MEMORANDUM

SUBJECT: Review of Cybersecurity Requirements in WMATA's Procurements (OIG 19-08)

DATE: March 5, 2019

FROM: OIG – Geoffrey A. Cherrington

TO: GMGR – Paul J. Wiedefeld

During our audit of *WMATA's Cybersecurity over Rail Industrial Control Systems*, OIG became aware of cybersecurity risks over rail procurements. The contract for 7000 series railcars did not contain specific cybersecurity[1] requirements. As such, contractors are not obligated to address cybersecurity. At the time of this review, the Request for Proposal (RFP) for the 8000 series railcars also did not contain cybersecurity requirements.[2] Consequently, WMATA may be vulnerable to (1) cyberattacks and data breaches resulting from compromised third-party systems and services, and (2) manipulation of rail software which could adversely impact the safe operation of Metro's rail system and potentially threaten national security.

WMATA's Internal Business Operations (IBOP) provided written comments dated February 15, 2019 (see Appendix). IBOP concurred with the findings and recommendations. Corrective actions have taken place or begun on several recommendations prior to report issuance. Regarding recommendation 3, WMATA has amended the RFP for the 8000 series railcars to include cybersecurity requirements. With the issuance of this report, we consider this recommendation closed. Regarding recommendations 1 and 2, WMATA is developing cybersecurity requirements for applicable procurements and approved funding to test the effectiveness of security controls. The target completion date for all recommendations is September 27, 2019. OIG considers management's comments responsive to the recommendations and corrective actions taken or planned should correct the deficiencies identified in the report.

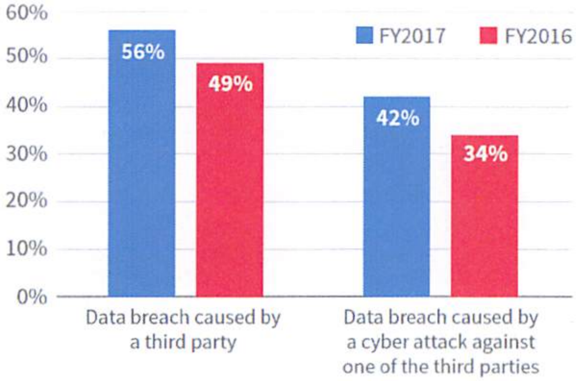
[1] Per Department of Homeland Security's Glossary, cybersecurity is defined as the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

[2] The RFP was subsequently amended on February 6, 2019 to include cybersecurity requirements.

Background

Perspective – According to Ponemon Institute's *Data Risk in the Third-Party Ecosystem Second Annual Study*, in 2017, 56 percent of respondents reported that their organizations experienced a data breach caused by one of their vendors (refer to Figure 1).

Figure 1: Data Breach of Cyber-attack caused by a Third-Party



The reported breaches in 2017 showed a significant increase from 2016. Also, cyber-attacks against third-parties that resulted in the misuse of their company's sensitive or confidential information increased from 34 percent to 42 percent of the respondents.

A third-party attack occurs when a third party system is compromised and subsequently used to gain unauthorized access to other trusted systems. For example, the 2013 breach of Target Corporation was caused by inadequate security controls by a third-party HVAC vendor, whose credentials were used to access Target's internal network and internal systems. As a result, personal information for approximately 70 million customers was compromised and 40 million customers' credit/debit card information stolen. This compromise cost Target over $150 million.

Attacks on transit system's IT resources have also become commonplace and increasingly sophisticated. For example, on November 25, 2016, the San Francisco Municipal Transportation Agency incurred a cyberattack that disabled critical rider systems and may have exposed thousands of employees' and customers' personal information. The cyber bandits demanded approximately $73,000. If the attack was on WMATA's rail control system, the result could shut down the Metrorail or even result in a rail accident.

Cybersecurity Requirements for Railcar Procurements – Cybersecurity is a growing concern for public transit managers, as control and management systems become increasingly dependent on information technology. WMATA issued RFP No. CQ19038-8K/FRV on September 2018 for the 8000 series railcars and proposals are due by April 4, 2019. In addition, WMATA has an existing contract for the purchase of the 7000 series railcars. Both series of railcars contain complex automated control systems, such as supervisory control and data acquisition (SCADA),[3] remote terminal units (RTUs),[4] and sensors to control and monitor operations to ensure a safe and efficient rail system. WMATA employs contractors to maintain these control systems. Contractors may provide potential additional avenues for cyberattacks.

WMATA's Office of Procurement and Materials is responsible for solicitation, award and administration of all Authority contracts and the purchase of supplies, services, equipment, and construction. Under the Information Technology Department, Office of Cyber Security (formerly Metro Information Technology Security) is responsible for determining the required security controls that should be applied to IT procurements.

What is Required

A description of the best practices and WMATA guidance OIG used for this review is provided below:

- *National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity* provides an objective for cyber supply chain risk management (SCRM) to identify, assess, and mitigate products and services that may contain potentially malicious functionality within the cyber supply chain. The SCRM include determining, enacting and communicating to suppliers how cybersecurity requirements will be verified and validated through formal agreements/contracts.

- *NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations* provides detailed guidelines for managing IT supply chain risks, such as insertion of counterfeits, tampering and insertion of malicious software/hardware.

- *Department of Homeland Security, Cyber Security Procurement Language for Control Systems* summarizes security principles and controls to consider when designing and procuring control system products and services and provides example language that could be incorporated into procurement specifications.

- *American Public Transportation Association (APTA)* provides cybersecurity standards for Public Transit to help protect the sector's cyber systems and physical automations against malicious and inadvertent manipulation.

- *WMATA's IT Security Standards and Guidelines* – provide a framework that establishes data security, availability and integrity of the WMATA data and its operations.

[3]Per techopedia, SCADA refers to industrial control systems that are employed to control and keep track of equipment or a plant in industries like water and waste control, telecommunications, energy, transport, and oil and gas refining.

[4]Per techopedia, RTU is a multipurpose device used for remote monitoring and control of various devices and systems for automation.

- *WMATA's Procurement Procedure Manual* – describes general procurement procedures which shall govern the solicitation, award and administration of all Authority contracts and purchase of supplies, services, equipment, and construction.

What We Found

The 8000 RFP[5] and 7000 series contract contained some references to IT security requirements for contractors and did not contain specific process-related cybersecurity requirements[6] as follows:

1. Provide adequate security (e.g., hardware, software/firmware) on all applicable contractor information systems;
2. Identify, assess and mitigate cybersecurity risks or threats;
3. Ensure hardening of vendor or contractor systems;
4. Investigate, report, and assess damage on any compromise of systems;
5. Preserve and protect all media involved in a cyber incident;
6. Provide access to contractor systems/equipment for forensic analysis; and
7. Mitigate cyber incidents, malicious code, or data breaches.

Procurement officials armed with contractual cybersecurity requirements are intended to be the first line-of-defense against third party cyber-attacks. At the time of this review, contractors bidding on the 8000 series railcar were not required to address cybersecurity risks in their proposals. The procurement process also did not contain any cybersecurity evaluation factors.

Why this Occurred

These conditions occurred for the following reasons:

- *WMATA has Not Adopted or Implemented a Cybersecurity Framework or Program* – Per NIST Cybersecurity Framework, a cybersecurity program provides guidelines for establishing cybersecurity requirements. WMATA is adopting the NIST Cybersecurity Framework so no recommendation was made in this report.

- *Inadequate Cybersecurity Requirements or Language for Procurements* – WMATA has not developed specific cybersecurity requirements for procurements. In addition, the PPM does not contain cybersecurity language, references, or criteria that define the terms and conditions for acquiring IT-related systems and services.

- *Lack of Policies and Procedures for Cybersecurity Requirements for Procurement* – WMATA has not developed policies and procedures to manage, oversee and communicate cybersecurity requirements for procurements.

[5] Subsequently amended to include cybersecurity requirements.

[6] Requirements for contractors include systems developed for WMATA and contractor/subcontract systems that interface with WMATA systems.

- *Cybersecurity Awareness and Training is Inadequate* – WMATA has not performed specific cybersecurity awareness and/or training to procurement officials on contracts.

Why this is Important

Without the cybersecurity requirements in RFPs, contractors are not obligated to respond to cybersecurity risks in their proposals. Consequently, those requirements are not formalized in a contract. Contract requirements are necessary to:

- Provide assurance that contractors are adequately protecting WMATA's systems and data against malicious code by hackers.
- Decrease vulnerability to cyberattacks and potential data breaches from compromised contractor systems and services.
- Decrease vulnerability to manipulation of rail software which could adversely impact the safe operation of Metro's rail system and potentially threaten national security.[7]

Recommendations

We recommend the General Manage/Chief Executive Officer:

1. Develop cybersecurity requirements for procurements. (Action: Chief of Internal Business Operations)
2. Conduct cybersecurity risk assessments; identify and test the effectiveness of controls; and implement mitigation strategies for applicable existing WMATA contracts. (Action: Chief of Internal Business Operations)
3. Immediately update the RFP for the 8000 series railcars with cybersecurity requirements. (Action Completed -- Closed)
4. Define and implement a process to ensure future applicable procurements include specific cybersecurity requirements. (Action: Chief of Internal Business Operations)
5. Create policies and procedures for managing and overseeing cybersecurity requirements for procurements. (Action: Chief of Internal Business Operations)
6. Develop specific cybersecurity awareness training for the Office of Procurement and Materials. (Action: Chief of Internal Business Operations)

[7] Washington Post's article of January 17, 2019, *Could a Chinese-made Metro car spy on us? Many experts say yes.*

Objective, Scope and Methodology

Our objective was to determine whether cybersecurity requirements were incorporated into WMATA contracts, RFPs and procurement processes. The scope included the RFPs for the 8000 series railcars and the contract for the 7000 series railcars.

To address the review objective, we:

1. Reviewed relevant documents, including WMATA's P/I's, Security Standards, and the Procurement Procedures Manual.

2. Reviewed related best practices guidelines related to cybersecurity and procurement, such as the NIST Cybersecurity Framework, NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, Department of Homeland Security's Cyber Security Procurement Language for Control Systems, and American Public Transportation Association's practice on Cybersecurity Considerations for Public Transit.

3. Interviewed WMATA staff from the departments of Rail Services, Procurement, and Information Technology.

4. Reviewed best practices for information security controls related to supply chain procurement including: System Hardening, Perimeter Protection, Account Management, Coding Practices, Flaw Remediation, Malware Detection and Protection, Host Name Resolution, End Devices, Remote Access, Physical Security and Network Partitioning.

5. Reviewed RFP and Technical Specifications for the 8000 series railcars and the contract for the 7000 series railcars for cybersecurity requirements.

This evaluation was conducted in accordance with the Council of Inspectors General on Integrity and Efficiency "*Quality Standards for Inspection and Evaluations.*" Those standards required that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objective.

Appendix

MEMORANDUM

SUBJECT: Audit of WMATA's Cybersecurity over Rail Industrial Control Systems – Review of Cybersecurity Requirements in WMATA's Procurements

DATE: February 15, 2019

FROM: IBOP – John T. Kuo [redacted]

THRU: GM – Paul J. Wiedefeld [redacted]

TO: OIG – Geoffrey A. Cherrington

WMATA IBOP management has prepared the following response to the OIG draft report for the WMATA's Cybersecurity over Rail Industrial Control Systems – Review of Cybersecurity Requirements in WMATA's Procurements.

WMATA IBOP has reviewed the memorandum and has held preliminary discussions regarding OIG's findings and recommendations with the offices of IT and Procurement. In the following memorandum, WMATA IBOP has detailed its initial plans to address referenced areas and to improve cybersecurity involvement in WMATA's procurements in line with OIG's recommendations.

WMATA IBOP is confident in its current programs and processes and welcomes the opportunity to improve and enhance its cybersecurity capabilities. IBOP concurs with the recommendations in the report and will proactively use OIG's recommendations to address each of the identified areas. IT recognizes the need to synchronize its current processes and procedures with Procurement to further develop and formalize cybersecurity within the procurement program, and IBOP will take the following corresponding actions by end of FY 2020 Quarter 1:

- Develop cybersecurity requirements for procurements
- Conduct penetration testing of existing procurements including the 7000-series railcar
- Update ongoing procurements including the RFP for the 8000 series railcars with cybersecurity requirements
- Amend existing procurement workflows in PeopleSoft to be inclusive of cybersecurity reviews and hire additional resources to support the change in process
- Develop a Policy Memorandum to include cybersecurity verbiage, references, or criteria that define the terms and conditions for acquiring goods and services
- Develop a specific cybersecurity awareness training for the Office of Procurement

Washington
Metropolitan Area
Transit Authority

Audit of WMATA's Cybersecurity over Rail Industrial Control Systems – Review of Cybersecurity Requirements in WMATA's Procurements
Page 2

OIG Recommendations & Management Response:

1. Develop cybersecurity requirements for procurements.
    a. IBOP accepts this recommendation. IT will create guidance for procurement professionals describing the language that must be included in every contract, as well as targeted language that may be included based on the products or services being procured.

       The guide will be circulated for comment, review and ultimate approval prior to implementation. Estimated completion date for this cybersecurity procurement guide is March 29, 2019.

2. Conduct cybersecurity risk assessments; identify and test the effectiveness of controls; and implement mitigation strategies for applicable existing WMATA contracts.
    a. IBOP accepts this recommendation. Funding has currently been approved for a penetration test of the 7000-series railcar. While it is too late to affect the procurement, we will be able to leverage this test to identify any severe cybersecurity vulnerabilities in those cars and begin the process of remediation.

       Penetration testing will be completed by August 30, 2019.

3. Immediately update the RFP for the 8000 series railcars with cybersecurity requirements.
    a. IBOP accepts this recommendation. After extensive coordination, the RFP for the 8000 series railcars was updated to include industry standard cybersecurity language, as well as industry leading requirements in the following areas:
        i. The modification of the debarment and suspension language (already part of the RFP) to clarify that those clauses flow down not only from contractor to subcontractors at any tier, but to the manufacturers of hardware, software and firmware that are installed on the railcars. This flow allows Metro to execute all contract options should we discover any devices or code that fall into the category of malware.
        ii. Mandating an independent third-party assessment of all code included as part of the contract at several key stages of contract progression.
        iii. Mandating an independent third-party penetration test of completed railcars at several key stages of the contract.

       We are not aware of any other major purchase in the federal or private industry that includes such aggressive protective measures. This amendment was issued to the public on February 6, 2019.

4. Define and implement a process to ensure future applicable procurements include specific cybersecurity requirements.
    a. IBOP accepts this recommendation. A review point will be added to the existing workflow within PeopleSoft CLM to ensure all procurements have completed a cybersecurity review. Due to the large amount of procurements that are handled by WMATA daily, additional dedicated resources will be required to adequately support the change in workflow.

       The change in workflow and hire of additional resources will be completed by August 16, 2019.

5. Create policies and procedures for managing and overseeing cybersecurity requirements for procurements.
    a. IBOP accepts this recommendation. Cybersecurity verbiage, references, or criteria that define the terms and conditions for acquiring goods and services will be issued by IT Cybersecurity. Procurement will develop a Policy Memorandum to guide procurement staff on routing procurements through IT Cybersecurity and update the solicitation templates with any required language.

       The Policy Memorandum will be issued by May 31, 2019.

6. Develop specific cybersecurity awareness training for the Office of Procurement and Materials.
    a. IBOP accepts this recommendation. Upon completion of the above recommendations, a targeted cybersecurity awareness training will be mandated for all relevant stakeholders.

       The cybersecurity awareness training will be mandatory for existing Procurement personnel and will be an onboarding requirement for any new personnel. The cybersecurity awareness training will be made available by August 30, 2019. All mandated personnel will have four weeks to complete this training (September 27, 2019).