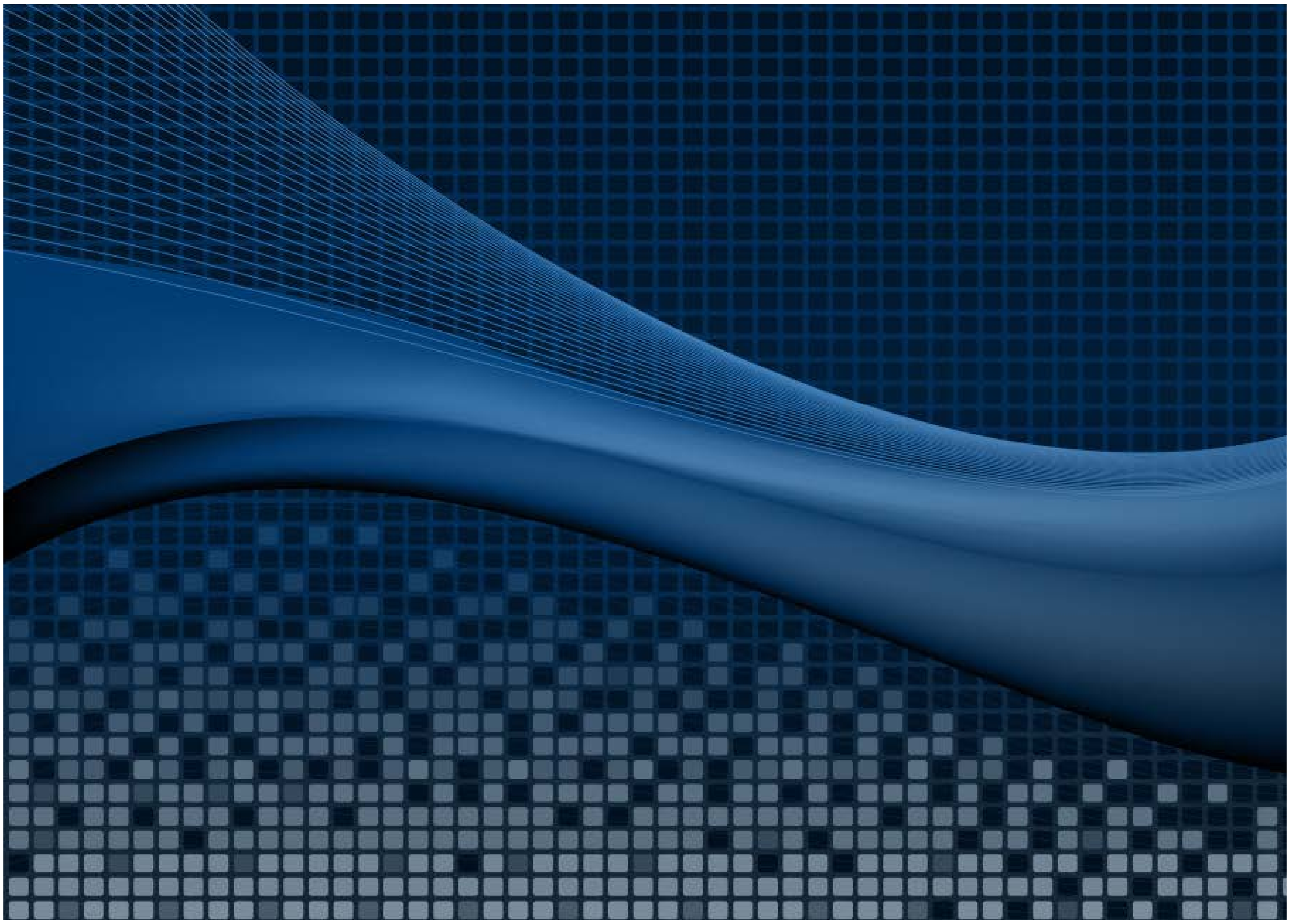
City of Pflugerville, Texas

America’s Water Infrastructure Act

Risk & Resilience Assessment



TETRA TECH

October 2020

Risk & Resilience Assessment

October 2020

Prepared for

City of Pflugerville

100 East Main Street
Suite 100
Pflugerville, Texas 78660

Prepared by

Tetra Tech

8911 North Capital of Texas Highway
Suite 2310
Austin, TX 78759

Phone: 512.338.1667
Fax: 512.338.1331
tetratech.com

Third-Party Disclaimer

The content of this document is not intended to be of use nor relied upon by any person, firm or corporation, other than the addressee. Tetra Tech denies any liability whatsoever to other parties for damages or injuries incurred by the use of this document without prior express written approval of Tetra Tech and the addressee. This document is subject to further restrictions imposed by the contract between the addressee and Tetra Tech.

Tetra Tech Project #200-302595-20001

\\tt.local\ier\Projects\San Antonio\302595\200-302595-20001\Deliverables\Pflugerville Final Report_dpedit.docx

CONTENTS

Tables

Figures

ACRONYMS/ABBREVIATIONS

Acronym or Abbreviation	Definition
2FA	two-factor authentication
ACL	access control list
AD	active directory
AMI	advanced metering infrastructure
AMP	Advanced Malware Protection (part of the brand name AMP for Endpoints)
ANSI	American National Standard Institute
APT	advanced persistent threat
ASCE	American Society of Civil Engineers
ASR	aquifer storage and recovery
AV	anti-virus
AWIA	America's Water Infrastructure Act
AWWA	American Water Works Association
BL	baseline (existing condition) value
CSF	Cybersecurity Framework
EMP	electromagnetic pulse
EPA	U.S. Environmental Protection Agency
ERP	emergency response plan
GIS	geographic information system
HVAC	heating ventilation and cooling
IPS	Intelligent Process Solutions (a brand name)
IT	information technology
LIMS	laboratory information management system
mgd	millions of gallons per day
Mi	mitigated condition values
NIST	National Institute of Standards and Technology
OSI PI	process information system (a data historian application) developed by OSIsoft
OT	operational technology
OTP	one-time PIN
PARRE	Program to Assist Risk and Resilience Examination
PCI	payment card industry
PIN	personal identification number
PIO	public information officer
PLC	programmable logic controller
RAMCAP	Risk Analysis and Management for Critical Asset Management Protection
RCP	reinforced concrete pipe
RRA	risk and resilience assessment
SCADA	supervisory control and data acquisition

Acronym or Abbreviation	Definition
SHA2	secure hash algorithm 2
SNP	brand name of a monitoring provider
VLAN	virtual local area network
WHEAT	Water Health and Economic Analysis Tool

1. INTRODUCTION

The City of Pflugerville has undertaken a water system risk and resilience assessment (RRA) addressing its physical operational assets and cyber networks, in compliance with the America's Water Infrastructure Act (AWIA). The RRA assesses mission-critical physical assets and cyber networks of the City's water systems, including both administrative and operations facilities. It identifies the water system's vulnerabilities to malevolent acts and natural hazards, as well as dependency risks (risks to resources that the systems depend on, such as suppliers or employees) and proximity risks (risks to nearby sites that could affect water system operation).

The RRA also provides documentation and discussions to inform an AWIA-required update of Pflugerville's water system emergency response plan, which is being completed under separate contract.

1.1 GENERAL APPROACH

The RRA evaluated risks to critical water system assets and the City's ability to quickly and effectively recover from disruptions of these assets. The City retained Tetra Tech to perform the RRA, which was completed in conformance with the following standards:

- The Risk Analysis and Management for Critical Asset Management Protection (RAMCAP) standard developed by the American Society of Mechanical Engineers. The American National Standard Institute and American Water Works Association's J100-10 standard adapts the RAMCAP method for use in the water and wastewater sector (ANSI/AWWA, 2010).
- For the evaluation of cyber assets, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) (NIST, 2020).

1.2 REGULATORY REQUIREMENT

The AWIA mandates the completion of an RRA (and subsequent update or creation of an emergency response plan) by community water systems serving a population greater than 3,300 people. The RRA must assess the risk to, and resilience of the community water system. This assessment requires an "all-hazards" approach, considering intentional malevolent acts, natural hazards, and dependency and proximity threats.

The RRA is to be conducted in accordance AWIA requirements, using the RAMCAP methodology for evaluation and the PARRE tool (Program to Assist Risk and Resilience Examination) for data analytics. RAMCAP and PARRE are both approved tools under the Department of Homeland Security SAFETY Act.

As an outcome of the RRA, a capital and operational needs plan is to be developed for assets determined to be the most critical during the initial assessment.

This RRA was completed by Tetra Tech with input from City of Pflugerville staff, and the tools and assessment data have been provided to the City to facilitate an update of the RRA on the required 5-year interval (by December 2025). The RRA considers:

- Risk from malevolent acts, natural hazards, and dependency and proximity threats
- The resilience of pipes, constructed conveyances and physical barriers; source water, water collection, intake, pretreatment, treatment, storage and distribution facilities; and electronic, computer, or other automated systems (including the security of such systems)
- Monitoring practices
- Financial infrastructure
- Use, storage, or handling of chemicals
- Operation and maintenance of the system

1.3 ASSESSMENT PARTICIPANTS

The following City and Tetra Tech staff participated in development of the RRA:

City of Pflugerville Staff:

- Matt Woodward, Project Manager
- Amy Giannini
- Patricia Davis
- Romulus Atanasiu
- Brandon Pritchett
- Brian Camp
- Cody Collina

Tetra Tech Staff:

- Brian Murphy, PE, Project Manager
- Ken Nichols
- Jeremy Kaufman
- Dan Franz
- Elston Johnson
- Mary Martin
- Robert George
- Corey Lamb
- Sara van der Capellen

1.4 THE UTILITY THREAT ENVIRONMENT

1.4.1 Physical Threats

In response to the September 11, 2001, attacks, the 2002 Bioterrorism Act required water system vulnerability assessments that focused on threats to physical assets from intentional malevolent acts. Since then, utilities have found that they more commonly experience losses of assets due to natural disasters, and emergency response planning has identified threats arising from proximity and dependency. As part of the evolving practice of asset protection, the AWIA calls for assessments that address threats from all hazards:

- Malevolent acts with the intention of doing damage to an asset or using an asset to cause harm
- Natural disasters that can occur without warning, cannot be prevented and vary regionally
- Dependency on other critical networks for operability, such as power, fuel, chemicals, and transportation
- Proximity to other potential targets that may result in damage to a water asset if attacked or damaged

For this assessment, the City's physical assets against which these threats were considered include all critical assets of the water system, including physical cyber assets. Malevolent threats against physical assets have not substantially evolved, and reducing risk from these threats still relies largely on maintaining a secure perimeter.

1.4.2 Cyber Threats

The Evolving Nature of Threats to Cyber Assets

Given the increasing occurrences of system intrusions, database hacks, and ransomware attacks, AWIA requirements emphasize cybersecurity threats. The mechanisms for launching attacks against cyber assets are constantly evolving. Traditionally, disaster recovery and contingency planning for cyber assets has focused on large-scale natural events such as flooding or fire impacting a limited number of facilities. Recovery typically consisted of moving data processing operations to another facility, restoring recent backups, and resuming operations until the primary facility could be restored. Individual system recovery plans could be invoked when an equipment failure or cyber-attack disabled a handful of systems. Malware cleanup activities involved isolating and cleaning or restoring individual systems.

The sophistication of modern cyber threats has rendered many of the old isolation and clean-up efforts ineffective. The availability of sophisticated cyber-warfare technologies on the open market has lowered the level of specialized knowledge required to mount a successful cyber-attack. A large-scale event affecting large portions of an organization's cyber systems might be triggered from across the globe and can be enabled through the careless actions of a single employee. Attacks can move rapidly within a networked system and impact multiple systems simultaneously. Unlike natural disasters that occur and then stop, these attacks can regenerate and repeat until they are eradicated, which can take weeks or months to accomplish.

Utilities must be prepared for sophisticated, rapidly spreading attacks throughout their networked computer infrastructure at any time. Information technology departments must be prepared to counter threats that can cause system-wide damage on a daily basis. Response to cyber-attacks increasingly requires disaster-level recovery efforts on a large scale.

Advanced Persistent Threats

Advanced persistent threat are cyber-attacks designed to burrow deep into systems and maintain an active presence on the victim network, potentially remaining undetected for long periods of time. Unlike earlier generations of malware and attacks that would quickly identify, compromise and corrupt or deface systems, advanced persistent threats are designed to quietly evade detection through a multi-step strategy.

The attackers attempt to remain hidden in the victim system and to plant back doors that will allow them to maintain a persistent presence on the network. Hidden, encrypted tunnels are created to one or more internet-based control centers, allowing the attacker ready access on demand. An advanced persistent threat attack may cycle repeatedly for weeks or months, remaining undetected until complete access is obtained. The final step after this prolonged preparation period can come in various forms:

- **Botnets**—Hundreds of thousands of compromised devices that can be directed to deluge target systems with traffic under the direction of a remote server operated by the attacker
- **Crypto-mining**—The use of computing resources—often on victims' little-used but continually powered systems—to "mine" crypto-currencies using CPU-intensive calculations
- **Data exfiltration**—Moving sensitive data, such as email server databases and sensitive financial and personnel information, to attackers' systems for future use and manipulation

- **Denial-of-Service**—Generating excessive network traffic to impede normal communications or to take target systems offline for political or extortion purposes
- **Ransomware**—Sophisticated encryption of any accessible data on compromised systems (e.g. images, databases or other files), rendering them inaccessible, followed by automated demands for payment to obtain the keys required to decrypt the locked data. Upon payment, the keys may or may not actually be delivered.

Advanced persistent threat attacks use a combination of techniques to maintain a presence on the victim network and know when their activities have been discovered:

- **Trojan horse** programs may be hidden with program executables to re-infect a cleaned system. When a user next launches the infected application, software is triggered that begins the attack cycle anew, re-establishing connection to the attacker's command and control center.
- **Software time bombs** may be set to "go off" at preset hours, days or months in the future to re-infect systems.
- **Dead-man's switch** mechanisms may perform checks on other infected systems, alerting the attacker or launching other attacks when one infected system is cleaned.

This combination of pervasive intrusion, complete and rapid encryption, and external access can overwhelm an unprepared utility's ability to respond and recover assets in a timely manner.

Data Breaches

In many systems, the value of personal data stored in enterprise applications exceeds the value of the computers and software. Customer information system and human resource databases are common examples. Most states have data breach laws that establish minimum responses to any breach of personally identifiable information that may be used for identity theft or criminal activity. Most such laws mandate at least written notification of individuals whose data may have been exposed during a breach. Industry estimates for generation of written notification is $15 per record. Should additional relief be required (e.g. providing credit monitoring services for affected individuals), costs can go well beyond these levels.

Providing Resilience

It is essential to be able to restore critical cyber functionality—at least to the point of restoring vital servers to a snapshot in time before the attack. This generally requires at least the following:

- Backups must be maintained for sufficient durations to allow restoration to a pre-attack point in time. Complete system snapshots in a pre-attack state must be available. Backups made after infection may contain infected software, encrypted or corrupted data and any number of other hazards.
- Plans must include procedures for invoking disaster recovery measures in response to loss of assets regardless of the underlying cause of that loss. A system rendered unusable due to a cyber-attack or storage loss is no more accessible than one destroyed in a fire.

2. APPROACH

The RRA was conducted in accordance with published and voluntary standards using a series of facilitated workshops to manage decision-making and prioritization by City staff. Following each workshop, desktop processing of data and quantitative analysis of workshop collected data were performed.

2.1 RAMCAP METHODOLOGY

The RRA was conducted using RAMCAP, which is a seven-step methodology created by the American Society of Mechanical Engineers after the September 11, 2001 attacks to enable asset owners to analyze risks and risk-reduction options relative to specific malevolent attacks. The ANSI/AWWA J100-10 standard adapts the RAMCAP method for application in the water sector (ANSI/AWWA, 2010). RAMCAP provides a statistical method for comparing threats to system assets. It provides minimum objectives for risk and resilience analysis and prescribes methods to achieve the objectives. Figure 1 shows an overview of the process.

- Step 1, Asset Characterization is covered in Chapter 3 (Screening for High-Priority Assets). City of Pflugerville staff reviewed all major City assets and rated the consequences of each asset's failure for human, utility financial, and regional economic impact. Consequence scores on a scale of 1 to 5 were assigned for each asset and impact. Facilities that scored high enough were moved forward to Step 2.
- Step 2, Threat Characterization is covered in Chapter 4 (Threat-Asset Pair Development). City of Pflugerville staff rated possible consequences to the assets carried forward from Step 1 for 27 threats (25 RAMCAP reference threats and two additional threats added by City staff). The ratings used the same 1 to 5 consequence scale used in Step 1. Any combination of an asset and a threat that received a consequence score of 5 was carried forward. These threat-asset pairs were moved forward to Step 3.
- Step 3, Consequence Analysis is covered in Chapter 5 (Consequence Analysis). The team quantified the impact in dollars for each threat-asset pair. Costs were quantified by values assigned to estimated loss of life, estimated serious injuries, financial loss to the City, and estimated economic impact on the community. The total financial impact on each threat-asset pair was calculated.
- Step 4, Vulnerability Analysis and Step 5, Threat Analysis are both covered in Chapter 6 (Vulnerability and Threat Analysis). Vulnerability is the probability that an estimated consequence will result if an identified threat occurs. Threat likelihood is the probability of the threat occurring for a specific asset. The vulnerability probabilities and threat likelihood for each threat-asset pair were developed based on professional judgment, City staff institutional knowledge, City of Pflugerville reports, and literature with information on the threats.
- Step 6, Risk/Resilience Analysis is covered in Chapter 7 (Risk and Resilience Analysis). The risk and resilience values were calculated for each threat-asset pair. The risk calculation was based on the financial impacts developed in Step 3, and the vulnerability and threat likelihood developed in Step 4. The resilience calculation was based on the threat duration and severity developed in Step 3, the vulnerability developed in Step 4, and the threat likelihood developed in Step 5.

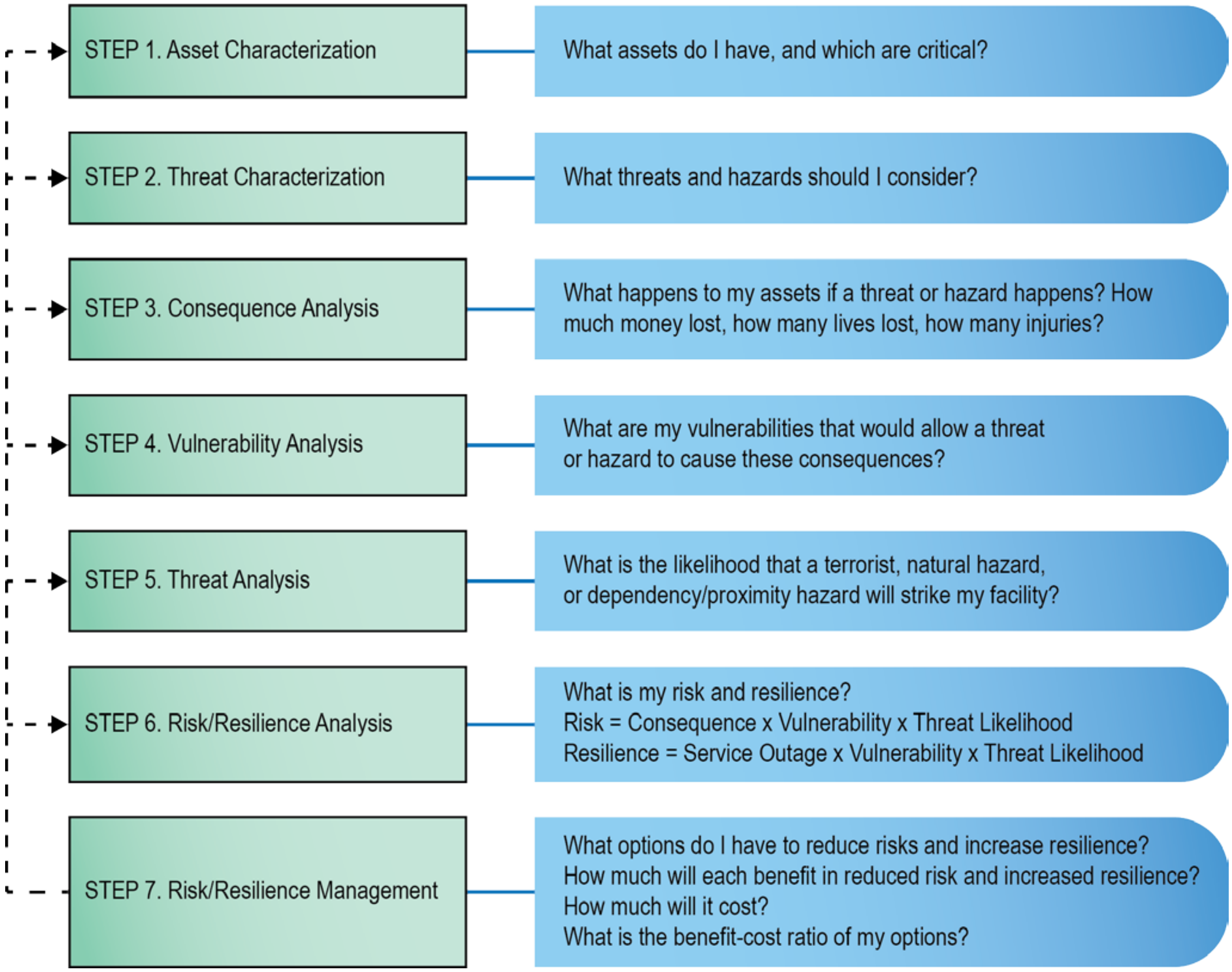

STEP 1. Asset Characterization
What assets do I have, and which are critical?
STEP 2. Threat Characterization
What threats and hazards should I consider?
STEP 3. Consequence Analysis
What happens to my assets if a threat or hazard happens? How much money lost, how many lives lost, how many injuries?
STEP 4. Vulnerability Analysis
What are my vulnerabilities that would allow a threat or hazard to cause these consequences?
STEP 5. Threat Analysis
What is the likelihood that a terrorist, natural hazard, or dependency/proximity hazard will strike my facility?
STEP 6. Risk/Resilience Analysis
What is my risk and resilience?
Risk = Consequence x Vulnerability x Threat Likelihood
Resilience = Service Outage x Vulnerability x Threat Likelihood
STEP 7. Risk/Resilience Management
What options do I have to reduce risks and increase resilience?
How much will each benefit in reduced risk and increased resilience?
How much will it cost?
What is the benefit-cost ratio of my options?

Figure 1. RAMCAP Process Overview

- Step 7, Risk/Resilience Management is covered in Chapter 8 (Assessment and Development of Mitigation) and Chapter 0 (Capital Improvement Plan). Chapter 8 describes site conditions for categories of assets and provides the proposed mitigation and cost for each asset. Chapter 0 calculates the benefit-cost ratio for each mitigation and prioritizes recommended actions.

2.2 NIST CYBERSECURITY FRAMEWORK

The RRA considered the water system cyber assets critical to the safe production of drinking water and business operations of the utility: computers, networks, data and communications systems, and billing systems. These consist of both information technology (IT) and operational technology (OT) systems:

- Plant industrial control systems
- Supervisory control and data acquisition (SCADA) systems
- Supporting network and computer infrastructure
- Business applications supporting utility operations

The cyber-asset assessment closely mirrored the physical RAMCAP assessment steps but involved different City staff with knowledge of computerized systems from both IT and SCADA perspectives. RAMCAP does not provide specific measures for evaluating the risk and resilience of cyber assets. Therefore, the NIST CSF was used as the basis for evaluating cyber assets.

The CSF is the leading guidance for planning, design and implementation of cybersecurity programs. It considers cybersecurity risks as part of an organization's risk management processes. The CSF was developed in response to Presidential Executive Order 13636 (Improving Critical Infrastructure; February 19, 2013), to address a lack of specific guidance for critical infrastructure sectors as identified in a report by the General Accounting Office. It provides a voluntary framework for organizations to manage cybersecurity risk.

The CSF has been widely adopted as a best practice in many sectors and incorporates links to several existing cybersecurity standards. It evaluates an organization's security readiness and resilience in the following categories of control:

- **Identify** critical assets—hardware, software, data and communications—necessary to conduct essential business functions
- **Protect** assets from natural and malicious disruptions
- **Detect** anomalies within the IT infrastructure that can potentially disrupt operations
- **Respond** to emergencies of varying magnitude
- **Recover** from emergencies of varying magnitude

For this RRA, cyber assets (hardware, software, policies and procedures) were evaluated in terms of the controls in place to protect them. The categories of control affect risk and resilience:

- Controls in the protect and detect categories provide direct protection and monitoring of assets. They correlate to risk.
- Controls in the identify, respond and recover categories are important to system identification and recovery. They correlate to resilience, but do not directly protect assets.

The Federal Information Processing Standard 199 (*Standards for Security Categorization of Federal Information and Information Systems*) classifies risks to cyber assets according to three criteria:

- **Confidentiality**—Disclosure of sensitive or protected information to unauthorized parties
- **Integrity**—Corruption or unauthorized manipulation of data
- **Availability**—Threats or denial of access to systems or data

Risks relating to OT systems such as SCADA were evaluated in terms of impacts caused by or contributed to by a loss of the ability to manage and control systems:

- **Compliance**—Risks to compliance with federal, state or local regulation
- **Liability**—Risk of consequences due to damage to property, wildlife or the environment
- **Safety**—Risks to human life and safety

A summary risk score based on this evaluation was used as a factor in the PARRE analysis to identify residual risk in terms of potential consequences, and to evaluate recommended mitigations.

2.3 PARRE TOOL

The RAMCAP process involves the collection of data and subsequent calculations. Tetra Tech used the PARRE tool to facilitate organization of the data in two separate models: one for water system physical assets; and one for cyber assets. PARRE is a commercially available tool developed by the AEM Corporation that guides users through the RAMCAP methodology and calculations. PARRE is granted the "Designated" status under the Department of Homeland Security SAFETY Act, which means that its use is recognized as a best practice, therefore providing liability protection.

2.4 FIELD ASSESSMENTS

Tetra Tech provided a third-party assessments as follows of water system assets ranked high priority for criticality, risk, and/or vulnerability:

- Field assessments to evaluate physical security were performed in-person, escorted by City personnel, for the accessible physical assets. Physical asset assessments followed COVID-19 safety protocols.
- Cyber asset assessments were conducted by videoconferencing. Hardware critical to function of the City's IT and OT systems was assessed for both physical security (accessibility and ability to do physical damage by unauthorized personnel), and cybersecurity (accessibility by persons releasing a cyber-attack on the cyber assets).

2.5 RRA WORKSHOPS

City of Pflugerville personnel hold institutional knowledge of the water system. To document this knowledge, prioritize the assets to be evaluated in this RRA, and discuss findings and recommended mitigation strategies from the assessment, the Tetra Tech team facilitated three workshops with City staff, including decision makers, subject matter experts, and other key support staff. Due to COVID-19 restrictions, all workshops were conducted using videoconferencing tools.

2.5.1 Workshop #1 June 15-19, 2020

The objectives of Workshop #1 were the following:

- Identify critical assets
- Define consequence criteria
- Rate and screen the critical assets to determine which to further assess
- Determine relevant threats
- Rate all assets for all identified threats, using established rating criteria
- Screen threat-asset pairs to determine which to further assess
- For each threat-asset pair, assess the potential consequence to the asset should the threat be realized
- Perform remote field assessments of the high-priority assets

2.5.2 Workshop #2A July 15, 2020

In Workshop #2A, City staff provided feedback on the ratings of vulnerability and likelihood determined by Tetra Tech. Cyber assets were further evaluated using the NIST cybersecurity framework.

2.5.3 Workshop #2B August 19, 2020

In Workshop #2B, cyber and physical security experts presented proposed mitigation methods and their effects on the vulnerability and consequences for each threat-asset pair. Additional information about existing and planned natural hazard mitigation methods was gathered from city officials.

3. Screening for High-Priority Assets

3.1 INITIAL IDENTIFICATION OF CRITICAL ASSETS

Using the City's previously submitted 2002 *Security Vulnerability Assessment* and additional documents provided by the City, a list of physical assets critical to the provision of drinking water was identified prior to the workshop. Nine physical assets were identified within the following asset system categories included in the PARRE software: external assets, facilities, pump stations, water storage, and wells. Tetra Tech separately developed a list of six critical cyber assets.

3.2 CONSEQUENCE CRITERIA DEVELOPMENT

To assist with the prioritization of assets, a matrix was created during Workshop #1 (Table 1) to define relative consequence on a scale of 1 through 5, with 1 representing the least consequence and 5 the greatest. The consequence criteria matrix was used as a discussion guide to assign priority levels and distinguish higher priority assets from lower ones on a relative basis. Consequences were identified in three categories:

- **Human**—Addressing human health and safety
- **Utility financial**—Addressing financial consequence to the City as a result of increased labor costs, additional material or service contract procurement, and loss of revenue
- **Regional economic**—Addressing regional/community financial consequence from loss of water service, including but not limited to inability for businesses and institutions to function

3.3 RATING AND SCREENING OF ASSETS

Workshop #1 participants rated each critical asset, using the consequence criteria matrix in Table 1, based on the worst reasonable case consequence expected in the event of its failure. They assigned ratings to each asset for each of three categories of consequences (human, utility financial, and regional economic). Each asset was given a total priority level score equal to the sum of the rating of its three individual consequence categories. For this exercise, complete failure of each asset was assumed, regardless of the nature of the threat.

Results are summarized in Table 2 for physical assets and Table 3 for cyber assets. Based on review of the total scores, workshop participants agreed that all assets would be carried forward as top-priority assets for further evaluation.

Table 1. Consequence Criteria Matrix for Asset Rating and Screening

Potential Consequence	Criteria for Assigning Priority Level[a]				
	5	4	3	2	1
Human Health and Safety Consequences					
Fatalities	Any	None	None	None	None
Serious Injuries	Any off site	Any on site	None	None	None
Environmental Impacts	Catastrophic	Very Severe	Severe	Moderate	Negligible
Utility Financial Consequences					
Utility Economic Loss	>$5 million	$5 million – $1 million	$1 million – $500,000	$500,000 – $50,000	<$50,000
Public Confidence	Found Negligent	Do Not Drink	Boil Water Order	>10 Complaints	<10 Complaints
Magnitude of Service Denial	System Wide	Multiple Pressure Zones	Single Pressure Zone	Subdivision	Few Services
Water Loss (Curtailment)	Severe	Mandatory	Voluntary	Alert	None
Regional Economic Consequences					
Regional Economic Loss	>$25 million	$25 million – $5 million	$5 million -– $2.5 million	$2.5 million – $250,000	$250,000

a. Criteria for each score are based on City of Pflugerville data, level-of-service objectives, emergency response levels, and team consensus. The criteria are City-specific and can be revisited and confirmed or revised during the required 2025 update.

Table 2. Physical Asset Prioritization

Asset System	Critical Asset	Human Priority Level	Utility Financial Priority Level	Regional Economic Priority Level	Total Priority Level
Facility	Lake Pflugerville Dam	5	5	5	15
External Asset	1.5-MG Elevated Tank	5	5	4	14
Water Storage	Lake Pflugerville	4	5	5	14
Water Storage	Surface Water Treatment Plant	4	5	5	14
Water Storage	Lake Pflugerville Pump Station	4	4	5	13
Pump Station	Pfenning Pump Station	4	4	4	12
External Asset	Colorado River Intake	3	4	4	11
Well/Water Storage	1-MG North Stand Pipe	2	4	4	10
Water Storage	Public Works Building	5	3	1	9

Table 3. Cyber Asset Prioritization

Critical Asset	Human Priority Level	Utility Financial Priority Level	Regional Economic Priority Level	Total Priority Level
SUEZ	1	5	5	11
InCode	1	5	2	8
File Server	1	4	1	6
Historian	1	2	2	5
Neptune	1	3	1	5
SCADA Network VPN	1	3	1	5

SCADA = supervisory control and data acquisition; SUEZ = brand name, no definition; VPN = virtual private network

4. THREAT-ASSET PAIR DEVELOPMENT

Each identified top-priority asset was rated based on the expected consequence of specific relevant threats, using a 5-point priority-level scale. This assessment differed from the initial asset screening in two ways:

- A single overall consequence priority rating was assigned, rather than separate ratings for human, utility and community consequences.
- Consequences were assessed based on expected impacts (and likelihood) of a specific threat on each asset, rather than assuming total asset failure or loss.

4.1 CONSEQUENCE AND THREAT CRITERIA DEVELOPMENT

To assist with the prioritization of threat-asset pairs, a matrix was created during Workshop #1 (Table 4) to define relative consequence on a scale of 1 through 5, with 1 representing the least consequence and 5 the greatest. A priority level scale also was developed based on the likelihood of a threat occurring that would lead to the identified consequences, with 1 representing the least likelihood and 5 the most. The consequence/threat criteria matrix was used as a discussion guide to assign priority levels and distinguish higher priority threat-asset pairs from lower ones on a relative basis. Discrete quantified consequences for high-priority threat-asset pairs were defined later in the process (see Chapter 5).

Table 4. Consequence and Threat Criteria Matrix for Threat-Asset Rating

	Criteria for Assigning Priority Level[a]				
	5	4	3	2	1
Consequence Severity	Catastrophic	High	Medium	Low	None
Threat	Evidence of threat occurring to Pflugerville or regional utility	Strong potential of threat occurring	Reasonable potential of threat occurring	Low potential of threat occurring	Theoretical potential of threat occurring

a. Criteria for each score are based on City of Pflugerville data, level-of-service objectives, emergency response levels, and team consensus. The criteria are City-specific and can be revisited and confirmed or revised during the required 2025 update.

4.2 IDENTIFICATION OF RELEVANT THREATS

Relevant threats were selected from reference threats defined in RAMCAP and additional threats specific to the City of Pflugerville's water system as identified by City staff. Table 5 lists the threats selected for the evaluation.

Table 5. Threat List and Abbreviations

Product Contamination—*The intent of product contamination is to cause harm by introducing an undesired contaminant to the system that would cause harm to customers or to the system.*

Abbreviation	Threat Source
C(B)	Bio-toxin
C(C)	Chemical
C(P)	Pathogen
C(R)	Radionuclide
C(W)	Weaponization

Attack: Automotive—*An automotive attack assumes that the vehicle would be used as a weapon and would strike your asset directly. These threat scenarios do not include assault teams, only single vehicle based improvised explosive devices*

Abbreviation	Threat Source
(V1)	Car
(V2)	Van
(V3)	Mid-size Truck

Attack: Assault Team—*The assault team attack is more complex. It involves a lone assailant team of assailants with specific types of weapons, and various options for an approach.*

Abbreviation	Threat Source
(AT1)	1 Assailant

Sabotage—*In all of these threats, the intent is to cause harm by damaging, disabling, or destroying process control systems. The four ways an attack of this type can be accomplished are:*

Abbreviation	Threat Source	Abbreviation	Threat Source
S(CI)	Cyber – Insider	S(PI)	Physical – Insider
S(CU)	Cyber – Outsider	S(PU)	Physical – Outsider

Theft or Diversion—*In all of these threats, the intent is to steal or divert information, dangerous substances, valuable resources, etc. The four ways an attack of this type can be accomplished are:*

Abbreviation	Threat Source
T(CI)	Cyber – Insider
T(CU)	Cyber – Outsider
T(PI)	Physical – Insider
T(PU)	Physical – Outsider

Natural—*Natural Hazards fall into four categories in RAMCAP: hurricanes, earthquakes, tornadoes, and floods. Additional hazards were added for this RRA.*

Abbreviation	Threat Source	Abbreviation	Threat Source
N(F)	Flood	N(EH)	Extreme Heat
N(I)	Ice Storms	N(WS)[a]	Windstorm
N(T)	Tornado	N(D)[a]	Drought

Attack: Aircraft—*An attack by an aircraft assumes that the aircraft would be used as the weapon and would strike your asset directly.*

Abbreviation	Threat Source
(A1)	Helicopter
(A2)	Small Plane

Dependency and Proximity—*Dependency and proximity hazards are threats that occur outside the facility that could affect the facility and its operation. They include attacks on supplies, employees, and customers that are important to keep the facility running, as well as attacks on a nearby facility that can damage the facility being analyzed. As defined in RAMCAP they are:*

Abbreviation	Threat Source	Abbreviation	Threat Source
D(C)	Key Customers	D(S)	Key Suppliers
D(E)	Key Employees	D(T)	Transportation
D(P)	Proximity	D(U)	Utilities

a. These items were added specifically for the City of Pflugerville at the workshop. All others are defined by the U.S. EPA

The following RAMCAP reference threats were not used because they are not reasonable or possible for the City, based on its location and regional significance.

- Attack/aircraft by regional jet
- Attack/assault team by more than one assailant
- Attack/marine (any size)
- Attack/vehicle by semi-trailer truck
- Natural hazard/earthquake
- Natural hazard/wildfire

4.3 THREAT ASSESSMENT FOR PHYSICAL ASSETS

Each critical physical asset was scored for its likely exposure to all threats listed in Table 5 except the cyber-specific sabotage and theft threats. Threats were scored for each asset using the criteria for threat potential and consequence potential listed in Table 4. Where the threat potential and consequence potential rankings disagreed, participants used discretion to choose a reasonable rank. Table 6 summarizes the results of the threat scoring for the physical assets. Threat-asset pairs with a score of 5 were selected for further analysis. These are highlighted in red in Table 6.

Workshop participants agreed that for most of the assets to be carried forward, there would be no difference in subsequent analysis results for the five contamination threats. Therefore, instead of five threat-asset pairs separating each contamination threat, a single threat-asset pair for “Contamination” was evaluated. The exception to this is for the Surface Water Treatment Plant, for which it was decided that radionuclide contamination should be considered separately, as it would result in more severe disposal, remediation, and regional economic impacts than the other types of contaminants. Based on this process, 23 threat-asset pairs were carried forward, associated with eight assets, as listed in Table 7.

4.4 THREAT ASSESSMENT FOR CYBER ASSETS

For this RRA, cyber assets were evaluated for the following threats, which are the most relevant of the threat categories identified in Table 5 to cyber assets:

- **Sabotage of Cyber Asset (by Insider or Outsider)**—Corruption or destruction (e.g. encryption) of data, or denial-of-service
- **Theft of Cyber Asset (by Insider or Outsider)**—Theft of sensitive data pertaining to customers and individuals, or critical device configurations. For enterprise systems, this includes personally identifiable information associated with customer or employee records. For SCADA systems, this includes device configurations and programs
- **Dependency/Key Employee**—Unavailability of a particular employee greatly impacts ability of the District to provide water service and/or operating and response procedures are not well documented
- **Dependency/Key Supplier**— Limited number of suppliers for replacement hardware and equipment

For the RRA, insiders and outsiders are defined as follows:

- **Insiders**—Employees or other trusted insiders with authorized access to some or all of the critical assets
- **Outsiders**—Non-employees or others with no authorized access to the critical asset

With the increased prevalence of advanced persistent threat attacks (see Section 1.4.2) using sophisticated social engineering methods, the line between insider and outsider has largely been blurred. While an outsider might have difficulty breaching network protections, it has become common for them to deceptively enlist insiders to bypass network protections.

Each critical cyber asset was scored for likely consequences from each of the above threats, using the scales presented in Table 4. Where the threat potential and consequence potential rankings disagreed, participants used discretion to choose a reasonable rank. Table 8 summarizes the results of the threat scoring for the cyber threat-asset pairs. threat-asset pairs with a score of 5 were selected for further analysis, highlighted in red in Table 8. This process identified 13 such threat-asset pairs, associated with four assets, as summarized in Table 9.

Table 6. Physical Asset Threat Characterization

	Lake Pflugerville Dam	1.5-MG Elevated Tank	Lake Pflugerville	Surface Water Treatment Plant	Lake Pflugerville Pump Station	Pfenning Pump Station/Storage	Colorado River Intake	1-MG North Stand Pipe	Public Works Building
Product Contamination									
C(C)	1	5	4	5	1	5	3	5	1
C(R)	1	5	4	5	1	5	3	5	1
C(B)	1	5	4	5	1	5	3	5	1
C(P)	1	5	4	5	1	5	3	5	1
C(W)	1	5	4	5	1	5	3	5	1
Sabotage									
S(PI)	1	3	1	5	5	3	3	3	1
S(PU)	1	2	1	3	3	2	2	2	1
Theft									
T(PI)	1	1	1	3	1	1	1	1	5
T(PU	1	1	1	2	1	1	1	1	5
Attack: Aircraft									
(A1)	5	3	4	4	4	3	1	3	5
(A2)	5	3	4	4	4	3	1	3	5
Attack: Automotive									
V(1)	2	1	1	1	3	1	1	1	5
V(2)	3	2	1	1	4	2	1	2	5
V(3)	4	3	1	2	5	3	1	3	5
Attack: Assault Team									
(AT1)	1	1	1	5	1	1	1	1	5
Natural									
N(EH)	1	1	1	3	3	3	3	1	1
N(F)	1	1	1	1	1	1	1	1	4
N(I)	1	1	1	1	1	1	1	1	1
N(T)	1	3	1	5	3	4	1	3	1
Dependency/Proximity									
D(U)	1	1	1	5	5	1	1	1	3
D(S)	1	1	1	4	1	1	1	1	1
D(E)	1	1	1	3	1	1	1	1	2
D(C)	1	1	1	3	1	1	1	1	1
D(T)	1	1	1	1	1	1	3	1	1
D(P)	1	1	4	1	3	1	1	3	3
Pflugerville-Specific									
N(WS)	1	2	1	1	1	2	1	2	1
N(D)	1	4	4	4	4	4	5	4	1

Table 7. Physical Threat-Asset Pairs for Further Analysis

Asset	Threat	Asset	Threat
Lake Pflugerville Dam	(A1) – Helicopter	Pfenning Pump Station/Storage	C – Contamination
	(A2) – Small Plane	Colorado River Intake	N(D) - Drought
1.5-MG Elevated Tank	C – Contamination	1-MG North Stand Pipe	C – Contamination
Surface Water Treatment Plant	C – Contamination[a]	Public Works Building	T(PI) – Theft – Inside
	C(R) – Radionuclide		T(PU) – Theft – Outsider
	(AT1) – Active Shooter		(A1) – Helicopter
	S(PI) – Sabotage - Insider		(A2) – Small Plane
	N(T) – Tornado		(V1) – Car
	D(U) – Dependency – Utility		(V2) – Van
Lake Pflugerville Pump Station	S(PI) – Sabotage - Insider		(V3) – Mid-Size Truck
	(V3) – Mid-Size Truck		(AT1) – Active Shooter
	D(U) – Dependency – Utility		

a. For the Surface Water Treatment Plant, the "Contamination" threat includes all contamination threats except radionuclide contamination, which is evaluated separately. The "Contamination" threat for other assets in this list includes the radionuclide threat along with the other contamination threats.

Table 8. Cyber Asset Threat Characterization

	Sabotage		Theft		Dependency	
Asset	S(CI)	S(CU)	T(CI)	T(CU)	D(E)	D(S)
SUEZ	5	5	1	1	3	5
InCode	5	5	5	5	1	1
File Server	5	5	5	5	1	1
Historian	3	3	1	1	1	1
Neptune	3	3	1	1	1	2
SCADA Network	5	5	1	1	1	3

Table 9. Cyber Threat-Asset Pairs for Further Analysis

Asset	Threat	Asset	Threat
SUEZ	S(CI) – Cyber – Insider	File Server	S(CI) – Cyber – Insider
	S(CU) – Cyber – Outsider		S(CU) – Cyber – Outsider
	D(S) – Key Suppliers		T(CI) – Cyber – Insider
InCode	S(CI) – Cyber – Insider		T(CU) – Cyber – Outsider
	S(CU) – Cyber – Outsider	SCADA Network	S(CI) – Cyber – Insider
	T(CI) – Cyber – Insider		S(CU) – Cyber – Outsider
	T(CU) – Cyber – Outsider		

5. Consequence Analysis

5.1 APPROACH

The “worst reasonable consequence” for each identified threat-asset pair was quantified as described below.

5.1.1 Consequences on the City

Consequences on the City are referred to as owner impacts. They consist of the following elements:

- **Estimated liability for fatalities**—Consequence calculated in the PARRE tool at $9,100,000 per fatality
- **Estimated liability for serious injuries**—Consequence calculated in the PARRE tool at $955,500 per serious injury
- **Owner financial impact**—Consequence calculated in terms of capital replacements, claims and labor resources used to recover an asset, and revenue loss from denial of service

The Owner Financial Total is the sum of these elements.

5.1.2 Consequences on the Community

Consequences on the community were evaluated as economic impacts. Tetra Tech used the EPA’s Water Health and Economic Analysis Tool (WHEAT) to determine a cost of $316,200 for a system outage that reduces water supply by 1 percent for one day. The WHEAT calculates this value based on the rates customers pay for water, the average daily water demand on the system, the population served, and the geographic area (based on ZIP code).

The community economic impact varies linearly with the outage duration in days and the outage severity in millions of gallons per day (mgd). The team employed the following equation for each threat-asset pair:

$$\text{Community Economic Impact} = \$316{,}200 \times \text{Outage Duration} \times \frac{\text{Water Supply Loss}}{\text{Total Demand}} \times 100$$

5.2 RESULTS

Table 10 and Table 11 summarize the results for the physical assets and cyber assets, respectively.

Table 10. Physical Threat-Asset Pair Consequences

Threat-Asset Pair		Owner Financial				Community Economic Impact		
Asset	Threat	Fatalities	Serious Injuries	Owner Financial Impact	Owner Financial Total	Outage Duration (days)	Severity (mgd)	Impact
Lake Pflugerville Dam	(A1) – Helicopter	0	0	$16 million	$16 million	60	8	$337 million
	(A2) – Small Plane	0	0	$16 million	$16 million	60	8	$337 million
1.5-MG Elevated Tank	Contamination	1	5	$1 million	$14.9 million	30	30	$632 million
Surface Water Treatment Plant	Contamination	0	0	$18 million	$18 million	180	4	$506 million
	Contamination (R)	0	0	$20 million	$20 million	180	4	$506 million
	(AT1) – Active Shooter	1	3	$70 million	$82 million	365	4	$1.026 billion
	S(PI) – Sabotage – Insider	0	0	$250,000	$250,000	1	8	$6 million
	N(T) – Tornado	1	3	$70 million	$82 million	365	4	$1.026 billion
	D(U) – Dependency – Utility	0	0	$250,000	$250,000	5	8	$28 million
Lake Pflugerville Pump Station	S(PI) – Sabotage – Insider	0	0	$3.8 million	$3.8 million	14	8	$79 million
	(V3) – Mid-Size Truck	0	0	$4 million	$4 million	2	16	$22 million
	D(U) – Dependency – Utility	0	0	$1.2 million	$1.2 million	5	40	$141 million
Pfenning Pump Station/Storage	Contamination	1	5	$1 million	$14.9 million	30	30	$632 million
Colorado River Intake	N(D) - Drought	0	0	0	0	0	0	0
1-MG North Stand Pipe	Contamination	3	10	0	$36.9 million	30	40	$843 million
Public Works Building	T(PI) – Theft – Inside	0	0	0	0	0	0	0
	T(PU) – Theft – Outsider	0	0	0	0	0	0	0
	(A1) – Helicopter	8	8	$3.5 million	$83.9 million	0	0	0
	(A2) – Small Plane	8	8	$3.5 million	$83.9 million	0	0	0
	(V1) – Car	8	8	$3.5 million	$83.9 million	0	0	0
	(V2) – Van	8	8	$3.5 million	$83.9 million	0	0	0
	(V3) – Mid-Size Truck	8	8	$3.5 million	$83.9 million	0	0	0
	(AT1) – Active Shooter	8	8	$300,000	$80.7 million	0	0	0

Table 11. Cyber Threat-Asset Pair Consequence

Threat-Asset Pair		Owner Financial				Community Economic Impact		
Asset	Threat	Fatalities	Serious Injuries	Owner Financial Impact	Owner Financial Total	Outage Duration (days)	Severity (mgd)	Impact
SUEZ	S(CI) – Cyber – Insider	0	0	$1.14 million	$1.14 million	30	225	$8.955 billion
	S(CU) – Cyber – Outsider	0	0	$1.14 million	$1.14 million	30	225	$8.955 billion
	D(S) – Key Suppliers	0	0	$1.14 million	$1.14 million	30	225	$8.955 billion
InCode	S(CI) – Cyber – Insider	0	0	$2.85 million	$2.85 million	30	0	0
	S(CU) – Cyber – Outsider	0	0	$2.85 million	$2.85 million	30	0	0
	T(CI) – Cyber – Insider	0	0	$2.85 million	$2.85 million	30	0	0
	T(CU) – Cyber – Outsider	0	0	$2.85 million	$2.85 million	30	0	0
File Server	S(CI) – Cyber – Insider	0	0	$180,000	$180,000	0	0	0
	S(CU) – Cyber – Outsider	0	0	$180,000	$180,000	0	0	0
	T(CI) – Cyber – Insider	0	0	$180,000	$180,000	0	0	0
	T(CU) – Cyber – Outsider	0	0	$180,000	$180,000	0	0	0
SCADA Network	S(CI) – Cyber – Insider	0	0	$750,000	$750,000	0	0	0
	S(CU) – Cyber – Outsider	0	0	$750,000	$750,000	0	0	0

6. Vulnerability and Threat Analysis

The comparison of threat-asset pairs considers threat likelihood and vulnerability, defined as follows in the ANSI/AWWA J100-10 standard:

- **Threat Likelihood**—probability that an undesirable event will occur
- **Vulnerability—**probability, given that the attack or natural event occurs, that it will cause specifically estimated consequences

Tetra Tech assigned vulnerability and threat likelihood values for each threat-asset pair using professional judgement based on the site visits, information gathered during Workshop #1, and national data (EPA, 2019). Specific information used about natural hazards included the following:

- The threat likelihood for tornado was based on a recurrence of 1.1 tornadoes per 10,000 square miles per year, according to National Oceanic and Atmospheric Administration data.
- The threat likelihood for drought was assumed to be 1 percent, based on historical water level data and past curtailment.

The physical and cyber vulnerability and threat likelihood are summarized in Table 12 and Table 13, respectively.

Table 12. Physical Threat-Asset Pair Vulnerability and Likelihood

Threat-Asset Pair			
Asset	Threat	Vulnerability	Likelihood
Lake Pflugerville Dam	(A1) – Helicopter	0.1	0.000001
	(A2) – Small Plane	0.2	0.000001
1.5-MG Elevated Tank	Contamination	0.6	0.000001
Surface Water Treatment Plant	Contamination	0.3	0.000001
	Contamination (R)	0.3	0.000001
	(AT1) – Active Shooter	0.6	0.000001
	S(PI) – Sabotage - Insider	0.6	0.050000
	N(T) – Tornado	0.8	0.010000
	D(U) – Dependency – Utility	1.0	0.000001
Lake Pflugerville Pump Station	S(PI) – Sabotage – Insider	0.6	0.050000
	(V3) – Mid-Size Truck	1.0	0.000001
	D(U) – Dependency – Utility	1.0	0.000001
Pfenning Pump Station/Storage	Contamination	0.6	0.000001
Colorado River Intake	N(D) - Drought	0.1	0.010000
1-MG North Stand Pipe	Contamination	0.6	0.000001
Public Works Building	T(PI) – Theft – Inside	0.2	0.200000
	T(PU) – Theft – Outsider	0.2	0.200000
	(A1) – Helicopter	0.1	0.000001
	(A2) – Small Plane	0.1	0.000001
	(V1) – Car	0.1	0.000001
	(V2) – Van	0.1	0.000001
	(V3) – Mid-Size Truck	0.1	0.000001
	(AT1) – Active Shooter	1.0	0.000001

Table 13. Cyber Threat-Asset Pair Vulnerability and Likelihood

Threat-Asset Pair			
Asset	Threat	Vulnerability	Threat Likelihood
SUEZ	S(CI) – Cyber – Insider	0.5	0.3
	S(CU) – Cyber – Outsider	0.5	0.3
	D(S) – Key Suppliers	0.5	0.3
InCode	S(CI) – Cyber – Insider	0.1	0.3
	S(CU) – Cyber – Outsider	0.1	0.3
	T(CI) – Cyber – Insider	0.1	0.3
	T(CU) – Cyber – Outsider	0.1	0.3
File Server	S(CI) – Cyber – Insider	0.1	0.3
	S(CU) – Cyber – Outsider	0.1	0.3
	T(CI) – Cyber – Insider	0.1	0.3
	T(CU) – Cyber – Outsider	0.1	0.3
SCADA Network	S(CI) – Cyber – Insider	0.5	0.3
	S(CU) – Cyber – Outsider	0.5	0.3

7. RISK AND RESILIENCE ANALYSIS

7.1 RISK

The ANSI/AWWA J100-10 standard defines risk as the expected value of the consequences of an event, weighted by the likelihood of the event's occurrence and the likelihood that the event will result in the consequences if it occurs. It is calculated as follows:

RISK = Consequence x Vulnerability x Threat Likelihood

When calculating risk using owner financial total as the consequence, the risk value is in units of dollars per year. This estimate of risk can be interpreted as the annual amount that a utility would have to put into savings at zero interest to reconstruct the asset or recover from the financial impact after it has been impacted by the threat. The physical meaning of these risk values is less significant than their ability to be compared among threat-asset pairs for purposes of prioritization.

7.2 RESILIENCE

The ANSI/AWWA J100-10 standard defines resilience as the ability of an asset or system to withstand an attack or natural hazard without interruption of performing the asset's or system's function or, if the function is interrupted, to restore the function rapidly. It is calculated for physical assets as follows:

RESILIENCE = Duration x Severity x Vulnerability x Threat Likelihood

The resilience metric is an indicator of the level of water service denial due to a threat-asset pair, weighted by vulnerability and threat likelihood. Lower values indicate greater resilience—an asset that is completely resilient to a threat has a resilience metric value of zero, indicating no loss of service.

7.3 RESULTS

Following the determination of consequences, vulnerability, and threat likelihood for the threat-asset pairs, the baseline (i.e., existing) risk of the threat and the resilience of the asset were calculated, as shown in Table 14 for the physical assets, and Table 15 for the cyber assets.

Table 14. Physical Threat-Asset Pair Risk and Resilience

Threat-Asset Pair		Outage						
Asset	Threat	Duration (days)	Severity (mgd)	Consequence[a]	Vulnerability	Threat Likelihood	Risk ($/year)	Resilience
Lake Pflugerville Dam	(A1) – Helicopter	60	8	$16,000,000	0.1	0.000001	$2	0.00
	(A2) – Small Plane	60	8	$16,000,000	0.2	0.000001	$3	0.00
1.5-MG Elevated Tank	Contamination	30	30	$14,907,500	0.6	0.000001	$9	0.00
Surface Water Treatment Plant	Contamination	180	4	$18,000,000	0.3	0.000001	$5	0.00
	Contamination (R)	180	4	$20,000,000	0.3	0.000001	$6	0.00
	(AT1) – Active Shooter	365	4	$81,966,500	0.6	0.000001	$49	0.00
	S(PI) – Sabotage - Insider	1	8	$250,000	0.6	0.050000	$7,500	0.24
	N(T) – Tornado	365	4	$81,966,500	0.8	0.010000	$655,732	11.68
	D(U) – Dependency – Utility	5	8	$250,000	1.0	0.000001	$0	0.00
Lake Pflugerville Pump Station	S(PI) – Sabotage – Insider	14	8	$3,800,000	0.6	0.050000	$114,000	3.36
	(V3) – Mid-Size Truck	2	16	$4,000,000	1.0	0.000001	$4	0.00
	D(U) – Dependency – Utility	5	40	$1,200,000	1.0	0.000001	$1	0.00
Pfenning Pump Station/Storage	Contamination	30	30	$14,907,500	0.6	0.000001	$9	0.00
Colorado River Intake	N(D) - Drought	0	0	0	0.1	0.010000	$-	0.00
1-MG North Stand Pipe	Contamination	30	40	$36,855,000	0.6	0.000001	$22	0.00
Public Works Building	T(PI) – Theft – Inside	0	0	$0	0.2	0.200000	$-	0.00
	T(PU) – Theft – Outsider	0	0	$0	0.2	0.200000	$-	0.00
	(A1) – Helicopter	0	0	$83,944,000	0.1	0.000001	$8	0.00
	(A2) – Small Plane	0	0	$83,944,000	0.1	0.000001	$8	0.00
	(V1) – Car	0	0	$83,944,000	0.1	0.000001	$8	0.00
	(V2) – Van	0	0	$83,944,000	0.1	0.000001	$8	0.00
	(V3) – Mid-Size Truck	0	0	$83,944,000	0.1	0.000001	$8	0.00
	(AT1) – Active Shooter	0	0	$80,744,000	1.0	0.000001	$81	0.00

a. Consequence is equal to the owner financial total shown in Table 10

Table 15. Cyber Threat-Asset Pair Risk and Resilience

Threat-Asset Pair		Outage Duration	Severity			Threat	Risk	
Asset	Threat	(days)	(mgd)	Consequence[a]	Vulnerability	Likelihood	($/year)	Resilience
SUEZ	S(CI) – Cyber – Insider	30	225	$1.14 million	0.5	0.3	$171,000	1,012
	S(CU) – Cyber – Outsider	30	225	$1.14 million	0.5	0.3	$171,000	1,012
	D(S) – Key Suppliers	30	225	$1.14 million	0.5	0.3	$171,000	1,012
InCode	S(CI) – Cyber – Insider	30	0	$2.85 million	0.1	0.3	$85,500	0
	S(CU) – Cyber – Outsider	30	0	$2.85 million	0.1	0.3	$85,500	0
	T(CI) – Cyber – Insider	30	0	$2.85 million	0.1	0.3	$85,500	0
	T(CU) – Cyber – Outsider	30	0	$2.85 million	0.1	0.3	$85,500	0
File Server	S(CI) – Cyber – Insider	0	0	$180,000	0.1	0.3	$5,400	0
	S(CU) – Cyber – Outsider	0	0	$180,000	0.1	0.3	$5,400	0
	T(CI) – Cyber – Insider	0	0	$180,000	0.1	0.3	$5,400	0
	T(CU) – Cyber – Outsider	0	0	$180,000	0.1	0.3	$5,400	0
SCADA Network	S(CI) – Cyber – Insider	0	0	$750,000	0.5	0.3	$112,500	0
	S(CU) – Cyber – Outsider	0	0	$750,000	0.5	0.3	$112,500	0

a. Consequence is equal to the owner financial total shown in Table 11

8. Assessment and Development of Mitigation

8.1 PHYSICAL ASSETS

The following sections provide a detailed assessment of the vulnerability of the City's critical assets to the threats identified through the threat-asset pair development process. Mitigation measures are presented to address identified vulnerabilities.

8.1.1 Public Works Building

Assessment

Active Shooter Threat

The lobby entrance to this facility is a vulnerable location in the event of an active shooter. A valid access badge is required to gain entrance into the building, but inside the building there is open access from the public area to the semi-public area. Under current practice, one must wait for an escort into the semi-public area using a valid access badge. The lack of physical access restriction is not adequate to control assailant access.

The public access point at the Public Works Building is the only entry to the building that is glass-enclosed. It is the logical place for an assailant to enter. A center punch, hammer, rock, or bullet would crumble the tempered glass doors, giving the assailant unimpeded access into the building.

Aircraft Attack Threat

The building's proximity to the Austin Executive Airport presents the possibility of an aircraft attack. The ability of the structure to withstand an impact from a small aircraft is not known.

Vehicle Attack Threat

The facility lacks physical deterrents to a vehicle breach of the facility gate.

Theft or Diversion Threat

There has been a reported history of insider theft at the facility.

Mitigation Measures

Based on the assessment of Public Works Building vulnerabilities, the following mitigation measures are recommended for the active shooter threat:

- **Lobby Reconfiguration**—Consider a secure vestibule arrangement with lockout feature for each entrance. Evaluate the possibility of permanently sealing some of the superfluous doors (back doors), and conduct a National Fire Protection Association evaluation. It would be best to have a small lobby with bullet-resistant panels and glass, with intercom and pass-through if required. For ballistic protection, use a minimum UL 752, Level 2 with shotgun protection. Another option would be a security film and a protective attachment system. Security film prevents the tempered glass from crumbling to the floor and significantly increases the delay time of the assailant.
- **Active Shooter Training**—Conduct annual active shooter drills or table-top training exercises. Purchase trauma kits and provide staff training.
- **Visitor Management**—Institute a visitor management system. This can be as basic as a logbook with self-adhesive, self-expiring badges (Figure 2) or could be expanded to include pre-enrollment, notification of arrival, driver's license scanners, local printer, and issuing of a valid access badge through integration with the existing access control system, up to and including a self-service kiosk, as shown in Figure 3.

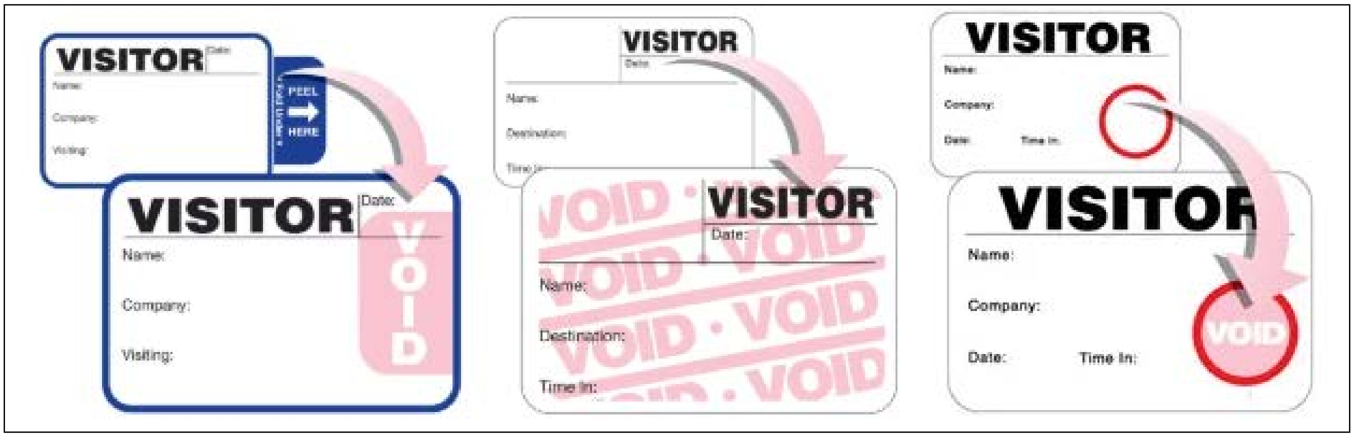


Figure 2. Self-Expiring Badges

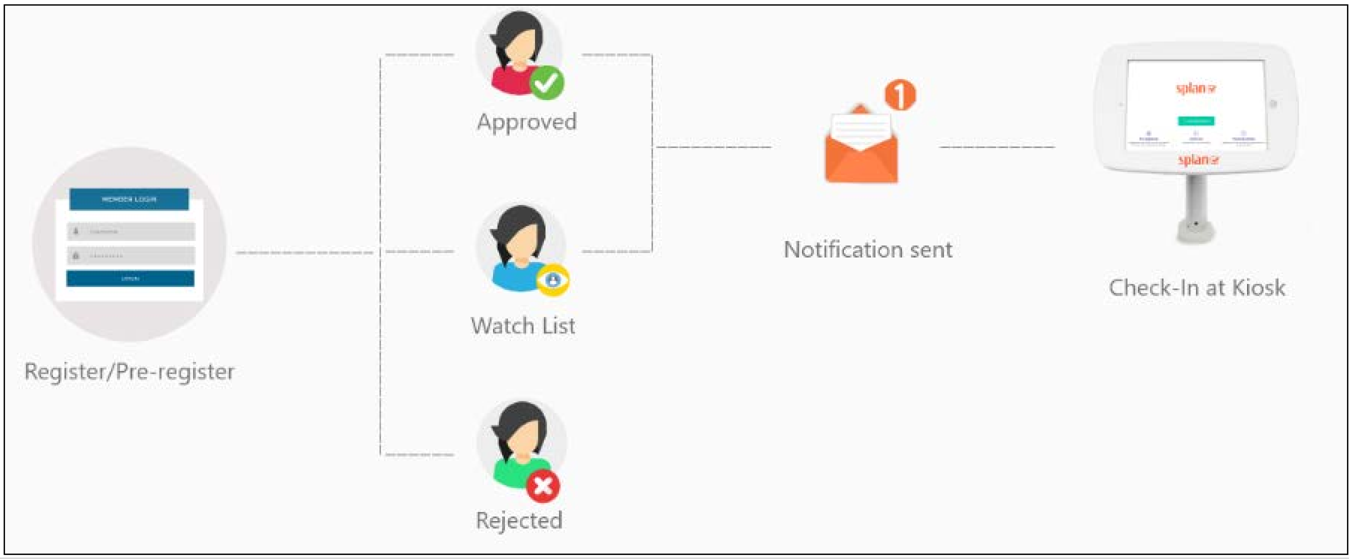


Figure 3. Visitor Registration Process

The following mitigation measures are recommended for other threats to the Public Works Building:

- Install a video monitoring system using smart cameras with facial recognition software.
- Create a centralized operations center for monitoring.
- Install a vehicle barrier system along the site perimeter, around specific assets (e.g. public works building), or, ideally, both. On improved surfaces, this may include cabling, bollards, anchored planters, benches or fountains, or other architectural features. On unimproved surfaces, it may include terrain adjustment (boulders, retaining walls, vertical grading, etc.) around frontages of specified assets. Structural hardening (e.g. blast mitigation coatings or fragmentation retention film) is a consideration where achieving standoff is not operationally feasible.
- Mitigate aircraft impact by requiring high performance concrete. If life safety is the objective rather than total structure resiliency, then blast mitigation coatings may suffice; these hold the structure together to permit evacuation, but the building may need to be rebuilt. An engineering evaluation is recommended.
- Include anti-cut/anti-climb fencing around the perimeter.
- Install security hinges on all exterior doors.

8.1.2 Surface Water Treatment Plant

Assessment

The Surface Water Treatment Plant is located on a high-traffic road but is partially protected with berms around most of the perimeter. The first security measure encountered at the facility is an automatic key card access-controlled gate. There is no interior fencing. Once inside the perimeter fencing, there is complete access to all of the facility, including clearwells and service pumps.

The treatment plant building has key-card access control. All employees have the same level of access to the facility. There is no video camera monitoring of the facility, but the plant is staffed at all hours. No access control is provided inside the building. Once inside, the entire building is accessible.

Chemical storage areas are covered by a roof and surrounded by three walls behind a chain link fence with barbed wire secured by a padlock. The facility does not have back-up power or additional protection for exterior electrical control boxes.

Mitigation Measures

Based on the assessment of Surface Water Treatment Plant vulnerabilities, the following mitigation measures are recommended:

- Install a video monitoring system using smart cameras with facial recognition software
- Provide a dual power feed to the plant
- Provide a secure vestibule arrangement with lockout feature for each entrance. Harden doors and windows, similar to the recommendation for the Public Works Building.
- Conduct annual active shooter drills or table-top training. Purchase trauma kits and provide staff training.
- Install vehicle barriers at the gate similar to the recommendation for the Public Works Building
- Conduct an evaluation to determine the feasibility of hardening the main building against tornadoes.
- Improve perimeter fencing similar to the recommendation for the Public Works Building.

8.1.3 Colorado River Intake and Lake Pflugerville Dam

Assessment

Lake Pflugerville Dam is part of a public park recreational area. The dam impounds the reservoir of water pumped from the Colorado River intake structure. The Lake Pflugerville impoundment provides approximately 30 days of water supply. The intake structure is remote and in a very low traffic area and uses submersible pumps; these conditions all help to minimize threats to the intake. Primary vulnerabilities are as follows:

- The primary threat to the dam is an attack by an aircraft on the spillway.
- The main threat to the intake is a lack of water supply due to drought. The City does not have an alternate supply readily available with sufficient capacity.

Mitigation Measures

The suggested mitigation measure for the dam is to conduct an engineering evaluation to determine the feasibility of reinforcing the dam's spillway to harden against a small aircraft attack.

The suggested mitigation measure for the intake is to obtain another readily available City water supply that could provide a sufficient supply of water during extended periods of drought.

8.1.4 Remote Storage and Pumping Facilities

Assessment

Contamination is the common threat for the City's remote pumping and storage facilities (the 1.5-MG Elevated Tank, 1-MG North Stand Pipe, Lake Pflugerville Pump Station, and Pfenning Pump Station and Storage). All four facilities are protected by some type of fencing and restricted access gate. None have video monitoring or intrusion alarms. Staff do conduct daily site visits. All sites are in high traffic areas.

Mitigation Measures

Based on the assessment of remote facility vulnerabilities, the following mitigation measures are recommended:

- Install perimeter intrusion detection systems comprising monitored video surveillance systems, with analytics for each site. The system would use fixed cameras along fences with pan-tilt-zoom capabilities to support active tracking within the fenced perimeter.
- Provide hardened fencing (anti-cut/anti-climb)
- Replace regular hinges with security hinges (see Figure 4) to keep the door in the frame even if the pin is removed. At a minimum, the top and bottom hinge on each door should be replaced; replacement of all hinges is recommended.
- Install full-height latch guards on all doors to prevent easy entry by slipping a lock.
- Install remote and on-site alarms on tank hatches and consider automated valving to remove the tank from service if the hatch is opened without authorization.
- Coordinate with the law enforcement agency of jurisdiction for directed patrols at all remote facilities. Identify environmentally controlled spaces on sites that may be used by law enforcement for report writing, etc. (i.e., to serve as mini-substations).

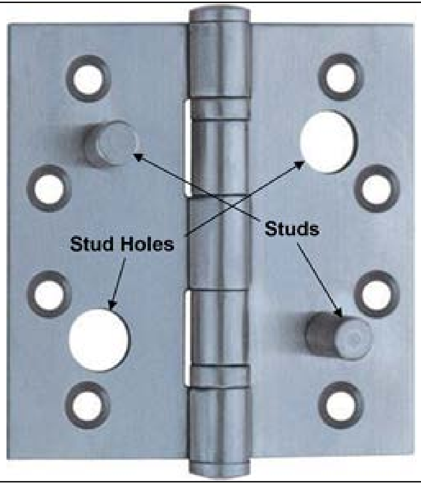


Figure 4. Security Hinge

8.2 CYBER ASSETS

This section summarizes assessment findings for cyber assets and presents mitigation measures to address threats. Table 15 summarizes the vulnerability, risk and resilience of critical water system cyber assets. Appendix A provides the notes taken at project workshops on the assessment of individual assets and their ability to achieve the control categories of identify, protect, detect, respond and recover.

Cyber assets are primarily protected by the network on which they are operated. Cyber asset mitigation measures were therefore developed for wo overall networks—enterprise and SCADA—with the understanding that the measures for each network would improve protections for all associated individual assets. The recommended mitigation measures identify improvements in the following areas:

- **Organization**—Staffing and personnel expertise
- **Methods**—Policies and practices used to operate City systems
- **Technology**—Hardware, software, communications and network infrastructure supporting the organization and methods
- **Security**—Physical and cybersecurity of IT systems and communications

Each mitigation measure is based on a core of security and reliability criteria to ensure that current and future City enterprise and SCADA systems can be operated, maintained and scaled as needs change without compromising security or capabilities. Recommendations in each category are designed to support and reinforce those in other categories.

8.2.1 Enterprise Network

Assessment

The City of Pflugerville's enterprise network infrastructure consists of current network equipment and is regularly evaluated for security vulnerabilities. A clear demarcation between the enterprise network and outside internet is actively maintained. Active monitoring is provided to detect anomalies within the network. The vulnerability of the network is relatively low. Recovery plans need to be created and tested. Backup and recovery procedures need to be formalized and tested.

The InCode and file server assets reside on the enterprise network and derive protection from controls applied to that network. Both systems have separate user credentials for system access and administration.

Mitigation Measures

Recommended mitigation for protection of assets on the enterprise network is as follows:

- **Develop formal cybersecurity policy**—Existing policies have not been fully formalized and codified as written documents. Formalizing policies provides clear direction for the management and operation of each system.
- **Update formal response plans and update to reflect current equipment**—Existing response plans have not been actively updated to reflect current equipment configurations. This may hinder recovery efforts in times of emergency.
- **Update recovery plans to reflect current equipment**—Existing system recovery plans have not been actively updated to reflect current equipment configurations. This may hinder recovery efforts in times of emergency.
- **Conduct third-party infrastructure disaster-readiness assessment**—This RRA evaluated the ability of the existing network and server infrastructure to support operation and recovery of systems during disaster conditions. An external evaluation is recommended to identify possible issues with physical facilities, HVAC, power, equipment and other essential infrastructure.

8.2.2 SCADA Network

Assessment

SCADA Network

The SCADA network is isolated from the enterprise network. City staff are not trained on the system and rely on vendors for system support and maintenance. SCADA equipment is not physically secure; it is vulnerable to unauthorized access. Lack of detection capabilities may slow response. Lack of formal response plans may hinder recovery efforts.

SUEZ SCADA

The SUEZ SCADA system is isolated from the enterprise network. City staff are trained on the system but rely on vendors for system support and maintenance. The equipment is not physically secure; it is vulnerable to unauthorized access. Lack of detection capabilities may slow response. Lack of formal response plans may hinder recovery efforts.

Mitigation Measures

The enterprise network has been updated and maintained throughout the years, adding layers of security, but the SCADA network has not kept pace. Equipment and devices are continually getting “smarter,” requiring a robust, secure network to support them. Utilities are increasingly becoming aware of the valuable data collected by SCADA systems, and this data is being shared with enterprise users. The advent of smarter devices and the sharing of data collected from these devices on a network that has not been updated has created a vulnerability in the City’s cyber presence. The SCADA network is exposed to significant physical threats as well. Exposed computers and network equipment can be easily compromised.

Recommendations for protection of assets residing on the SCADA network are as follows:

- **Develop formal cybersecurity policy**—Existing policies have not been fully formalized and codified as written documents. Formalizing of policies provides clear direction for the management and operation of each system.
- **Develop formal contingency, response and recovery plans**—Informal plans for the SCADA system are largely dependent on the availability of key personnel with deep system knowledge. Formalization of these plans in written form will aid rapid system recovery.
- **Develop and test backup and recovery features**—Backup and recovery procedures, including "bare metal" recovery of a completely disrupted system, have not been fully tested. Such procedures should be developed and tested on all components of the SCADA system.
- **Develop and implement formal change control process**—Formal change control procedures ensure that code and configuration changes are documented and centrally stored for ready access when needed to restore system components. Change control procedures and supporting tools should be provided to aid in the automated backup and rapid recovery of essential SCADA components.
- **Conduct third-party cybersecurity assessment**—This RRA evaluated the systems based on available information; a third-party assessment is recommended to identify other vulnerabilities and exposures within the SCADA system.
- **Conduct third-party infrastructure DR readiness assessment**—This RRA evaluated the ability of the existing network and server infrastructure to support operations and recovery of systems during disaster conditions; an external evaluation is recommended to identify possible issues with physical facilities, HVAC, power, equipment and other essential infrastructure.
- **Design and implement cybersecurity overlay on priority basis**—Expedited implementation of additional security controls to provide separation and segmentation within the existing SCADA system is recommended to provide additional short-term protection without significant changes to the logical network architecture.
- **Design and implement secure logical SCADA future network architecture**—As part of the next planned SCADA system upgrade, inclusion of a system-wide secure logical network architecture reflecting current cybersecurity best practices is recommended. Transition to such an architecture is likely to require logical network changes, device readdressing and migration, and other impactful changes that must be planned, staged and conducted in a coordinated manner.
- **Design and implement internal anomaly detection and logging systems**—Additional network and system monitoring and reporting capabilities are recommended for the SCADA system to allow proactive detection of anomalies and rapid response. Such improvements can be sed on the existing network and migrated to future network architectures.

9. CAPITAL IMPROVEMENT PLAN

9.1 BENEFIT-TO-COST RATIO

A process was developed to prioritize the mitigation measures identified in Chapter 8 based on their relative benefits and costs:

- Total benefit is estimated by calculating the reduction in risk brought about by implementing the measure (baseline risk minus mitigated risk):
  - ➢ Baseline risk is the risk shown in Table 14 and Table 15.
  - ➢ Mitigated risk was calculated for each threat-asset pair as shown in Table 16 and Table 17.
- Net benefit was calculated at the total benefit minus the mitigation cost.

Based on these estimates, the ratio of net benefit to cost was calculated as follows:

- Net Benefit/Cost Ratio = ((Baseline Risk – Mitigated Risk) – Mitigation Cost)/(Mitigation Cost)

Table 16 and Table 17 show the calculated net benefit/cost ratios sorted from greatest to least benefit-cost ratio.

9.2 CAPITAL IMPROVEMENT PLAN

The capital improvement plan (Table 18) summarizes the proposed mitigation methods and costs. The mitigation methods are prioritized by their net benefit/cost ratio; however, the reduction in risk to human life should also be considered. For cyber assets, the mitigation methods are applied to the networks rather than to individual assets.

Table 16. Physical Baseline vs. Mitigated Consequences

Asset-Threat Pair &	Fatalities		Serious Injuries		Owner Financial Total		Vulnerability		Likelihood		Risk		Net Benefit/
Proposed Mitigation	BL	Mi	BL	Mi	BL	Mi	BL	Mi	BL	Mi	BL	Mi	Cost Ratio
Surface Water Treatment Plant – N(T) **Mitigation Method:** Retrofit, Engineering Assessment **Mitigation Cost:** $250,000	1	0	3	0	81,966,500	0	0.8	0.2	0.010000	0.010000	$655,732	$0	1.62
Lake Pflugerville Pump Station – S(PI) **Mitigation Method:** Video Surveillance **Mitigation Cost:** $80,000	0	0	0	0	3,800,000	0	0.6	0.2	0.050000	0.050000	$114,000	$0	0.43
Surface Water Treatment Plant – S(PI) **Mitigation Method:** Video Surveillance, Access Control **Mitigation Cost:** $150,000	0	0	0	0	250,000	0	0.6	0.2	0.050000	0.050000	$7,500	$0	-0.50
Public Works Building – (AT1) **Mitigation Method:** Active Shooter Training, Ballistic Protection **Mitigation Cost:** $20,000	8	0	8	0	80,744,000	0	1.0	0.05	0.000001	0.000001	$81	$0	-0.99
Lake Pflugerville Dam – (A1) **Mitigation Method:** Monitored Video Surveillance System, Analytics, Dam Assessment, Structural Reinforcement **Mitigation Cost:** $500,000	0	0	0	0	16,000,000	0	0.1	0.05	0.000001	0.000001	$2	$0	-1.00
Lake Pflugerville Dam – (A2) **Mitigation Method:** Monitored Video Surveillance System, Analytics, Dam Assessment, Structural Reinforcement **Mitigation Cost:** $500,000	0	0	0	0	16,000,000	0	0.2	0.1	0.000001	0.000001	$3	$0	-1.00
1.5-MG Elevated Tank – Contamination **Mitigation Method:** Monitored Video Surveillance System, Analytics **Mitigation Cost:** $60,000	1	0	5	0	14,907,500	0	0.6	0.2	0.000001	0.000001	$9	$0	-1.00
Surface Water Treatment Plant – Contamination[a] **Mitigation Method:** Fencing, Vehicle Barrier **Mitigation Cost:** $2,000,000	0	0	0	0	20,000,000	0	0.3	0.2	0.000001	0.000001	$6	$0	-1.00
Surface Water Treatment Plant – (AT1) **Mitigation Method:** Reinforce Doors/Windows, Active Shooter Training **Mitigation Cost:** $50,000	1	0	3	0	81,966,500	0	0.6	0.2	0.000001	0.000001	$49	$0	-1.00

Asset-Threat Pair & Proposed Mitigation	Fatalities		Serious Injuries		Owner Financial Total		Vulnerability		Likelihood		Risk		Net Benefit/ Cost Ratio
	BL	Mi	BL	Mi	BL	Mi	BL	Mi	BL	Mi	BL	Mi	
Surface Water Treatment Plant – D(U) **Mitigation Method:** Generator, Dual Power Feed, Electrical Box Barriers **Mitigation Cost:** $100,000	0	0	0	0	250,000	0	1.0	0.2	0.000001	0.000001	$0	$0	-1.00
Lake Pflugerville Pump Station – D(U) **Mitigation Method:** Generator, Dual Power Feed **Mitigation Cost:** $100,000	0	0	0	0	1,200,000	0	1.0	0.2	0.000001	0.000001	$1	$0	-1.00
Pfenning Pump Station – Contamination **Mitigation Method:** Access Control, Monitored Video Surveillance System, Analytics, Vegetation Removal **Mitigation Cost:** $80,000	1	0	5	0	14,907,500	0	0.6	0.2	0.000001	0.000001	$9	$0	-1.00
Colorado River Intake – N(D) **Mitigation Method:** Alternate Water Source **Mitigation Cost:** $175,000	0	0	0	0	0	0	0.1	0.05	0.010000	0.010000	$-	$0	-1.00
1-MG North Stand Pipe - Contamination **Mitigation Method:** Access Control, Monitored Video Surveillance System, Analytics **Mitigation Cost:** $70,000	3	0	10	0	36,855,000	0	0.6	0.2	0.000001	0.000001	$22	$0	-1.00
Public Works Building – T(PI) **Mitigation Method:** Access Control, Interior Compartmentalization **Mitigation Cost:** $10,000	0	0	0	0	0	0	0.2	0.1	0.200000	0.200000	$-	$0	-1.00
Public Works Building – T(PU) **Mitigation Method:** Clearing, Smart Locks **Mitigation Cost:** $75,000	0	0	0	0	0	0	0.2	0.1	0.200000	0.200000	$-	$0	-1.00
Public Works Building – (A1) **Mitigation Method:** Engineering Study, Reinforcement, Blast Mitigation Coating **Mitigation Cost:** $150,000	8	0	8	0	83,944,000	0	0.1	0.08	0.000001	0.000001	$8	$0	-1.00
Public Works Building – (A2) **Mitigation Method:** Engineering Study, Reinforcement, Blast Mitigation Coating **Mitigation Cost:** $150,000	8	0	8	0	83,944,000	0	0.1	0.08	0.000001	0.000001	$8	$0	-1.00

Asset-Threat Pair &	Fatalities		Serious Injuries		Owner Financial Total		Vulnerability		Likelihood		Risk		Net Benefit/
Proposed Mitigation	BL	Mi	BL	Mi	BL	Mi	BL	Mi	BL	Mi	BL	Mi	Cost Ratio
Public Works Building – (V1) Mitigation Method: Reinforcement, Vehicle Barrier Mitigation Cost: $25,000	8	0	8	0	83,944,000	0	0.1	0.05	0.000001	0.000001	$8	$0	-1.00
Public Works Building – (V2) Mitigation Method: Reinforcement, Vehicle Barrier Mitigation Cost: $50,000	8	0	8	0	83,944,000	0	0.1	0.05	0.000001	0.000001	$8	$0	-1.00
Public Works Building – (V3) Mitigation Method: Reinforcement, Vehicle Barrier Mitigation Cost: $50,000	8	0	8	0	83,944,000	0	0.1	0.05	0.000001	0.000001	$8	$0	-1.00

a. The proposed mitigation methods address both the Contamination and Contamination (R) threats. These threats have been combined and the greater Owner Financial Total was used in calculations

Note: BL = baseline (existing); Mi = mitigated

Table 17. Cyber Baseline vs. Mitigated Consequences

Asset-Threat Pair &	Owner Financial Total		Vulnerability		Likelihood		Risk		Net Benefit/
Proposed Mitigation	BL	Mi	BL	Mi	BL	Mi	BL	Mi	Cost Ratio
SCADA Networked Assets—Various Threats Mitigation Method: See Table 18 Mitigation Cost: $584,600	$1,890,000	$1,890,000	0.5	0.3	0.3	0.3	$283,500	$170,100	-0.81
Enterprise Networked Assets—Various Threats Mitigation Method: See Table 18 Mitigation Cost: $136,000	$3,030,000	$3,030,000	0.1	0.1	0.3	0.3	$90,900	$90,900	-1.00

Note: BL = baseline (existing); Mi = mitigated

Table 18. Capital Improvement Plan

Asset[a]	Mitigation	Mitigation Cost
1. Surface Water Treatment Plant – N(T)[b]	Retrofit, Engineering Assessment	$250,000
2. Lake Pflugerville Pump Station – S(PI)	Video Surveillance	$80,000
3. Surface Water Treatment Plant – S(PI)	Video Surveillance, Access Control	$150,000
4. SCADA Networked Assets – Various Threats	Develop formal cybersecurity policy	$10,800
	Develop formal contingency, response and recovery plans	$18,000
	Develop & test backup and recovery features	$60,800
	Develop & implement formal change control process	$12,200
	Conduct third-party cybersecurity assessment	$63,600
	Conduct third-party infrastructure disaster recovery readiness assessment	$63,600
	Design & implement cybersecurity overlay on priority basis	$84,000
	Design & implement secure logical SCADA future network architecture	$164,400
	Design & implement internal anomaly detection and logging systems	$107,200
	Total	*$584,600*
5. Public Works Building – (AT1)[b]	Active Shooter Training, Ballistic Protection	$20,000
6. Surface Water Treatment Plant – (AT1)[b]	Reinforce Doors/Windows, Active Shooter Training	$50,000
7. 1-MG North Stand Pipe – Contamination[b]	Access Control, Monitored Video Surveillance System, Analytics	$70,000
8. 1.5-MG Elevated Tank – Contamination[b]	Monitored Video Surveillance System, Analytics	$60,000
9. Pfenning Pump Station – Contamination[b]	Access Control, Monitored Video Surveillance System, Analytics, Vegetation Removal	$80,000
10. Public Works Building – (A1)[b]	Engineering Study, Reinforcement, Blast Mitigation Coating	$150,000
11. Public Works Building – (A2)[b]	Engineering Study, Reinforcement, Blast Mitigation Coating	$150,000
12. Public Works Building – (V1)[b]	Reinforcement, Vehicle Barrier	$25,000
13. Public Works Building – (V2)[b]	Reinforcement, Vehicle Barrier	$50,000
14. Public Works Building – (V3)[b]	Reinforcement, Vehicle Barrier	$50,000
15. Surface Water Treatment Plant – Contamination	Fencing, Vehicle Barrier	$2,000,000
16. Lake Pflugerville Dam – (A2)	Monitored Video Surveillance System, Analytics, Dam Assessment, Structural Reinforcement	$500,000
17. Lake Pflugerville Dam – (A1)	Monitored Video Surveillance System, Analytics, Dam Assessment, Structural Reinforcement	$500,000
18. Lake Pflugerville Pump Station – D(U)	Generator, Dual Power Feed	$100,000
19. Surface Water Treatment Plant – D(U)	Generator, Dual Power Feed, Electrical Box Barriers	$100,000
20. Colorado River Intake – N(D)	Alternate Water Source	$175,000
21. Public Works Building – T(PI)	Access Control, Interior Compartmentalization	$10,000
22. Public Works Building – T(PU)	Clearing, Smart Locks	$75,000
23. Enterprise Network – Various Threats	Develop formal cybersecurity policy	$10,800
	Develop formal contingency, response, and recovery plans	$14,400
	Develop and test backup and recovery features	$57,200
	Conduct third-party infrastructure disaster recovery readiness assessment	$53,600
	Total	*$136,000*

a. Assets are numbered in order of benefit-to-cost ratio, highest to lowest.

b. These mitigation measures address potential loss of life associated with threats to physical assets.

REFERENCES

American National Standard Institute and American Water Works Association (ANSI/AWWA). 2010. Risk Analysis and Management for Critical Asset Protection (RAMCAP) Standard for Risk and Resilience Management of Water and Wastewater Systems Using the ASME-ITI RAMCAP Plus Methodology. ANSI/AWWA J100-10(R13). First Edition. July 1, 2010.

American Society of Civil Engineers (ASCE). 2011. Guidelines for the Physical Security of Water Utilities. p.7.

Environmental Protection Agency (EPA). 2019. Baseline Information on Malevolent Threats Acts for Community Water Systems. July 2019.

National Institute of Standards and Technology (NIST). 2020. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. April 2018. Accessed February 27, 2020.

Risk & Resilience Assessment

Appendix A. Workshop Notes on Cyber Asset Assessment

A. Workshop Notes on Cyber Asset Assessment

This appendix provides the raw notes taken at project workshops on the assessment of individual assets in the enterprise and SCADA networks and their ability to provide the following control categories:

- **Identify** critical assets—hardware, software, data and communications—necessary to conduct essential business functions
- **Protect** assets from natural and malicious disruptions
- **Detect** anomalies within the IT infrastructure that can potentially disrupt operations
- **Respond** to emergencies of varying magnitude
- **Recover** from emergencies of varying magnitude

ASSET 1: SCADA NETWORK

The SCADA Network is characterized as follows:

- Identify
    - Equipment primarily maintained by vendor – Alterman
    - No formal policies exist
    - No formal risk assessments or strategies outside of AWIA
- Protect
    - Individual user accounts. Certain address can be accessed from the Enterprise network for firmware upgrades
    - Annual training provided by KnowBe4
    - Radio and IP communication links are not encrypted
    - No formal policies exist
    - No logging, audits or other active protections
- Detect
    - No independent monitoring
    - No system monitoring / notifications
- Respond
    - No formal plan, call Alterman, they call IT

- Recover
    - No formal plan, contact communications team

ASSET 2: SUEZ SCADA

The SUEZ SCADA System is characterized as follows:

- Identify
    - Equipment primarily maintained by vendor – Alterman
    - No formal policies exist
    - No formal risk assessments or strategies outside of AWIA
- Protect
    - Individual user accounts. Certain address can be accessed from the Enterprise network for firmware upgrades
    - Annual training provided by KnowBe4
    - Radio and IP communication links are not encrypted
    - No formal policies exist
    - No logging, audits or other active protections
- Detect
    - No known independent monitoring
    - No known system monitoring / notifications
- Respond
    - No formal plan, call Alterman, they call IT
- Recover
    - No formal plan, contact communications team

ASSET 3: ENTERPRISE NETWORK

The Enterprise network is characterized as follows:

- Identify
    - Computer systems (PCs, network equipment, software, licensing, procurement) are identified and inventoried in Kace.
    - No formal cybersecurity policy has been developed
    - Periodic threat and vulnerability testing has been done / continues to be done
    - No formal Risk Management Strategy
- Protect
    - Users authenticate against Active Directory. Police Department has 2FA login
    - Access to server rooms is restricted by card access.
    - No network equipment is exposed to public access.

  - Annual training provided by KnowBe4.
  - Data is encrypted between sites. Disk data is not encrypted. Backup data is encrypted in transfer and at rest.
  - Switch Logs, informal plan and procedure. Police Department backs up to City Hall and back to PD, both backup to the cloud.
  - NAC on switches reading ports, in monitor mode now, force mode once defines. Don't currently block USB's. CrowdStrike monitors. Varonis flags suspicious data
- Detect
  - Varonis is used to collect log aggregation and analysis
  - PRTG is used for network performance monitoring.
  - Email notifications on health and performance
  - Varonis and CrowdStrike monitor and flag suspicious data
- Respond
  - No formal response plan
  - Communications team in place – rely on City's PIO. Staff is aware of procedures.
- Recover
  - No formal Disaster Recovery plans exist
  - City's PIO communicates with public.

ASSET 4: INCODE

InCode is characterized as follows:

- Identify
  - Computer systems (PCs, network equipment, software, licensing, procurement) are identified and inventoried in Kace.
  - No formal cybersecurity policy has been developed
  - Periodic threat and vulnerability testing has been done / continues to be done
  - No formal Risk Management Strategy
- Protect
  - Users authenticate against Active Directory. Police Department has 2FA login
  - Access to server rooms is restricted by card access.
  - No network equipment is exposed to public access.
  - Annual training provided by KnowBe4.
  - Data is encrypted between sites. Disk data is not encrypted
  - Switch Logs, informal plan and procedure. Police Department backs up to City Hall and back to PD, both backup to the cloud.
  - NAC on switches reading ports, in monitor mode now, force mode once defines. Don't currently block USB's. CrowdStrike monitors. Varonis flags suspicious data

- Detect
    - Varonis is used to collect log aggregation and analysis
    - PRTG is used for network performance monitoring.
    - Email notifications on health and performance
    - Varonis and CrowdStrike monitor and flag suspicious data
- Respond
    - No formal response plan
    - Communications team in place – rely on City's PIO. Staff is aware of procedures.
- Recover
    - No formal Disaster Recovery plans exist
    - City's PIO communicates with public.

ASSET 5: FILE SERVER

The Utility network is characterized as follows:

- Identify
    - Computer systems (PCs, network equipment, software, licensing, procurement) are identified and inventoried in Kace.
    - No formal cybersecurity policy has been developed
    - Periodic threat and vulnerability testing has been done / continues to be done
    - No formal Risk Management Strategy
- Protect
    - Users authenticate against Active Directory. Police Department has 2FA login
    - Access to server rooms is restricted by card access.
    - No network equipment is exposed to public access.
    - Annual training provided by KnowBe4.
    - Data is encrypted between sites. Disk data is not encrypted
    - Switch Logs, informal plan and procedure. Police Department backs up to City Hall and back to PD, both backup to the cloud.
    - NAC on switches reading ports, in monitor mode now, force mode once defines. Don't currently block USB's. CrowdStrike monitors. Varonis flags suspicious data
- Detect
    - Varonis is used to collect log aggregation and analysis
    - PRTG is used for network performance monitoring.
    - Email notifications on health and performance
    - Varonis and CrowdStrike monitor and flag suspicious data

- Respond
  - No formal response plan
  - Communications team in place – rely on City’s PIO. Staff is aware of procedures.
- Recover
  - No formal Disaster Recovery plans exist
  - City’s PIO communicates with public.