

Public Audit Report

2017 – 0045

Jefferson Parish

Water Department-Physical Security

OFFICE OF INSPECTOR GENERAL JEFFERSON PARISH



PUBLIC AUDIT REPORT

WATER DEPARTMENT-PHYSICAL SECURITY

2017-0045

AUDIT SECTION
ISSUED 12/4/2018



OFFICE OF INSPECTOR GENERAL
JEFFERSON PARISH

DAVID N. McCLINTOCK
INSPECTOR GENERAL



DATE: 12/04/2018

TO: The Citizens of Jefferson Parish

FROM: David McClintock, Inspector General

RE: Audit Report #2017-0045, Jefferson Parish Water Department-Physical Security

Honorable Chairman and Members of the Ethics and Compliance Commission:

The Jefferson Parish Office of Inspector General (JPOIG) performed an audit on the Physical Security of the Jefferson Parish Water Department. The objectives of this audit were to provide assurance that:

- Evaluate the overall physical security of the facility.
- Survey the facilities existing security assets.
- Determine the existence and status of security protocols over increased risk storage areas.
- Review the employee access card system and analyze the integrity of issued credentials, permissions, and access card management protocols.

The results of this audit indicated that the Parish is not maintaining a minimally acceptable level of physical security oversight, even amongst its critical infrastructure facilities.

Based upon the data analysis, the JPOIG reached four (4) separate findings. Each finding has accompanying recommendations to the Parish. The findings and recommendations follow in Attachment A.

The draft report, dated 10/14/2018, was directed to the Parish President, all Parish Councilmembers, and the Parish Attorney. One request for an extension of time to provide a response was received and was granted.

The JPOIG received a written response to the audit report from the Administration on 11/16/2018. This response was made a part of the final report (*See* Attachment D.) In its response, the Administration outlined a corrective action plan with an estimated completion date in late 2019. It should also be noted that the Administration stated it is currently addressing perimeter fencing and surveillance camera issues, and has established and achieved a baseline level of security for the Water Department.

The JPOIG would like to thank the management and staff of the Water Department, the Security Division, and the Administration for their assistance and cooperation throughout this audit.

Sincerely,



David McClintock
Inspector General

c c :

Honorable Michael S. Yenni, Parish President
Keith A. Conley, Chief Operating Officer
Natalie D. Newton, Deputy Chief Operating Officer
Jeremy Dwyer, Parish Attorney
Honorable Steve D. Caraway, Chief Administrative Assistant
Chairwoman Cynthia Lee-Sheng, At-Large "B"
Councilman Chris Roberts, At-Large "A"
Councilman Ricky J. Templet
Councilman Paul D. Johnston
Councilman Mark D. Spears, Jr.
Councilman Dominic Impastato
Councilwoman Jennifer Van Vrancken

WATER DEPARTMENT-PHYSICAL SECURITY 2017-0045

Table of Contents

EXECUTIVE SUMMARY	001
OBJECTIVES, SCOPE, AND METHODOLOGY	003
Objectives	003
Scope & Methodology.....	003
Acronyms	003
BACKGROUND	004
DATA REVIEW & ANALYSIS	006
East bank Water Complex Security.....	006
West Bank Water Complex Security.....	008
The Security Division.....	010
Physical Security Best Practices.....	013
Benchmarking Physical Security Best Practices.....	016
Conclusion.....	017
ATTACHMENTS	018
Attachment A: Findings and Recommendations.....	018
Finding #1 Water Department Physical Security.....	019
Finding #2 Unauthorized Employee Badge Access.....	020
Finding #3 Security Requirements Not Followed.....	021
Finding #4 No Baseline Security Requirements in Effect.....	022
Attachment B: Security Measures By Location.....	023
Attachment C: Security Ordinance JPCO 2-515.16.....	025
Attachment D: Administration Response and Action Plan.....	027



OFFICE OF INSPECTOR GENERAL JEFFERSON PARISH

DAVID N. McCLINTOCK
INSPECTOR GENERAL



EXECUTIVE SUMMARY

The Jefferson Parish Office of Inspector General (JPOIG) has completed an audit of the Jefferson Parish Water Department physical security measures. The audit was initiated based upon information received concerning physical security at the East Bank Water Complex (EBWC). The EBWC is considered a critical infrastructure facility and should be afforded an adequate baseline level of protection.

Objectives

The objectives of this investigation were to:

- Evaluate the overall physical security of the facility.
- Survey the facilities' existing security assets.
- Determine the existence and, when relevant, the status of security protocols over access to increased risk storage areas.
- Review the employee access card system and analyze the integrity of issued credentials, permissions, and access card management protocols.

Audit Results

The JPOIG observed weaknesses in the perimeter security and internal security of sensitive chemical storage areas within the Water Department. The JPOIG found no evidence that Parish ordinances requiring annual inspections, assessments and evaluation of Parish facilities, including those representing critical infrastructure, have been performed as required by the Department of Security. The audit indicated instances of under-secured facilities/areas, inoperable security equipment and erroneous active access credentials for retired and terminated employees.

Recommendations

The JPOIG issued four (4) findings.

1. Water Department Physical Security
2. Unauthorized Employee Badge Access
3. Security Requirements Not Followed
4. No Baseline Security Requirements in Effect

Findings 1 through 3 generally address failures of the Parish Administration's Department of Security to perform security-related obligations pursuant to existing law. The 4th addresses a weakness in the existing system that does not mandate a department adopt a baseline level of security as "recommended" by the Department of Security. This latter recommendation may be addressed by the Administration through policy or the Council by ordinance.

The JPOIG findings and recommendations follow the report and are found at *Attachment A*.



OFFICE OF INSPECTOR GENERAL
JEFFERSON PARISH

DAVID N. McCLINTOCK
INSPECTOR GENERAL



Date of Report: 11/20/2018	PUBLIC AUDIT REPORT	Case # 2017-0045
Timeframe: 11/27/2017 - 06/30/2018		Report By: Jim Mitchell
<u>Subject of Audit</u> Jefferson Parish Water Department-Physical Security		
<u>Confidentiality Notice</u> This confidential report is issued by the Inspector General pursuant to the authority conferred by JPCO 2-155.10. It is intended for the sole use of the named recipients. It is not intended to be read, disclosed, reproduced, distributed, disseminated, in whole or in part by anyone other than the recipients. The report may contain confidential information, information which would not be subject to public records request, and/or information which is subject to other agreements of confidentiality and nondisclosure.		

INTRODUCTION

Pursuant to JPCO§2-155.10(11) (a), the Jefferson Parish Office of Inspector General (“JPOIG”) initiated an audit of Water Department operations. The audit was undertaken based upon confidential information concerning personnel and facility security. This audit was conducted in accordance with the Association of Inspectors General (“AIG”) Standards.

As part of this audit, the JPOIG tested the accuracy of the Parish’s physical access cards with an initial focus on the Water Department. The results of the testing demonstrated significant weaknesses in several departments. Thus, and in accordance with AIG Standards and pursuant to the JPOIG Policy 2-7-1, *Reports to Appropriate Officials*, the JPOIG issued a confidential management letter dated 04/09/2018 addressing specific security concerns relating to the Water Department.¹ On or about 04/10/2018, the JPOIG staff met with Directors of the Security Division and the Water Department. The Water Department Director acknowledged the concerns, and the Security Division Director prepared an action plan by way of a management memorandum that incorporated recommendations.

¹ JPOIG Policy 2-7-1, *Reports to Appropriate*, provides at Section IV that the “JPOIG will inform appropriate individuals as soon as possible, consistent with confidentiality requirements of credible allegations or other evidence of a significant and immediate danger to the health or safety of people or property.

OBJECTIVES

The objectives were to:

- Evaluate the overall physical security of the facility.
- Survey the facilities existing security assets.
- Determine the existence and, when relevant, the status of access security protocols for increased areas within the facility.
- Review the employee access card system and analyze the integrity of issued credentials, permissions, and access card management protocols.

SCOPE & METHODOLOGY

The scope of this audit considered existing security systems within the Jefferson Parish Water Department's facilities. The report discusses Parish security processes and systems. However, the scope of this audit does not include assessments or determinations of specific measures needed or taken.

To accomplish this audit, the following was undertaken:

- Conducted interviews of Water, Security, and Electronic Information Systems Department management and staff;
- Reviewed applicable Louisiana water quality regulations;
- Reviewed Parish, U. S. Department of Homeland Security (DHS), EPA, and professional association guidelines for physical security;
- Conducted onsite visits to observe plant operations;
- Reviewed duties and responsibilities of the Director of Security Division as it pertained to facility security, employee access, and contract management;
- Performed a benchmarking study of physical security protocols at other water treatment facilities.

Acronyms

ACL	Access Control List	EIS	Electronic Information Systems Department
AWWA	American Water Works Association	JPCO	Jefferson Parish Code of Ordinances
CCTV	Closed circuit television	JPSO	Jefferson Parish Sheriff's Office
CRT	Cathode ray tube (older design for televisions and computer monitors)	NIPP	National Infrastructure Protection Plan
DBT	Design basis threat	PTZ	Cameras with ability to Point, Tilt and Zoom
DHS	U. S. Department of Homeland Security	SCADA	Supervisory Control and Data Acquisition
EBWC	East Bank Water Complex	WBWC	West Bank Water Complex
EPA	U. S. Environmental Protection Agency		
GOHSEP	Governor's Office of Homeland Security and Emergency Preparedness		

BACKGROUND

A. Water Department

The Jefferson Parish Water Department is one of several Parish departments which collectively comprise Jefferson Parish Public Works.² The Water Department functions include a river intake; pump stations; treatment facilities, above and underground storage and clean water distribution. It has a current budget of \$39.5 million. See Table 1.

Table 1	Budget for Consolidated Waterworks District #1			
	2016 Actual	2017 Adopted	2017 Amended	2018 Adopted
Expenditures	\$34,633,429	\$38,385,023	\$42,286,398	\$39,515,599
Positions	269	269	269	269

The Water Department employs approximately 269 employees who work across four (4) shifts to ensure operations 24 hours/day and 7 days/week. These employees include 14 scientific professionals who monitor and maintain water quality, and perform over 80,000 analyses annually.

The Water Department operates water purification complexes on the East bank and West bank of the Mississippi River, as well as, a distribution system of approximately 1,600 miles of water mains.

The East Bank Water Complex (“EBWC”) is located at 3600 Jefferson Highway and houses four water purification plants which can process up to 87 million gallons of potable water for the East bank. The complex is bounded by Jefferson Highway, Arnoult Street, River Road, and adjacent residential properties on Lions Street See Image #1.

Image 1 – East Bank Water Complex



The West Bank Water Complex (“WBWC”) is located in Marrero. The WMWC is bounded by the West Bank Expressway, Avenues C, D, and 7th Street See image 2.

² Other Public Works departments include Drainage, Sewerage, Streets, Parkway, Environmental Affairs, and Engineering.

Image 2 – Westbank Water Complex



B. Security for water treatment complexes – Jefferson Parish Security Division

The Security Division provides services designed to “optimize the protection of employees, visitors, and property by providing a Threat/Risk analysis of all parish wide operations, facilities, [and] properties . . . in order to identify all critical infrastructure vulnerabilities to prevent the loss of life, loss of property, loss of operation by reducing the threat and risk from acts of violence and theft.”³ The 2018 budget for the Security Division was \$2.3 million. The Water department is one of several departments whose dedicated tax revenue supports the budget of the Security Division, in exchange for operational guidance and support.⁴ Maintaining the overall operational security of water and waste systems is the responsibility of Parish government. Therefore, the Parish established the Security Division to fulfill that function.

The Water Department is part of the Water and Wastewater Systems Critical Infrastructure Sector designated by the Patriot Act and the DHS.⁵ The physical security and the resilience of critical infrastructure assets, systems, and networks are also the subject of the National Infrastructure Protection Plan (NIPP).⁶

³ 2018 Annual Budget, p. 474.

⁴ Revenue is generated from charges for service based on square footage covered by the security system. 2018 Annual Budget, p. 474.

⁵ P.L. 107-56 and the U.S. Department of Homeland Security site at <https://www.dhs.gov/water-and-wastewater-systems-sector>

⁶ U.S. Department of Homeland Security - NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. The goals of the NIPP are to: (1) assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure. Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments; (2) enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services; (3) Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and (4) promote learning and adaptation during and after exercises and incidents. Implementation of the NIPP depends on a collaborative public-private partnership that operates as a unified national effort, recognizes multi-level authorities, responsibilities, and regulations. In addition, the Bioterrorism Act of 2002 requires all public water systems serving 3,300 or more conduct a vulnerability assessment, and submit a response plan to the U. S. Environmental Protection Agency (EPA). P.L. 107-188

DATA REVIEW & ANALYSIS

A. East bank Water Complex ("EBWC") Security

There were two security incidents in the Fall of 2017 involving the EBW. Both involved threats to facility staff that were not related to the facility operations.

The JPOIG staff completed a site visit of the EBWC on 04/25/2018. The JPOIG observed and assessed the physical security of the EBWC in the context of this audit. The EBWC physical security measures consist of controlled access measures, external physical barriers and video surveillance.

1. Controlled access measures include:

- A mechanical gate on the Arnoult Street side of the property, which serves as the main entry point to the facility. See image 3. Employees can gain access by either swiping an ID card or entering a code into the keypad.
- An electronically controlled door on the Arnoult Street side of the facility that access the chemical lab. See image 4.
- Controlled doors with swipe card access to the Ammonia and Chlorine storage rooms at the newer treatment plants on the River Road side of the complex See images 6 & 7.

All fencing and restricted access locking mechanisms appeared to be in functional condition.

2. External physical barriers include:

- [REDACTED]

3. Video surveillance measures include:

- The ability to monitor all exterior and interior closed circuit cameras from the [REDACTED].
- Exterior camera [REDACTED],
- Interior chemical storage cameras [REDACTED].

The JPOIG was informed by EBWC staff that currently the following security cameras were not functional:

- River intake station,
- Chlorine rooms at both the new and old facilities, and
- Ammonia rooms at both the new and old facilities.

Security cameras at the main gate on Arnoult Street and the entrance call box.

Image 3 – Arnoult St. Gate



Image 4 - Arnoult St Door



Image 5 - Jefferson Hwy.



Chemical Storage Access

During the site visit, the JPOIG staff observed locked doors for the ammonia and chlorine rooms with swipe or key code access. See images 6 & 7.⁷ However, there are no controls or operating cameras [REDACTED].⁸

Operations control area

The JPOIG also observed doors with swipe card access to the operations control area located on the upper floor of the new treatment plant on the river side of the complex See image 8 below. Operators in this facility can monitor via closed circuit video the main gate and the Arnoult Street door from the control area. However, the main gate closed circuit video was not operational for approximately 30 days during gate repairs.

There are no other exterior cameras along the perimeter, or at the non-potable water holding tanks.

Image 6 - Ammonia Room



Image 7 - Chlorine Room



⁷ The JPOIG team did not tour the older water treatment facility on the Jefferson Highway side of the complex.

⁸ [REDACTED]

Security Incidents at EBWC

In the Fall of 2017, there were two security incidents involving threats to the facility staff that did not involve facility operations.⁹ Both matters occurred during a period when the Arnoult Street gate was inoperable and left open.

Delays in repairs to the gate resulted in the Water department contracting with a guard service during the period when the gate remained inoperable at a cost of \$1,347. Gate repairs were completed in January of 2018 at a cost of \$26,346. Additionally, the incidents resulted in JPSO details at both East and West bank facilities at a cost of \$11,220.

Image 8 - Operators Control Area



Table 2 Costs Associated with Security Incidents				
Description	Amount	Identified ¹⁰	Questioned ¹²	Avoidable ¹³
Guard Services	1,347	0	0	0
JPSO Details	11,220	0	0	11,220
Gate repairs	26,346	0	0	0
Totals	38,913	0	0	11,220

B. West bank Water Complex (“WBWC”) Security

The JPOIG staff visited the West Bank Water Complex (WBWC) on 05/16/2018 to compare measures with the EBWC. The WBWC, built in 1971, has a smaller footprint than the EBWC.

⁹ The Jefferson Parish Sheriff’s Office (JPSO) was notified and addressed both matters.

¹⁰ These are unallowable expenditures that are recoverable. These unallowable expenditures have been documented as being not supported by law, regulation, contract, grant, agreement, or other document. Identified costs are not curable. Identified amounts may be revenues either not collected, or improperly recorded in the books and records of the agency or department under audit.

¹¹ These unallowable expenditures have been documented as being not supported by law, regulation, contract, grant, agreement, or other document. Identified costs are not curable. Identified amounts may be revenues either not collected, or improperly recorded in the books and records of the agency or department under audit.

¹² Questioned Costs: are potentially allowable expenditures that are questioned due to a lack of supporting documentation; a potential legal issue, or are considered unnecessary or unreasonable. Questioned costs may be curable.

¹³ Avoidable Costs: are a projection of costs over a three year period, or other term based on existing agreements, if the issue is not modified or corrected. The above table of identified, questioned, and avoidable costs are based upon discussions with management and review of invoice detail. However, because security incidents have not occurred on a frequent or predictable basis, we believe that it is not practical to project these costs over three years.

Image 9 – Ave D



Image 10 Ave D.



Controlled access measures and physical barriers

The WBWC has mechanical gates on the Avenues C, and D sides of the property. Employees can gain access by either swiping an ID card or entering a code into the keypad. Visitors can use the keypad to call specific personnel in the plant. Six foot fencing topped by barbed wire secures most of the WBWC perimeter. There is wrought iron style fencing on the West Bank Expressway side, and wood fencing along Avenue D. See images 9 &10.

However, unlike the EBWC, the WBWC has public access to the customer billing office on the WestBank Expressway side of the property. See image 11.¹⁴

Video surveillance

The WBWC perimeter camera [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] have operating cameras accessible to operators in the control area. However, the monitors are of the older CRT design. See image 12.

Image 11- West Bank Water Complex



Image 12 - Security Monitors



¹⁴ The JPOIG did not tour the billing office because it is separate from plant operations. However, Water management did inform the JPOIG that the billing office has multiple internal cameras to observe customer transactions.

C. The Security Division

Parish security, including security of physical facilities as well as employees, is a function of the Security Division. The division is funded to perform the following nonexclusive functions:¹⁵

- Card swipe access systems;
- Employee Identification Card Systems; and
- Closed circuit video surveillance.

The responsibility for overseeing these systems is with the Director of Security. The duties of the director for the Security Division are established by Parish ordinance.¹⁶ These duties include by way of example:

- Overall security of employees and facilities of Jefferson Parish;
- Annual physical inspection of every parish owned or operated facility. The inspection will identify any potential security risks and provide recommendations on means and methods to reduce loss due to thefts and criminal conduct;
- Coordinate with local, state and federal law enforcement agencies on matters of criminal investigations and intelligence gathering on matters involving parish employees or facilities.¹⁷

The position has been occupied by Mr. Gary Hargroder since 2016. The Director of Security is appointed by the Parish President and reports to a Chief Administrative Assistant, the Honorable Steve Caraway. During the course of our audit and as set forth above, the JPOIG found that the Director of Security was not able to provide documentation or otherwise demonstrate that several functions mandated by Parish Code had been performed during his tenure.

Annual Physical Inspections

The JPOIG found no documentation or evidence that annual physical inspections were completed of Parish facilities to identify potential security risks and provide recommendations as required by JPCO 2-515.16. (6). The JPOIG did identify a few examples where the Director of Security was requested by a Department to respond to a specific security incident. However, in those instances no documented evaluative process was applied and no written assessment could be provided.

The Parish owns or operates 322 facilities, with an additional 147 structures within larger properties (such as parks and sewage treatment complexes). While the JPOIG does not see evidence of an imminent threat to the EBWC or WBWC, the lack of vulnerability assessments deprives the Parish of the opportunity to meaningful preventive measures. The result is that critical infrastructure is at risk.

Employee Identification Cards/Access

Overseeing the Parish card swipe access system is also a function of the Security Division. Security Division staff manages and maintains a parish-wide employee identification system,

¹⁵ 2018 Annual Budget, p. 474.

¹⁶ The position of the Director of Security was created by the Parish Council via Ordinance No. 23288 on 04/23/2008. The qualifications and responsibilities are set forth in detail at JPCO Sections 2-515.14-16.

¹⁷ JPCO 2-515.16, *duties of director of security*.

which includes the issuance and maintenance of employee’s facility access swipe cards, and closed circuit video surveillance within Parish facilities.

Under the Parish card access system, an employee must have an active employee swipe card to gain access to certain points of entry. The JPOIG assessed the protocols and tested the integrity of the employee identification swipe cards issued to the EBWC and WBWC employees. The JPOIG compared the employee permission coded onto the access cards with current payroll records. Based upon this comparison, the data revealed that 32 retired employees and 88 terminated employees had active employee swipe access cards. See Table 3.

Table 3 Former Water Employees with Security Access				
	April 2018		July 2018	
Location	Retired	Terminated	Retired	Terminated
East Bank	17	42	1	1
West Bank	15	46	0	0
Totals	32	88	1	1

The security data above contained instances of multiple credentials still assigned to terminated employees, and multiple active cards assigned to terminated employees.

Further, the JPOIG identified 79 active credentials that were not assigned to a specific individual. The existence of active access credentials, not assigned to a specific individual, creates an unnecessary weakness in overall security for the EBWC. The JPOIG can foresee the need for temporary access in some instances; however, unused valid access credentials creates a significant security risk to the EBWC.¹⁸

The JPOIG completed a follow-up review of credential assignments on 07/11/2018 and notes that the Security Division did adequately address the exceptions and is currently establishing a validation protocol. See Table 2. Overall, the security weaknesses identified in the employee access system demonstrates a lack of effective controls and validation protocols.

Contract with the Security Equipment Company

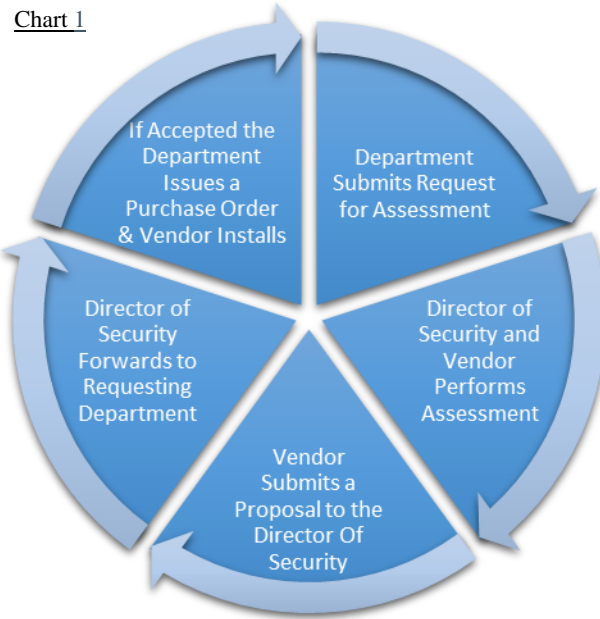
While the Security Division is responsible for identifying any potential security risks and providing recommendations, implementation of recommendations are left to the discretion of the department funding the security measure. In the absence of any policy or protocol to ensure implementation of needed security upgrades, the Security Division cannot fulfill its functions fully.

By way of example, the Security Division forwarded a quote to the Water Department in 02/2018 for \$57,221.32 in repairs and equipment related to the EBWC. The quote includes cameras to monitor the [REDACTED]

¹⁸ The JPOIG acknowledges that there may exist a valid reason for multiple credentials or cards. These include, by way of example: (1) a new credential may be assigned when an employee changes departments, or is re-hired and (2) multiple cards may be issued when an employee loses a card, later finds but does not return the original card. However and regardless of the reason, re-issuing cards should not present an overall threat to, or otherwise undermine, the security objectives intended to be met by the employee swipe card access system if proper validation is applied.

█. Due to concerns with quantity and price, the Water Department’s management has not taken action to approve any purchases based on the quote submitted. Thus, security measures proposed by the Security Division fall to the whim of the department receiving the necessary or added security measures.

As with the Water Department, security is a reactive, rather than, proactive process which is managed by the Security Division. A department may request repairs to, or new equipment, for security. Otherwise, a department may react to a specific instance. The request is received by the Security Division. Subsequently, an assessment, which involves the Parish’s vendor, is performed. Based upon the assessment, a proposal is made. If accepted, installation is approved by receiving department. See Chart #1. Under current Parish practices, the Security Division is a facilitator of security and not an initiator with the authority to plan or direct implementation.



The Parish has a \$2.9 million contract with New Era Technologies for the installation of security cameras at 59 buildings parish-wide.¹⁹ It is of import that the New Era contract is not only for hardware, but also includes site assessment and installation services.²⁰ This audit did not reveal any comprehensive plan of implementation or contract administration by the Security Division for security measures covered under the New Era contract with the Parish.

Additional security risks – cyber risk

In 08/2016, DHS cyber security team completed a review of Jefferson Parish Water Department security measures. The DHS team concluded that the Water Department had good physical protection, a working backup recovery process for its systems, and a skilled group of professionals with a healthy understanding of their information systems and operating technology environment. However, the primarily focus of the assessment was cyber security. The report outlined a number of cybersecurity weaknesses. The scope of this audit did not extend to cyber security in light of the recent DHS assessment. Consideration of any corrective action plan on the DHS reported concerns relative to cyber security may be included in a JPOIG follow-up.

¹⁹ Effective dates of contract is from 12/05/2017 through 12/05/2019.

²⁰ Administration of the contract necessarily involves delivery of services to the end user departments and coordination with the Parish Electronic Information Systems Department (EIS). For security purposes, EIS involvement is mostly limited to providing Internet Protocol (IP) addresses for new equipment at the time of installation.

D. Physical Security Best Practices:

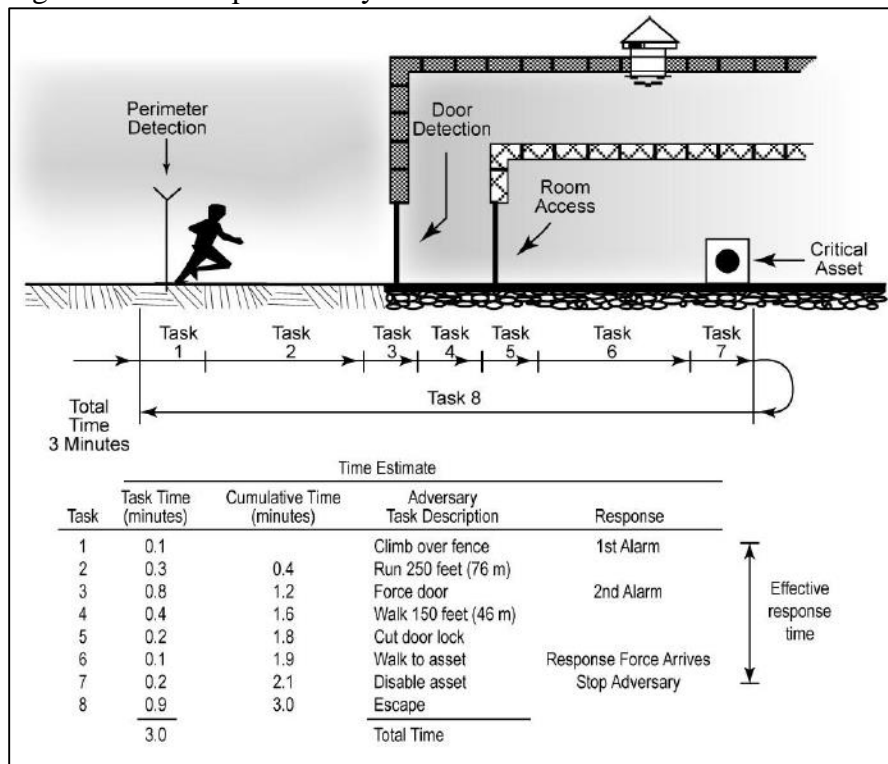
The JPOIG reviewed open source guidelines and best practice material that included a draft resources guide to water and wastewater facilities from the Governor’s Office of Homeland Security and Emergency Preparedness (GOHSEP), as well as, studies from the American Society of Civil Engineers (ASCE) and from a consortium of water agencies in the State of Oregon. Both studies recommended conducting a vulnerability assessment of facilities considering the size, type of threat, and desired level of protection before implementing any improvement plans.

The ASCE and the American Water Works Association (AWWA) published their guidelines in 2006 for physical security of water facilities based the concept of “design basis threats” or DBTs.²¹ These guidelines discuss four elements of a physical protection system:

- Deterrence by the presence of lighting, closed circuit television (CCTV), visible facility with no obstructions,
- Detection by installation of sensors, cameras, and alarms,
- Delay of entry by physical barriers, and other “hardening” devices,
- Response of facility staff and law enforcement.

The ASCE also developed a model illustrating the maximum time an agency would have to respond to an adversary’s sequence of actions. See Figure 1. The guidelines also define four differing threats areas including vandalism, criminal activity, terrorism and action by insiders.

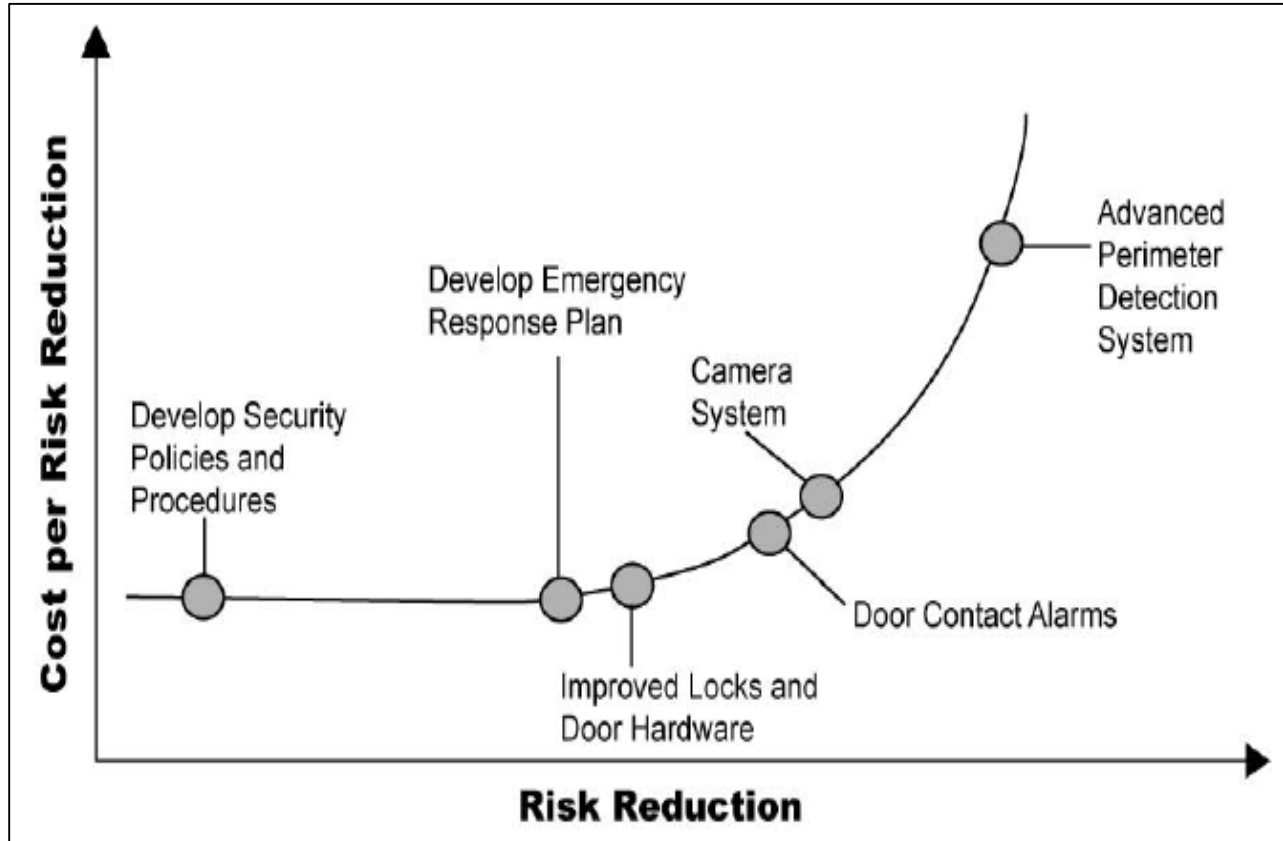
Figure 1 - ‘Concept of Delay’ Calculation



²¹ Guidelines for the Physical Security of Water Utilities, December 2006

The ASCE/AWWA also developed matrices that recommend physical security measures for the perimeter, areas between the perimeter and different types of internal facilities, structures, water quality monitoring, CCTV, power and wiring, and Supervisory Control and Data Acquisition (SCADA) systems. The ASCE study illustrated the different security risks for raw water intake locations, pumping stations, water treatment facilities, finished water storage, and distribution systems. The study also presented a cost reduction curve as tool to guide to determine the point at which the risk reduction associated with implementing additional security measures is marginal. See figure 2.

Figure 2 - Cost To Risk Reduction Curve



The State of Oregon, in association with the water departments in the Cities of Portland, Gresham, and the District of Tualatin Valley published a guide designed to provide operators a reference for evaluating their systems physical security and resources to improve security²² See Table 4 below.

²² *Physical Security for Drinking Water Facilities, December 2009 – State of Oregon*
Page 13 of 16

Table 4 - Physical Security Measure by Level of Security

Security Measures	Minimum recommended measures by Risk Level		
	Low	Medium	High
Perimeter			
Fencing			
No Trespassing signage every 50 feet			
Height greater than 6'			
Barbed or concertina wire			
tunneling resistant			
Climb / cut resistant			
Climb / cut sensors			
Gates with locks and alarms			
Keycard access			
Manned gates			
Lighting - always on			
Lighting - motion sensor activated			
Bollards or Jersey barriers to limit vehicle access			
Clear sight zones around entire perimeter			
No shrubbery or trees within 25 feet of fencing or structures			
Inner facility			
Motion activated lighting			
Commercial quality solid core wood or steel doors			
Commercial quality locks and hardware			
Roving guard patrols			
Alarms on all entry points to critical components or finished water			
CCTV of critical equipment and associated entry points			
Optional Measures			
Routine LEO patrols			
Emergency Responder familiarity with facilities			
Key control program			
Employee turnover/termination protocols			
Background checks for employees			

The guide emphasizes the development of protocols addressing employee turnover and terminations. These protocols include:

- Key issuance and collection,
- Password change requirements for computers and SCADA systems,
- Return of utility issued equipment.

The guide shares similar concepts as the ASCE guide, but presents a more simplified matrix listing of recommended security measures according to the level of security necessary for a facility.

E. Benchmarking Physical Security Best Practices

In visiting other area water treatment facilities, the JPOIG noted security processes that may guide the Parish in refining a process for assessing security risks to critical infrastructure. In one instance, the JPOIG learned that there was a dedicated team of security personnel with direct responsibility for security oversight, augmented by security contracts as needed. The process differed from the Parish, which acts in an advisory capacity, notwithstanding the mandated responsibilities of the Security Director set out by ordinance.

Cameras

The JPOIG also observed other facilities utilizing point, tilt and zoom (PTZ) cameras along perimeter and sensitive areas within the perimeter, as well as, within structures requiring higher security such as the chemical storage and operations areas. The use of cameras specifically mounted to record data on entering and exiting vehicles was also noted.

Physical Security Measures

The JPOIG observed the use of additional physical security measures in use at other facilities. These included the use of speed bumps along internal drives within the treatment facilities, additional fencing and Jersey style barriers to protect other infrastructure such as fuel tanks within the perimeter, bollards installed along public roadways near storage tanks and other critical areas.

Entry Procedures

The JPOIG also observed processes that more tightly controlled and documented ingress and egress to other facilities. These included the requirement that non-employees provide identification upon check-in and recordation of the license plate for all incoming vehicles. Additionally, the JPOIG staff observed the use of temporary dashboard placards to visually designate temporary approval of vehicles on the grounds.

Jefferson Parish-Wide Physical Security

The Security Division is responsible for the overall security of the employees and facilities of the Parish. We acknowledge the Department's prompt action to address the security card access issue in the Water Department. However, after review of existing policies, procedures, and consultation with management, the JPOIG determined that all requirements of the security ordinance have not been completed.

V. Conclusion:

The Water Department has an important responsibility to ensure the availability and quality of drinking water in addition to ensuring the safety and security of its facilities. To date, recent incidents have not caused damage or disabled the EBWC. The Department currently has physical security measures in place at the Water Complexes that include fencing with barbed wire, clear sight zones, key and swipe card access and cameras at some locations. The Water Department also has begun working with Security on outdated credentials. The EBWC repaired the main electronic gate, and updated access for one chemical room.

As compared to the EBWC, other water facilities in the New Orleans region have more restrictive physical security measures according to the security checklist (Appendix A). The JPOIG considers the Water Department treatment plants at both East and West Bank complexes between medium and high risk, based on guidelines provided by the ASCE/AWWA and direct observation. Unfortunately, the EBWC security measures are currently at a lower risk level than the other facilities. We encourage the Water Department to bring EBWC security measures up to at least equal with the WBWC and consider the optional measures listed in Attachment B.

On a parish-wide level, we are concerned that security measures to assess and reduce risk for facilities are not being implemented. The JPOIG also recognizes the need for the Security Division to fulfill all the requirements of the parish ordinance.

Among our recommendations that follow at Attachment A, we have included immediate, medium, and longer term actions that Water Department management can implement not only at the East and West bank treatment facilities, but at the pumping stations and other key distribution locations.

Findings and Recommendations



FINDINGS AND OBSERVATIONS

An observation is the result of looking at a process or procedure being performed by others and is typically founded upon a specific time, or period, during which the observations takes place.

A finding indicates a material or significant weakness in controls or compliance that was not detected or corrected by an entity in the normal course of performing its duties. Findings can be any one or the combination of the following: (1) significant deficiencies in internal controls; (2) fraud and illegal acts; (3) violations of contracts and grant agreements; (4) waste; or (5) abuse. For certain internal control elements, the JPOIG has utilized the GAO's "Standards for Internal Control in the Federal Government" as a guide to... "improving accountability"... and promoting and implementing... "an effective internal control system."

Finding #1 Water Department Physical Security

Condition:

The JPOIG determined that security weaknesses exist at the EBWC. Further, the JPOIG saw no evidence that an annual inspection or associated recommendations had been made by the Department of Security.

Criteria:

The Security Division is tasked under JPCO 2-515.16 with various responsibilities to include inspections, recommendations, access control, video surveillance, and hazardous materials. Best practice studies from the American Water Works Association and the American Society of Civil Engineers recommend security measures be combined with management policies, operational procedures and network security systems that provide multiple layers of protection for critical assets.¹

Cause:

Water Department management recently completed an assessment of cybersecurity, but not a comprehensive assessment of physical security. The Parish Administration's Security Division management has taken limited actions to address gaps in physical security measures. Additionally, the Security Division does not have written policies and procedures addressing physical security.

Exposure:

Under-secured facilities represent increased risks. Further, an open, unmonitored, or under secured entrance or storage area increases the risk to employees, plant operations, and the public. As part of critical infrastructure, the Water Department is vulnerable to a variety of physical and cyber-attacks.

Recommendations:

Administration:

1. The Security Division's management, within 60 days, should:
 - o Complete an updated comprehensive assessment of physical security consistent with best practices for Water Department facilities.

¹ *Guidelines for the Physical Security of Water Utilities, December 2006* - American Society of Civil Engineers and the American Water Works Association

- Make recommendations to address areas identified in the comprehensive assessment. The recommendations should include baseline needs in addition to more proactive or intelligence led elements.
 - Utilize written and supported security assessment protocols as required in Finding #4.
2. Water Department management, within 90 days, should implement at a minimum baseline security measures as addressed in Finding #4.

Finding #2 Unauthorized Employee Badge Access

Condition:

There were many instances of multiple cards and active credentials issued to current, retired, and terminated employees in the security database (Table 1).

Table 1: Former Water Employees with Security Access

Location	April 2018		July 2018	
	Retired	Terminated	Retired	Terminated
East Bank	17	42	1	1
West Bank	15	46	0	0
Totals	32	88	1	1

Criteria:

The Security Division is tasked under JPCO 2-515.16 (11) with supervising the identification control divisions of the Parish. Further, the federal government’s specific plan for the water sector emphasizes that public and private water utilities prepare to prevent, detect and respond to and recover from physical and cyber-attacks.² The plan specifically identifies intentional malicious acts as a high risk to water treatment facilities. Additionally, the GAO Green Book states that internal threats may come from former or disgruntled employees. Those employees pose unique risks because they may be both motivated to work against the entity and better equipped to succeed in carrying out a malicious act as they have greater access to and knowledge of the entity’s security management systems and processes.³

Cause:

The Security Division is responsible for the overall management of the access control functions. No effective written policies, procedures, controls or validation processes are in place.

Exposure:

Valid security credentials in possession of terminated or retired employees presents an increased threat to plant operations, and may result in a breach of physical security within the Water Department. The JPOIG recognizes that the Security Division has made significant progress between April and June of 2018. However, vulnerabilities still exist as 2 former employees still have access to the EBWC (Table 1).

Recommendations:

² *Water and Wastewater Sector Specific Plan (2015)* – Department of Homeland Security and Environmental Protection Agency

³ *Standards for Internal Control in the Federal Government, September 2014* – United States Government Accountability Office

1. The Security Division's management should develop and implement written policies and procedures for the management of Parish access control. The written policies and procedures should include controls and validation processes that can applied in a routine manner.
2. The Security Division's management should provide lists of all active employees to each Department periodically for departmental validation. The JPOIG suggests quarterly.

Finding #3 Security Requirements Not Followed

Condition:

The Security Division's management could not provide evidence of the required annual inspections of all Parish owned facilities as required by parish ordinance. The Division provided evidence to support a limited number of site visits that were reactive in nature and driven by specific departmental requests.

Criteria:

Parish ordinance requires the Director of Security to perform an annual inspection of every parish owned or operated facility and provide identify potential security risks and provide recommendations to reduce potential losses.⁴

Cause:

Both the Director of Security and the Chief Administrative Assistant agree that all elements of the ordinance are not being addressed. Implementation of all the elements of the ordinance has thus far not been a priority. The Security Division currently has a budgeted complement of three.

Exposure:

The lack of current threat and vulnerability assessments of parish facilities deprives the Parish of the opportunity to proactively prevent threats, and creates an environment where the parish may be blindsided by a future physical security-related incident.

Recommendations (Administration):

1. The Parish President or his designee, within 30 days, complete a comprehensive review of the Security Division's performance against the legal mandates and authority to determine what areas are not being performed or performed satisfactorily. The review must extend beyond the limited areas of this review i.e. inspections, recommendations, supervision of the parish access controls, etc.
2. The Office of the Parish President, within 90 days, should implement a written action plan to ensure that the Security Division is compliant with the parish ordinance and/or adjust the ordinance to reflect more effective and attainable outcomes.
3. Require confidential reports on the status of Parish facility and employee safety be prepared and submitted by the Director of Security on an annual basis.

⁴ Jefferson Parish Ord. No. 23288, § 5, 4-23-08

Finding #4 No Baseline Security Requirements in Effect

Condition:

Although Parish ordinance requires the Security Division to assess security risks for Parish facilities annually, the ordinance does not require the Division to establish a baseline for the security measures at critical infrastructure facilities. In addition, department directors are not required to implement the recommendations of the Security Division.

Criteria:

Best practice studies from the American Water Works Association and the American Society of Civil Engineers recommend that security measures be combined with management policies, operational procedures and network security systems that provide multiple layers of protection for critical assets.

Exposure:

The lack of a baseline implementation of security measures for specific critical infrastructure facilities leaves the Parish less prepared to deter or prevent and respond to future security-related incidents.

Recommendations (Administration):

1. That the Security Division management should develop and adopt supportable security assessment protocols to be applied across the various parish facilities to include facilities that represent critical infrastructure.
2. That the Security Division management establish baseline levels of security for all critical parish infrastructure, facilities and departments.
3. The Parish Administration and/or Council should mandate, through policy or law, that each parish department implement a baseline level of security.

Attachment B

Physical Security Measures in Effect by Location



Security Measures in Effect by Location*	EBWC	WBWC
<u>Perimeter</u>		
Fencing		
No Trespassing signage every 50 feet		
Height greater than 6'		
Barbed or concertina wire		
tunneling resistant		
Climb / cut resistant		
Climb / cut sensors		
Gates with locks and alarms		
Keycard access		
Manned gates		
Lighting - always on		
Lighting - motion sensor activated		
Bollards or Jersey barriers to limit vehicle access		
Clear sight zones around entire perimeter		
No shrubbery or trees within 25 feet of fencing or structures		
<u>Inner facility</u>		
Motion activated lighting		
Commercial quality solid core wood or steel doors		
Commercial quality locks and hardware		
Roving guard patrols		
Alarms on all entry points to critical components or finished water		
CCTV of critical equipment and associated entry points		
<u>Optional Measures</u>		
Routine LEO patrols		
Emergency Responder familiarity with facilities		
Key control program		
Employee turnover/termination protocols		
Background checks for employees		
TOTAL Number of Security Measures in effect:		

*Overall, the WBWC and the SCPW have implemented security measures at a medium level. Comparatively, the EBWC currently has the lowest level of security measures in effect.

Attachment C

Security Ordinance JPCO 2-515.16. - Duties of Director of Security.



Jefferson Parish, Louisiana - Code of Ordinances
Chapter 2 - ADMINISTRATION ARTICLE V. - DEPARTMENTS
DIVISION 34. - DEPARTMENT OF SECURITY

Sec. 2-515.16. - Duties of director of security.

The director of security shall:

- (1) The director will be responsible for the overall security of the employees and facilities of Jefferson Parish.
- (2) The director will interface with local, state and federal agencies to insure that intelligence files are kept up to date on matters concerning parish government and the security of the parish president.
- (3) The director shall provide security during meetings and hearings with employees.
- (4) The director shall coordinate police details with the parish departments to provide security at parish facilities and events.
- (5) The director shall coordinate with local, state and federal law enforcement agencies on matters of criminal investigations and intelligence gathering on matters involving parish employees or facilities.
- (6) The director shall perform an annual physical inspection of every parish owned or operated facility. The inspection will identify any potential security risks and provide recommendations on means and methods to reduce loss due to thefts and criminal conduct.
- (7) The director shall conduct internal investigations on crimes reported by or committed upon parish employees or at parish owned or operated facilities.
- (8) The director shall conduct investigations of unethical conduct by parish employees while on duty or representing the parish.
- (9) The director shall provide recommendations on security measures including, video, access control and loss control prevention on new parish buildings and facilities.
- (10) The director shall oversee and administer the contract between Jefferson Parish and the security equipment company.
- (11) The director shall supervise the identification control divisions of Jefferson Parish.
- (12) The director shall attend Department of Homeland Security and Louisiana OHSEP classes annually on anti-terrorism, response to weapons of mass destruction and related courses.
- (13) The director shall oversee and administer the parish's contract with the private security guard company.
- (14) The director shall review inspection reports from the safety officer regarding access and security issues involving hazardous or controlled substances. The director will coordinate the development of corrective measures with the facility that was inspected and the safety officer.
- (15) The director shall be available to perform special assignments as directed by the chief administrative officer on an as needed basis.
- (16) The director of security shall report to a chief administrative assistant.

(Ord. No. 23288, § 5, 4-23-08)

Administration Response
and Corrective Action
Plan (CAP)





JEFFERSON PARISH

Office of the President

Michael S. Yenni
Parish President

Stephen D. Caraway
CAA

November 16, 2018

Jefferson Parish Office of Inspector General
Susan Andrews
5401 Jefferson Hwy., Suite C
Jefferson, LA 70123

Dear Susan,

Attached are corrective measures concerning issues your office identified during a Risk Manage Assessment of the Jefferson Parish Department of Water. As discussed previously several items are currently being addressed. Some additional camera technology will be completed in 2019 with the delay due to budget constraints.

Regards,

A handwritten signature in blue ink that reads "Steve Caraway".

Steve Caraway
Chief Administrative Assistant

A handwritten signature in blue ink that reads "Gary Hargroder".

Gary Hargroder
Director of Security

JPOIG CASE: 2017-0045

DESCRIPTOR: WATER DEPARTMENT SECURITY REVIEW

029

CAP #1

IDENTIFIED ISSUES: Security weakness exists at the EBWC. Further, no evidence that an annual inspection or associated recommendations had been made by the Department of Security.

CORRECTIVE MEASURES: Recommended adding to the number of security cameras already in place at the facility. Upgrading the technology of the surveillance equipment, allowing for enhanced capture and storage of surveillance footage. Controlled access to specific areas will be addressed.

TIME FRAME: Upgrades have begun.

TIME FRAME EXTENSION: Extension would only be required if funding is unavailable.

ACTION DEEMED SUCCESSFUL WHEN: Video surveillance upgrades and controlled access is completed.

MEANS OF EVALUATION: Regular updates from the Department Director and visual inspections by the Security Department.

NAME AND TITLE OF PERSON RESPONSIBLE FOR THIS ISSUE: Director of Security, Gary Hargroder.

CAP #2

IDENTIFIED ISSUES: Identified instances of multiple cards and active credentials issued to current, retired, and terminated employees in the Security Database.

CORRECTIVE MEASURES: Coordinating employee status with Parish Departments, Human Resources, and the Personnel Department concerning daily leave, disciplinary status, and any other employment status affecting employee access.

TIME FRAME: Protocol enacted.

TIME FRAME EXTENSION: None.

ACTION DEEMED SUCCESSFUL WHEN: Accurate daily updates are continuously provided by all departments involved.

MEANS OF EVALUATION: Cross-referencing of Security Department files with individual department and H.R. files.

NAME AND TITLE OF PERSON RESPONSIBLE FOR THIS ISSUE: Director of Security, Gary Hargroder.

CAP #3

IDENTIFIED ISSUES: Security Division has not completed the required annual inspections of all Parish owned facilities as required by Parish Ordinance.

CORRECTIVE MEASURES: Establish a security matrix to be used in security inspections by the Security Division. Provide inspection lists/surveys to be used by department directors.

TIME FRAME: Process has been implemented.

TIME FRAME EXTENSION: No extension at this time.

ACTION DEEMED SUCCESSFUL WHEN: All departments and facilities are inspected by the Security Director or Department Directors and all lists/surveys are completed as required.

MEANS OF EVALUATION: Monitor all departments and facilities by evaluation of security matrix and surveys.

NAME AND TITLE OF PERSON RESPONSIBLE FOR THIS ISSUE: Director of Security Gary Hargroder and Director of Water, Thomas West.

CAP #4

IDENTIFIED ISSUES: Establish a baseline for the Security measures at Critical Infrastructure Facilities.

CORRECTIVE MEASURES: Working with the Department of Homeland Security we have established a D.H.S. Dashboard app that aids in establishing security protocol and improvements. Working with Director West, perimeter security will be enhanced, and updated and additional surveillance cameras are being installed.

TIME FRAME: Perimeter security enhancements and internal upgrades to surveillance cameras has begun. Completion anticipated by end of year.

TIME FRAME EXTENSION: Late 2019 for the addition of perimeter cameras due to budget constraints.

ACTION DEEMED SUCCESSFUL WHEN: All technology and perimeter upgrades are complete.

MEANS OF EVALUATION: Completion and evaluation of security matrix and surveys.

NAME AND TITLE OF PERSON RESPONSIBLE FOR THIS ISSUE: Director of Gary Hargroder and Director of Water, Thomas West

From: [Steve Caraway](#)
To: [Jim Mitchell](#)
Cc: [Susan Andrews](#)
Subject: RE: Security Response on the Water draft report
Date: Monday, November 19, 2018 9:25:58 AM

Jim, the Department of Security and Water Dept. have begun the process of updating the camera technology at the facility. The camera updates, removal of overgrown weeds along the fence line, and replacement of barbed wire is currently being done and should be completed soon. The addition of [REDACTED] security cameras is expected to begin and be completed in 2019. The reason for this delay is due to budget constraints. Also, the addition of a Neutral Zone or Perimeter Road is also being planned. This Neutral Zone is also something that cannot be completed until the funding can be obtained.

Jim, as I mentioned in our conversation this morning the Security Department has also changed the process for issuing and monitoring security access cards. This applies to all departments, not just water. I believe the Water Department has established it's baseline level of security.

From: Jim Mitchell [mailto:jmitchell@jpoig.net]
Sent: Friday, November 16, 2018 1:54 PM
To: Steve Caraway <SCaraway@jeffparish.net>
Cc: Susan Andrews <sandrews@jpoig.net>
Subject: Security Response on the Water draft report

Steve,

Thank you for the response. We appreciate Gary's personal attention. However, we need clarification on CAP #4 (Baseline for Security Measures):

- Have the facilities at the Water Department highlighted in the report achieved the established baseline level of security?
- If not, are the measures listed specific to the Water Department, and
- Is the timeframe for achieving the *baseline* level the end of this year, or late 2019?

Thanks again,

Jim

Jim Mitchell, MPA, CIGA
Auditor

Office of Inspector General
Jefferson Parish
5401 Jefferson Highway, Suite C
Jefferson, Louisiana 70123
Office: (504) 736-8962 Ext. 422

Fax: (504) 736-8963

CONFIDENTIALITY NOTICE: This e-mail and its attachments may be privileged and confidential. It is for the sole use of the intended recipient(s). If you have received this transmission in error, you are directed to delete it from your system. It is not to be read, disclosed, reproduced, distributed, disseminated, or otherwise used. Delivery of this message to anyone other than the intended recipient(s) is not to be construed in any way to waive privilege or confidentiality. Please notify sender by reply e-mail to jmitchell@jpoig.net if you have received this transmission in error.

LA PUBLIC RECORDS NOTICE: Please be advised any information provided to Jefferson Parish Government may be subject to disclosure under the Louisiana Public Records law. Information contained in any correspondence, regardless of its source, may be a public record subject to public inspection and reproduction in accordance with the Louisiana Public Records Law, La.Rev.State. 44:1 et seq.

Please be advised any information provided to Jefferson Parish Government may be subject to disclosure under the Louisiana Public Records Law. Information contained in any correspondence, regardless of its source, may be a public record subject to public inspection and reproduction in accordance with the Louisiana Public Records Law, La. Rev. Stat. 44:1 et seq.