NYPD personnel were redirected from the course of normal operations to assist with NYCWiN restoration activities.

6.0 WNRO Incident Analysis

The fundamental question of how the long planned,⁵² widely publicized⁵³ WNRO event was overlooked, given the vital role GPS plays in the operation of NYCWiN, is not answered by a single factor. Instead, it was a set of factors that had they happened individually, would not have led to an incident. However, when all of the factors align and occur simultaneously it results in an incident.⁵⁴ The WNRO event itself was unavoidable based on a mathematical certainty; however, its impact and this specific NYCWiN incident was the direct result of multiple avoidable active and latent factors.

Based on information provided by the City and Northrop Grumman, it is believed that the NYCWiN incident could have been prevented through a firmware update. A firmware update was required for the GPS receivers at each of the [REDACTED] nodes. The receivers were running on outdated firmware as of April 6, 2019. This firmware did not include a remedy for the WNRO event. The updated firmware that resolves the rollover issue was commercially available in advance of the WNRO event.⁵⁵ In order to upgrade the firmware, the City's NYCWiN support vendor, Northrop Grumman, would have had to physically visit all the [REDACTED] node sites to successfully update the firmware for each GPS receiver. However, this option was not brought to the City's attention in advance of the WNRO event.

Furthermore, a number of City agencies including NYPD, FDNY and DEP, began moving critical systems to modern, highly secure, faster third-party mobile broadband wireless networks that also included the GPS time sync. The incident can be primarily attributed to the following interconnected factors:

Finding 1. Failure to replace NYCWiN in a timely manner resulted in a high degree of risk associated with end of life technology.

End of life technology in any circumstance presents latent risk given the reduced attention and increased potential for time based software anomalies such as the WNRO event. The protracted migration of City agencies away from NYCWiN is a fundamental factor that created the basis for the incident to occur. Over the course of the last five years DoITT has been in an extended discussion and process of decommissioning NYCWiN. DoITT formally notified agencies of its intent to decommission NYCWiN in January 2016, requesting that agencies move off of NYCWiN no later than June 2019. All City agencies are projected to be off of NYCWiN by June 2020.⁵⁶ Furthermore, the NYCWiN decommissioning plan provided by DoITT indicates that the NYCWiN infrastructure would be fully decommissioned by the second quarter of 2022.

Moreover, some agencies reported in interviews a lack of clarity on the decommissioning schedule, creating the potential for further delays. An earlier enforced and fully executed

⁵² U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, *GPS Week Number Roll Over (WNRO)*.

⁵³ Michael Pesin, OE-10, "The April 2019 Global Positioning System (GPS) Week Number Rollover."

⁵⁴ Thomas V. Perneger, "The Swiss Cheese Model of Safety Incidents: Are There Holes in the Metaphor?," *BMC Health Services Research*, no. 5 (2005): 71, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1298298/> (last accessed April 28, 2019).

⁵⁵ Connor-Winfield, "Important Firmware Update for April 2019 GPW Week Number Rollover Event," Connor-Winfield Support, http://www.conwin.com/pdfs/gps_week_rollover.pdf (last accessed April 28, 2019).

⁵⁶ Interviews with the City conducted in preparation of this report.

decommissioning plan for NYCWiN would have rendered the WNRO a non-event. Yet, on April 6, there were approximately 10 agencies and approximately 12,000 devices⁵⁷ still on the network.

Finding 2. The heavy reliance on the long standing outsourced maintenance and support model was not counterbalanced by a consistent, well-executed vendor management discipline within DoITT.

Since January 2006 Northrop Grumman has served as the City of New York's Citywide Mobile Wireless Network provider for the design, construction, management and maintenance of NYCWiN.⁵⁸ At the time of design and development, Northrop Grumman partnered with IPWireless to provide NYCWiN's core 3G wireless broadband network equipment. On May 8, 2012 General Dynamics announced their acquisition of IPWireless.⁵⁹ Northrop partnered with General Dynamics to provide myriad services, including but not limited to U.S. based Help Desk services and United Kingdom based Engineering Support. The heavy reliance on Northrop is clearly illustrated by DoITT's extension of Northrop's support and maintenance contract twice over the last 13 years with an annual cost of up to \$40 million, including all leases.

Moreover, according to DoITT officials, there is a six-person team assigned to NYCWiN. In the wake of Commissioner Roest's decommissioning statement, several members of the DoITT NYCWiN team began to focus on the Citywide Commercial Enterprise Wireless Network (CCEWiN). [REDACTED]

This type of layered support model where prime and subcontractor relationships exist to fully maintain a critical, long-standing program necessitates the need for a strong vendor management discipline to ensure the continued health of the network. DoITT serves in that oversight/vendor management role and carries the responsibility of also understanding the network design and components in addition to overseeing the support and maintenance provided by Northrop, which maintains approximately 38 locally based resources and 2 remote resources, according to recent interviews.

The intersection of aging technology, the multi-vendor, fully outsourced support model and the stated intention to avoid further investment created the perception that NYCWiN would remain status quo until replacement. That said, with GPS playing such a critical role in operations of the City as well as General Dynamics' widely publicized role with Federal Government GPS satellites,⁶⁰ Northrop and its partners should have been pressed to certify and attest that no single point of failure changes were on the horizon.

⁵⁷ Citywide Service Desk Notifications, April 7, 2019-April 9, 2019, and interviews conducted in preparation of this report.

⁵⁸ Citywide Mobile Wireless Network Agreement by and between the City of New York Department of Information Technology and Telecommunications and Northrop Grumman Information Technology, Inc.

⁵⁹ General Dynamics, "General Dynamics to Acquire IPWireless, Inc.," May 8, 2012, <https://www.prnewswire.com/news-releases/general-dynamics-to-acquire-ipwireless-inc-150582145.html> (last accessed April 28, 2019). The acquisition was completed June 8, 2012. General Dynamics, "General Dynamics Completes Acquisition of IPWireless."

⁶⁰ General Dynamics Mission Systems, "Providing the GPS III Network Communications Element," <https://gdmissionsystems.com/en/communications/satellite-mission-payloads/gps-iii-satellites> (last accessed April 28, 2019).

Finding 3.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

What was clear was that the WNRO event had cyber implications. According to Cheri Caddy, “who leads a public-private program at the National Security Agency,” “We are looking at how time is critical to everything you do in cyber, from forensic logs to cryptography.... If you lose access to precision time, you can unlock everything, from a cryptography standpoint, or lock things forever.”⁶²

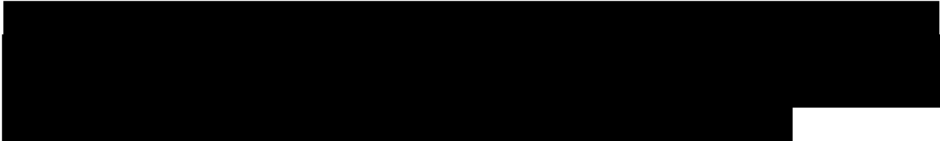
Finding 4. The WNRO event was known by multiple agencies.

In a complex organizational environment, information sharing is vital to efficient operations and resiliency, particularly in the case of a multi-agency asset such as NYCWiN. Based on multiple interviews several agencies including NYC3, DEP, NYPD and New York City Emergency Management (NYCEM) indicated that they received information regarding the WNRO event either by DHS or by their original equipment manufacturers for any systems that included GPS core functionality. However, DoITT, the City agency responsible for NYCWiN, confirmed that they were not aware of the WNRO event prior to April 6. In the absence of formalized cross-agency communications, the implications of the WNRO event on NYCWiN were not recognized as widely as necessary.

⁶¹ Bob Kolasky, “The GPS Rollover — What You Need to Know,” YouTube video, 10:15, posted by Auburn University Center for Cyber and Homeland Security, March 27, 2019 <https://www.youtube.com/watch?v=Aj9ZtdQ2g20> (last accessed April 29, 2019). The video is from an event hosted at the Auburn University Center for Cyber and Homeland Security that was “the rollout of the Department of Homeland Security’s guidance for the upcoming GPS rollover.” For more information, see Auburn University Center for Cyber and Homeland Security, “The GPS Rollover — What You Need to Know,” March 27, 2019, <http://cchs.auburn.edu/gps-rollover.html> (last accessed April 29, 2019).

⁶² Gopal Ratnam, “GPS Has Its Own 19-Year Cicada Problem,” Roll Call, April 2, 2019, <https://www.rollcall.com/news/policy/gps-satellites-cybersecurity> (last accessed April 29, 2019).

Based on these findings, the following recommendations are proposed:

- Recommendation 1.** Finalize the decommissioning of NYCWiN as soon as possible by mandating that all remaining agencies migrate either to CCEWiN or an alternative by a firm, established deadline.
- Recommendation 2.** Develop a comprehensive Citywide inventory of all end of life hardware and software assets associated with critical infrastructure in the next 30 days and create a risk based assessment for asset risk mitigation, contingency planning and asset upgrade.
- Recommendation 3.** Institute an ongoing process for identifying, classifying and prioritizing end of life assets that provide critical NYC capabilities and issue regular reports on progress to City Hall.
- Recommendation 4.** All vendors maintaining systems that provide critical NYC capabilities (or “critical functions”⁶³ as defined by DHS) must provide periodic attestation to the City that all patches and configuration changes are current, along with a forecast for upcoming required changes in the next 12 months.
- Recommendation 5.** 

⁶³ DHS CISA, “National Critical Functions Initiative.”

7.0 Incident Preparedness and Response

Government has a clear responsibility to prepare for an expansive set of potential events that may put public safety in jeopardy or that have the potential to disrupt essential public services.⁶⁴ These responsibilities are often codified in laws, rules and executive orders. For example, in New York City, every agency is required to have a Continuity of Operations Plan (COOP) to continue essential operations during an emergency or other incident that may disrupt normal agency operations.⁶⁵

It is important to highlight that until this incident NYCWiN had not experienced a networkwide service interruption since it was first announced as fully operational by the City in 2009.⁶⁶ DoITT has prepared for and successfully responded to threats to the NYCWiN network including protecting NYCWiN during Hurricane Sandy in October 2012.⁶⁷ After Hurricane Sandy, the City reported to the Federal Communications Commission (FCC) that NYCWiN “performed as designed during the storm and its aftermath,” and that “it exceeded public safety standards for resiliency, telecommunications redundancy and backup power.” The City further reported to the FCC that NYCWiN remained live and served as a critical mobile wireless network backbone during the recovery effort.⁶⁸ However, during this review significant deficiencies regarding preparedness and response to the NYCWiN incident were found as described below:⁶⁹

Finding 5.

[REDACTED]

[REDACTED]

[REDACTED]

⁶⁴ For example, the DHS, which includes CISA and Federal Emergency Management Agency (FEMA), and the Centers for Disease Control and Prevention (CDC).

⁶⁵ New York City Executive Order No. 107 of October 2, 2007, “Continuity of Operations Planning,” http://www.nyc.gov/html/om/pdf/eo/eo_107.pdf (last accessed April 29, 2019).

⁶⁶ DoITT, “Department of Information Technology and Telecommunications and Northrop Grumman Corporation Announce the New York City Wireless Network is Operational Citywide.”

⁶⁷ New York City Office of the Mayor, “Hurricane Sandy After Action,” May 2013, pages 14-15, https://www1.nyc.gov/assets/housingrecovery/downloads/pdf/2017/sandy_aar_5-2-13.pdf (last accessed April 29, 2019).

⁶⁸ Rahul N. Merchant, “Statement of NYC Chief Information & Innovation Officer Rahul N. Merchant to the Federal Communications Commission, PS Docket No. 11-60 Regarding Communications & Hurricane Sandy,” February 7, 2013, page 5, <https://ecfsapi.fcc.gov/file/7022119157.pdf> (last accessed April 29, 2019).

⁶⁹ The review did not include confirming compliance with applicable policy, laws, codes and rules.

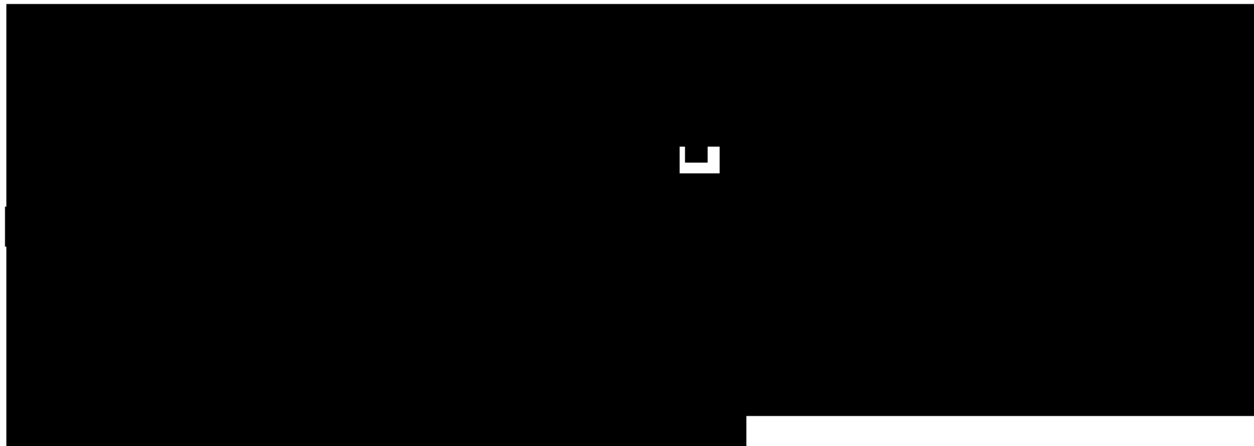
⁷⁰ For example, page 7 and Annex 6.20 of DoITT, “Continuity of Operations & Emergency Response Plan,” provided by the City on April, 24, 2019.



No single reason for the limited NYCWiN preparedness activities was reported. However, the active and latent factors described in Section 6.0, such as the protracted decommissioning of NYCWiN, and complete reliance on NG for all NYCWiN support and maintenance, serve as a starting point to investigate and determine underlying reasons for the limited NYCWiN preparedness activities.

Finding 6. DoITT’s incident management processes for NYCWiN are insufficient.

Detailed incident management processes are commonly developed, documented and maintained in large public and private enterprises for all core systems. For the purposes of this report, the incident management process documents provided by DoITT were compared to practices for incident management recommended by the widely recognized Information Technology Infrastructure Library (ITIL)⁷² to determine whether DoITT’s incident management processes for NYCWiN are sufficient.



Additionally, as part of the incident management process, there are some undeveloped references to problem management, the practice of minimizing the number and degree of problems an organization experiences with regard to its technology systems.⁷⁴ More details were expected within the major incident process documents addressing the integration with problem management and having references to both reactive and proactive problem management. Problem management is a process that is critical to the success and velocity of a restoration effort. Despite being in the process of decommissioning NYCWiN, DoITT’s problem

⁷¹ For example, see DHS, “Exercises,” Preparedness Planning for Your Business, <https://www.ready.gov/business/testing/exercises> (last accessed April 29, 2019).

⁷² U.K. Cabinet Office, *ITIL® Service Operation*, 2011 ed. (Norwich: The Stationery Office, 2011).



⁷⁴ U.K. Cabinet Office, *ITIL® Service Operation*.

management processes and practices should be reviewed systematically to identify potential gaps, so that, where possible, preventative actions can be taken in a timely manner.

Finding 7. Joint engagement among DoITT, NYC3, NYCEM and NG was limited and unstructured as it relates to NYCWiN incident preparedness.

In interviews, DoITT, NYC3, NYCEM and NG did not discuss specific, structured engagement with each other regarding NYCWiN preparedness. For instance, it did not appear that NG regularly reached out to DoITT regarding any corporate-level changes to their preparedness practices relevant to NYCWiN. NG claims leadership in end-to-end cyber,⁷⁵ and performs significant work with navigation systems,⁷⁶ including providing navigation systems support for military customers.⁷⁷ Therefore, it is assumed as part of its normal business activities NG regularly reviewed and updated its preparedness practices and capabilities, including ones that would be relevant to broadband wireless infrastructure systems such as NYCWiN.⁷⁸ This critical level of interaction did not seem to occur.

Similarly no key City agency — DoITT, NYC3 and NYCEM — appeared to regularly engage NG and its subcontractor GD in a specific and structured way regarding NYCWiN preparedness. Such interactions and coordination between vendors and customers regarding systems critical to business continuity are essential to preparedness. For example, the NYCEM gives similar guidance to businesses regarding preparedness on its website (“Coordinate with vendors, suppliers, and others you depend on to do business”).⁷⁹

It is possible that elements of preparedness were discussed between DoITT, NYC3, NYCEM and NG staff incidentally during the course of their normal interactions regarding the everyday NYCWiN operations, or perhaps were discussed in detail at the time NYCWiN first became fully operational in 2009.⁸⁰ The City may consider conducting a more detailed review to determine whether or not this was the case, and if so, the nature of the specific interactions around preparedness. However, even if it is found that preparedness was discussed when NYCWiN first became fully operational, or informally at times between DoITT, NYC3, NYCEM and NG since then, this is not an adequate substitute for structured engagement on preparedness, especially for a critical system such as NYCWiN.

⁷⁵ Northrop Grumman, “Cyber,” Northrop Grumman website, <http://www.northropgrumman.com/Capabilities/Cybersecurity/Pages/default.aspx> (last accessed April 29, 2019).

⁷⁶ Northrop Grumman, “Navigation Systems,” Northrop Grumman website, <http://www.northropgrumman.com/Capabilities/NavigationSystems/Pages/default.aspx> (last accessed April 29, 2019).

⁷⁷ Northrop Grumman, “Navigation Systems Support for Military Customers,” Northrop Grumman website, <http://www.northropgrumman.com/AboutUs/BusinessSectors/MissionSystems/Pages/NavMilitarySupport.aspx> (last accessed April 29, 2019).

⁷⁸ NG’s subcontractor, GD, which describes itself as “a global aerospace and defense company,” presumably also regularly reviewed and updated its corporate preparedness practices and capabilities as part of its normal business activities. See generally General Dynamics, “About GD,” General Dynamics website, <https://www.gd.com/about-gd> (last accessed April 29, 2019).

⁷⁹ NYC Emergency Management, “Take Action to Prepare Your Business,” *Ready New York*, Step 2, <https://www1.nyc.gov/site/em/ready/businesses.page> (last accessed April 29, 2019).

⁸⁰ DoITT, “Department of Information Technology and Telecommunications and Northrop Grumman Corporation Announce the New York City Wireless Network is Operational Citywide.”

Finding 8. NG did not promptly notify DoITT when it first detected the NYCWiN service interruption.

There was approximately a two to three hour gap between when the NYCWiN Network Operations Center (NOC), exclusively operated by NG, first detected GPS timing errors on the NYCWiN infrastructure around 8pm and when they notified DoITT between 10pm and 11pm.⁸¹ Prior to notifying DoITT, NG reported their team began troubleshooting the GPS timing errors on their own and identified the widely publicized WNRO event as a potential cause. They then began researching potential remedies, including available updates to the firmware of the GPS components resident within NYCWiN RAN sites. NG stated their team also realized they required support from their subcontractor, GD, but were unable to immediately reach key GD personnel directly. NG stated the difficulty in reaching those personnel located in the United Kingdom was due to GD being outside of business hours in that time zone (overnight hours). Once NG notified DoITT, DoITT began a series of informal notifications to some agencies it knew would be affected, including NYPD and DOT.

The delay of approximately two to three hours between the time that NG first detected the service interruption to when that interruption was reported to DoITT delayed full mobilization in response to the incident.


Finding 9.

⁸¹ Interviews conducted in preparation of this report with the City and NG.

⁸² DoITT, "Continuity of Operations & Emergency Response Plan," provided by the City on April, 24, 2019, Section 6.7.

⁸³ Ibid.

⁸⁴ Id., page 48.



Finding 10. A clear decision-making and communication structure was not promptly established during incident response.

Establishing clear lines of authority is core to effectively coordinating incident response.⁸⁵ Several of those interviewed reported that during the incident, it was not clear who was in charge and that different leaders from different agencies appeared to be responsible for making decisions at different times during the incident. This complicated the ability for the City to make timely decisions regarding restoration efforts. Had there been a clearer decision-making authority, there may have been a more effective and timely review and the proposal may have been enacted more quickly.

Establishing a clear operations communications plan is also core to effectively managing incident response. Operational communications focus “on the timely, dynamic, and reliable movement and processing of incident information in a form that meets the needs of decision makers at all levels.”⁸⁶ While there were several conference bridges and regular updates on the bridges, interviewees reported that the initial notifications and invites were not comprehensive in that they did not include some of the impacted agencies as well as did not include all the right personnel from agencies that were included. This led to a diverse group of agency stakeholders seeking different levels of information on conference calls, making the calls hard to manage. In an effort to structure communications, the City streamlined participants into a core team by Tuesday, April 9.

However, some confusion over incident updates and status persisted. Lastly, interviewees reported that priorities often came from different stakeholders and in some cases, the agencies became part of the critical path for NYCWiN restoration and were given short notice and tight deadlines for their own agency resources to fulfill key activities.

Finding 11. Limited data analytics in the early stages of the incident hindered response effectiveness and decision-making.

In the event of an incident the ability to make rapid, well informed, evidence based decisions is essential. This can be achieved in a multitude of ways whether it be manually or with advanced analytical tools that provide deep insight and underpin the decision-making as well as risk management processes. A data-driven response will lead to a more efficient and effective recovery that optimizes the people, processes and technology involved so that operations are restored as quickly as possible at the lowest possible cost.

The NYCWiN incident business impact assessment and subsequent recovery effort was hindered at the outset of the event by uncoordinated data collection and analytics processes by DoITT and Northrop Grumman. Once engaged by City leadership, NYCEM began to provide reports starting April 8.

⁸⁵ For example, see references to Incident Command System in DHS FEMA, “National Incident Management System,” 3rd Edition, October 2017, See https://www.fema.gov/media-library-data/1508151197225-ced8c60378c3936adb92c1a3ee6f6564/FINAL_NIMS_2017.pdf (last accessed April 29, 2019).

⁸⁶ DHS, “National Cyber Incident Response Plan,” December 2016, page 26, https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf (last accessed April 29, 2019).

Throughout the restoration, several agencies provided analyses regarding number of devices impacted, sites impacted, disposition of activities and restoration. However, there was not a robust, coordinated, centralized data analytics and reporting capability. This deficiency increased the probability for miscommunication, dissemination of inaccurate information, inefficiencies in the recovery effort and in turn may have impacted the financial investment to restore NYCWiN.

Finding 12. [REDACTED]**Finding 13. DoITT has yet to issue a formal post-incident report.**

The purpose of a post-incident report is to analyze the actions, process and results, including identifying strengths to be maintained and built upon, identifying potential areas for further improvement and support development of corrective actions. Although DoITT has stated that they are working on creating a post-incident report, a formal report had not been issued as of this assessment's publication. The extent of DoITT's post-incident review, including which external stakeholders are involved, is also not clear.

Post-incident reports are often actioned promptly after the incident itself so that interviewees still have the incident fresh in their minds and are able to easily recall incident activities, timeframes and events. This allows the report to focus and prioritize areas of improvement that otherwise might be lost.

This report should not be viewed as a substitute for DoITT's own post-incident report and that report should be completed as soon as possible to ensure that any opportunities to develop DoITT and vendor processes are not missed.

Based on these findings, the following recommendations are proposed:

- Recommendation 6.** Require regular, structured engagement on preparedness between parties operating critical technologies, including DoITT, NYC3, NYCEM and any involved vendors.
- Recommendation 7.** The City should evaluate the circumstances and thresholds where NYCEM is put in charge, or takes over, an incident response.
- Recommendation 8.** Require all necessary capabilities and equipment potentially required to service critical technology in the event of an incident, to be locally available whether the provider is the City or a vendor.

Recommendation 9.

[REDACTED]

Recommendation 10. Require standardized incident response procedures across City agencies and vendors that are consistent with Citywide Incident Management System (CIMS) protocols and enforce their use in response to incidents.

Recommendation 11.

[REDACTED]

Recommendation 12. Perform a detailed business impact analysis on all identified critical City technology infrastructure to understand the consequences of a disruption and gather the requisite information needed to develop robust recovery strategies.

Recommendation 13. Establish a critical technology task force to update all emergency and continuity of operations plans, as well as to evaluate preparedness in detail.

8.0 Conclusion

Based on the analysis, the NYCWiN incident could have been prevented. The findings outlined herein indicate that the City may be exposed to more risk than necessary regarding technology-related incidents and the disposition of critical infrastructure.

This incident serves as a clear signal to increase focus on critical technology infrastructure preparedness and response. These recommendations serve as a starting point. It is essential that the City take immediate action to examine preparedness regarding all its critical technology infrastructure, in-process projects and any related assets, including those that may be operated in whole or part by vendors on behalf of the City.

Finally, while this report identifies several issues regarding the NYCWiN incident, it is important to note that many City agencies and personnel actively worked together to restore NYCWiN as quickly as possible for the benefit of all New Yorkers.

9.0 Appendix

9.1 Interviews Conducted

In the preparation of this report, 51 interviews were conducted with the agencies and entities as enumerated in alphabetical order in Table 2.

Table 2. Interview List

Agency/Entity	
Fire Department of the City of New York (FDNY)	<ul style="list-style-type: none"> • Laura Kavanagh, First Deputy Commissioner • Jon-Paul Augier, Deputy Commissioner for Dispatch Operations and Public Safety Technology • Benny Thottam, Chief Information Officer
General Dynamics (GD)	<ul style="list-style-type: none"> • Bill Ross, Vice President for Information Security Systems • Steve Stoker, Systems Support Manager • Alan Jones, Software Development
New York City Cyber Command (NYC3)	<ul style="list-style-type: none"> • Geoff Browne, Chief Information Security Officer • Colin Ahern, Deputy Chief Information Security Officer • Mike Krygier, Deputy Chief Information Security Officer
New York City Department of Citywide Administrative Services (DCAS)	<ul style="list-style-type: none"> • Lisette Camilo, Commissioner • Quintin Haynes, Chief of Staff • Keith Kerman, Chief Fleet Officer • Nitin Patel, Chief Information Officer • Harris Kaplan, Director of Fleet Operations • Raj Lotwala, Executive Director for Network Infrastructure • Eric Richardson, Deputy Chief of Fleet Management
New York City Department of Environmental Protection (DEP)	<ul style="list-style-type: none"> • Vincent Sapienza, Commissioner • Cecil McMaster, Chief Information Officer • Joe Murin, Chief Financial Officer • Kieno Leach, Network Manager
New York City Department of Information Technology and Telecommunications (DoITT)	<ul style="list-style-type: none"> • Samir Saini, Commissioner • Vijay Gogineni, Chief Operating Officer • Michael Bimonte, Deputy Commissioner for Infrastructure • Frank Aghili, Assistant Commissioner for Wireless Technologies • Dan Nunez, Chief Information Security Officer

Agency/Entity	
	<ul style="list-style-type: none"> • JP Nicosia, Executive Director for Infrastructure Engineering • Roger Wang, Enterprise Systems Management • Shahrn Asim, Director
New York City Department of Parks and Recreation (Parks)	<ul style="list-style-type: none"> • Liam Cavanagh, First Deputy Commissioner • Margaret Nelson, Chief of Staff • Russell Antonucci, Assistant Commissioner & Performance Management • James Greenan, Chief of Information Technology & Telecommunications
New York City Department of Sanitation (DSNY)	<ul style="list-style-type: none"> • Edmund Lee, Chief Information Officer • Greg Anderson, Chief of Staff
New York City Department of Transportation (DOT)	<ul style="list-style-type: none"> • Polly Trottenberg, Commissioner • Joseph Jarrin, Executive Deputy Commissioner for Strategic & Agency Services • Joshua Benson, Deputy Commissioner for Traffic Operations • Cordell Schacter, Chief Technical Officer
New York City Emergency Management (NYCEM)	<ul style="list-style-type: none"> • Henry Jackson, Deputy Commissioner • Eric Smalls, Assistant Commissioner • Ben Krakauer, Assistant Commissioner
New York City Police Department (NYPD)	<ul style="list-style-type: none"> • Jessica Tisch, Chief Information Officer • Steven Harte, Assistant Commissioner
Northrop Grumman (NG)	<ul style="list-style-type: none"> • C.W. "Gator" Harvey, Business Unit Director • Doug Brown, Project Manager • Rhea Altamura, Senior Manager for Contracts
Office of the Mayor of New York City	<ul style="list-style-type: none"> • Laura Anglin, Deputy Mayor • Aloysee Heredia-Jarmoszuk, Deputy Mayor Chief of Staff • David Lara, Chief Administrative Officer • Dan Casey, Project Manager • Albert Pulido, Senior Policy Advisor

9.2 Glossary

The glossary in Table 3 below defines acronyms and initialisms used in the contents of the report.

Table 3. Glossary

Term	Definition
AMR	Automated Meter Reading
BIS	Building Information System
CCEWiN	Citywide Commercial Enterprise Wireless Network
CI	Critical Infrastructure
CIMS	Citywide Incident Management System
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
City	New York City
COO	Chief Operating Officer
COOP	Continuity of Operations Plan
DCAS	New York City Department of Citywide Administrative Services
DEP	New York City Department of Environmental Protection
DHS	United States Department of Homeland Security
DOHMH	New York City Department of Health and Mental Hygiene
DoITT	New York City Department of Information Technology and Telecommunications
DOT	New York City Department of Transportation
DSNY	New York City Department of Sanitation
ePCR	Electronic Patient Care Records
FCC	Federal Communications Commission
FDNY	Fire Department of the City of New York

Term	Definition
FEMA	Federal Emergency Management Agency
FISA	Financial Information Services Agency
GD	General Dynamics
InFO	Information for Operators
InfoSec	Information Security
ITIL	Information Technology Infrastructure Library
LPR	License Plate Reader
NG	Northrop Grumman
NOC	Network Operations Center
NYCEM	New York City Department of Emergency Management
NYCICC	New York City Infrastructure Coordinating Center
NYCWiN	New York City Wireless Network
NYC3	New York City Cyber Command
NYPD	New York City Police Department
OEM	Original Equipment Manufacturer
Parks	New York City Department of Parks and Recreation
RACI	A responsibility assignment matrix; it refers to Responsible, Accountable, Consulted and Informed
RAN	Radio Access Network
RFEI	Request for Expressions of Interest and Information
RFP	Request for Proposal
UMTS	Universal Mobile Telecommunications Systems
UTC	Coordinated Universal Time
WNRO	GPS Week Number Roll Over
Y2K	Year 2000