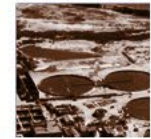
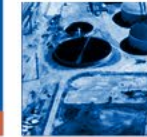


# Strategic Plan Development



## Tonight's Policy Discussions:

- Resilient Staffing
- Safety and Physical Security
- Cyber Security
- Property Management



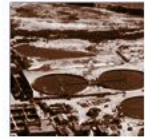
# Resilient Staffing

Book page: 261

Presented by Laura Maravilla  
*Human Resources & Risk Manager*

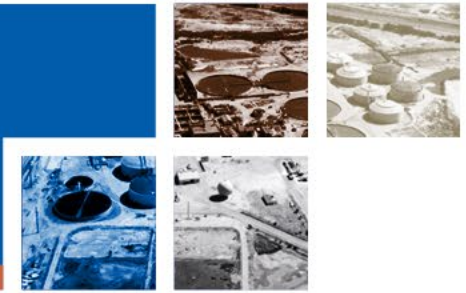


# Policy Question



***Is OCSD properly prepared for the future challenges of employee attrition and loss of institutional knowledge through employee development and leadership programs?***

# Background



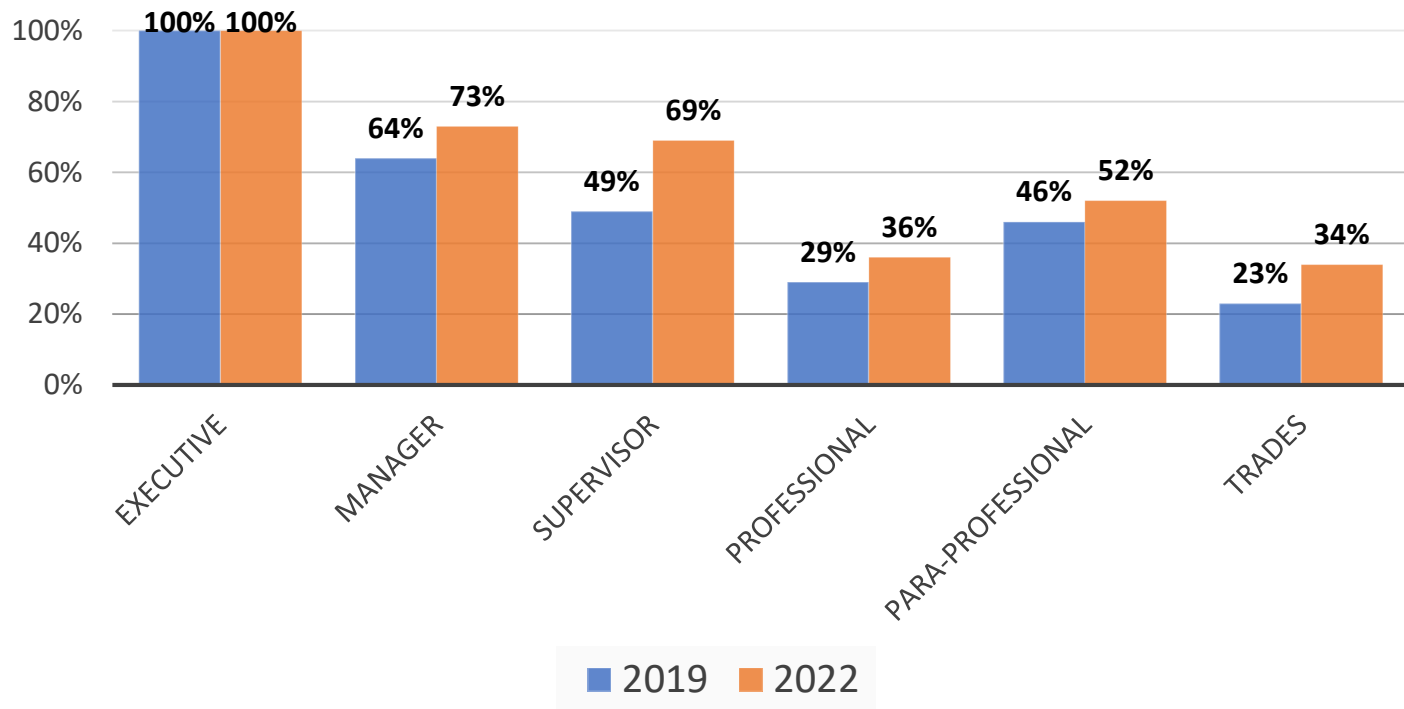
Diverse workforce of highly skilled and educated employees who carry out OCSD's mission and vision

- 640 budgeted full-time employees
- 70% of positions require a degree, certification, and/or license (scientists, engineers, environmental and regulatory specialists, operators, mechanics, construction inspectors, accountants, and specialized analysts)
- Since 2014, OCSD has lost 3,025 years of knowledge and experience primarily through retirement.

# Current Situation



45% of OCSD's employees are eligible for retirement which does not account for other forms of turnover



OCSD's current programs effectively develop and retain its current workforce, and attract highly technical and skilled talent

# Workforce Planning



## Workforce Vulnerability Assessments

Management evaluates key and vulnerable positions, based on:

- Criticality
- Retention
- Difficulty to Fill

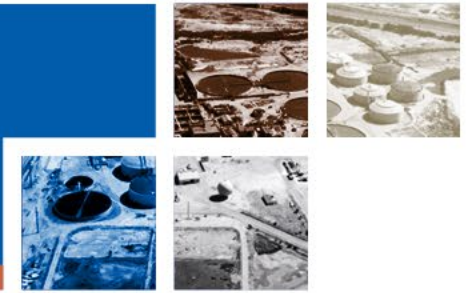
To develop current and future staffing plans.



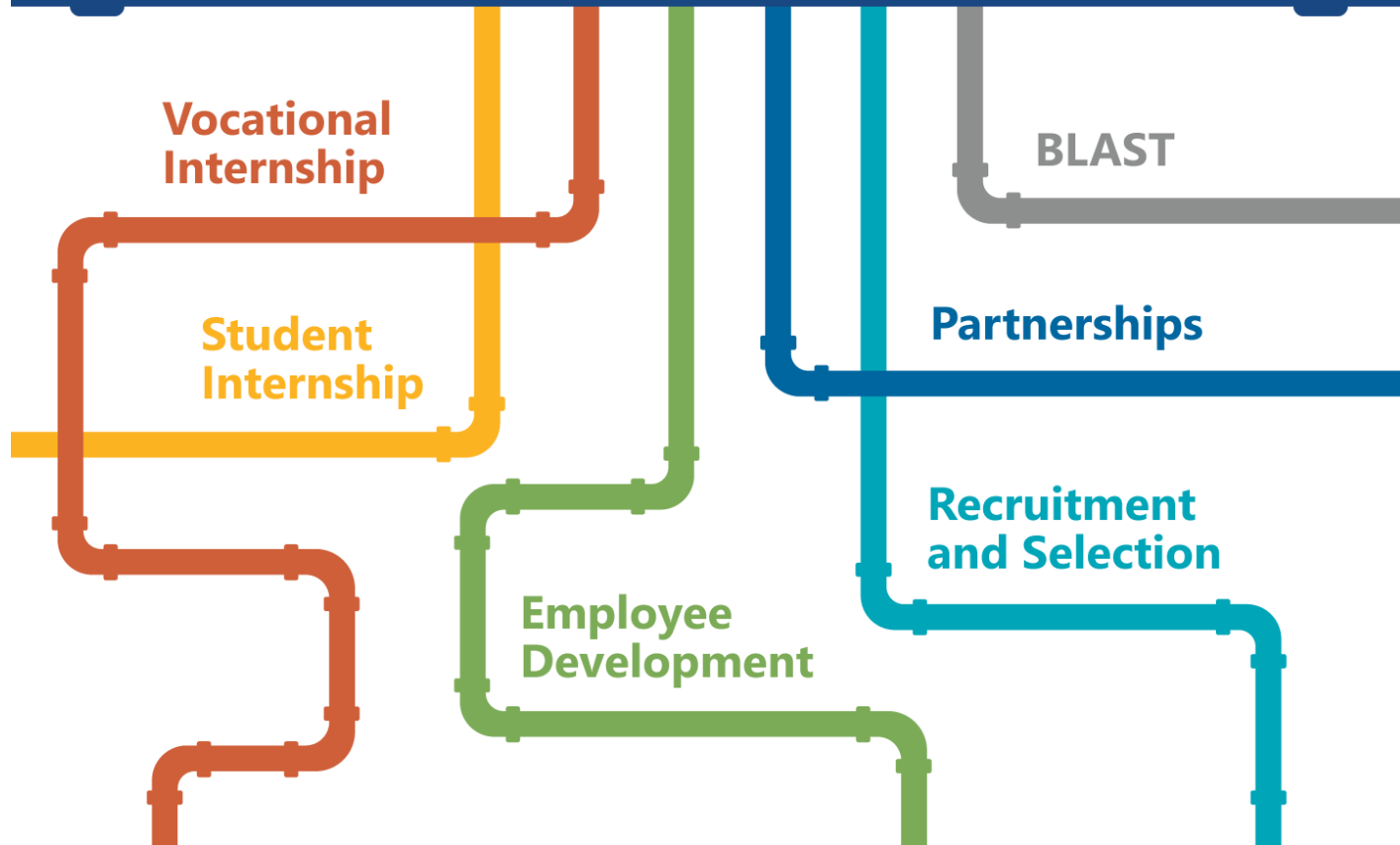
## Talent Readiness Assessments

Feeder positions are identified and talent pools are developed to build a **talent pipeline** for key and vulnerable positions.

# Overview of Existing Programs



## TALENT PIPELINE



# Vocational Internship



Technical Trades within  
Operations & Maintenance

Started in 2010 with 4 positions,  
currently at 10 positions

14 program participants have  
been hired





# Student Internships



# Employee Development



# Recruitment and Selection



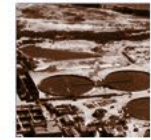
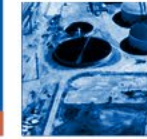
# Partnerships



**California Special  
Districts Association**  
*Districts Stronger Together*



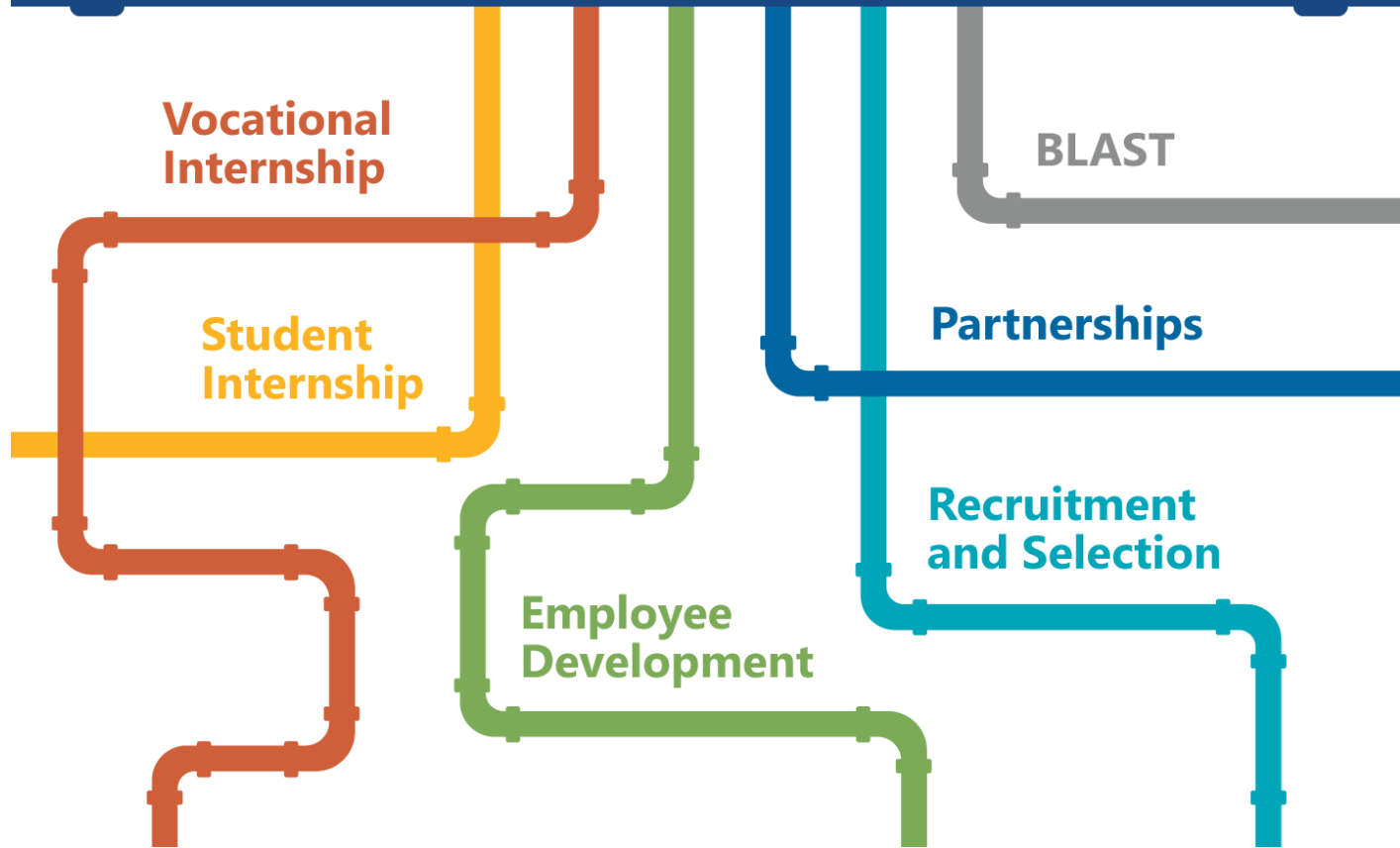
# Leadership Development



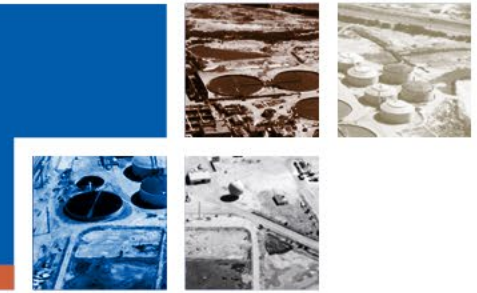
# Overview of Existing Programs



## TALENT PIPELINE



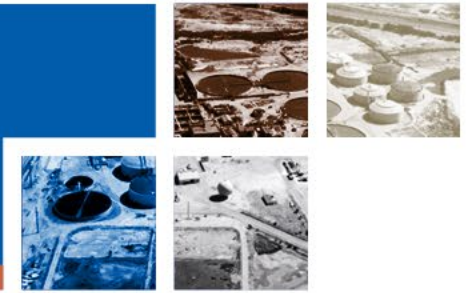
# Policy Statement



OCSD will attract and retain high-quality talent to support its mission and continue to be an industry leader.

OCSD will safeguard leadership continuity and support effective performance of the organization by proactively monitoring the changing work environment and requirements to ensure development programs are relevant and build a skilled bench of readily available successors for key leadership and mission-critical positions.

# Initiatives

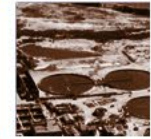
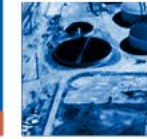


**Initiative:** Maintain and enhance current programs to provide the direction to identify, develop, attract and retain the next generation of prepared, capable and engaged leaders.

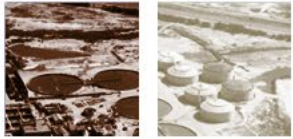
**Initiative:** Continue cyclical Classification & Compensation studies to ensure job classifications accurately depict the work and that compensation levels are set accordingly.



# Policy Question



***Is OCSD properly prepared for the future challenges of employee attrition and loss of institutional knowledge through employee development and leadership programs?***



**Questions?**



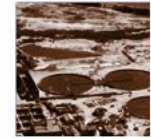
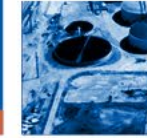
# Safety and Physical Security

**Book Page: 267**

**Presented by Rod Collins**  
*Safety & Health Supervisor*

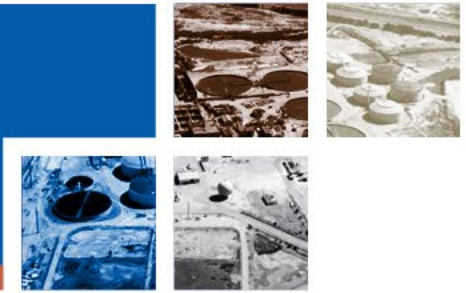


# Policy Question



***Is OCSD properly prepared to ensure the safety, health, and security of the workforce and have we adequately planned for emergencies?***

# Background



- OSHA requires a workplace free of recognized hazards
- Safety of the public and employees is OCSD's top priority
- OCSD is committed to identifying and mitigating all hazards
- OCSD has programs that have proved effective to ensure the safety and health of its workforce, visitors, and contractors

# Overview of Existing Programs



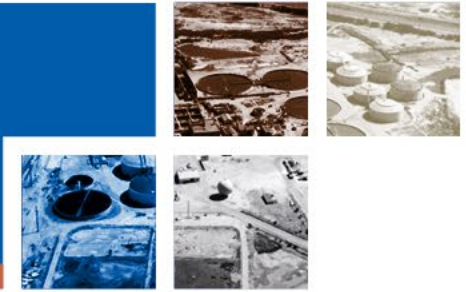
Safety



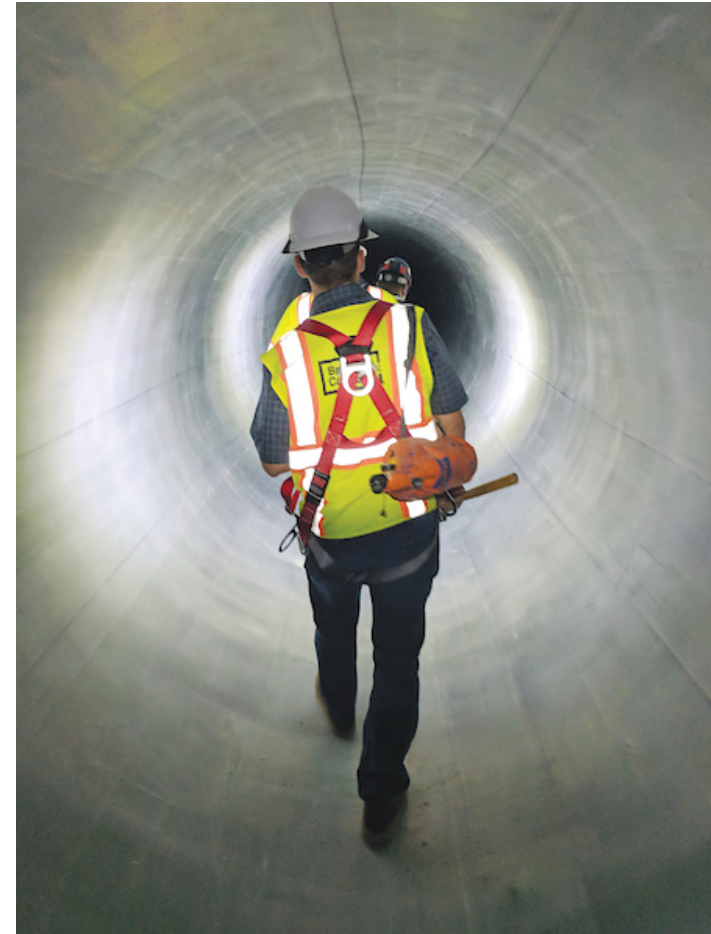
Security

Emergency

# Current Situation



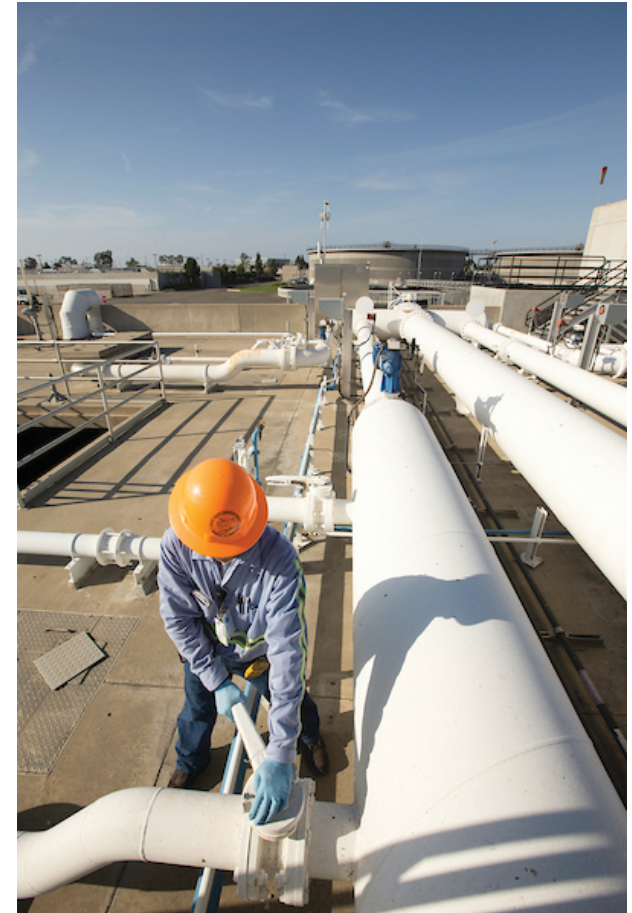
- Safety
  - Routinely review written policies and procedures by collaborating with internal stakeholders, third-party audits, and ensuring compliance with regulatory requirements
  - Preparing safety programs and facilities in pursuit of California OSHA Voluntary Protection Program status



# Current Situation

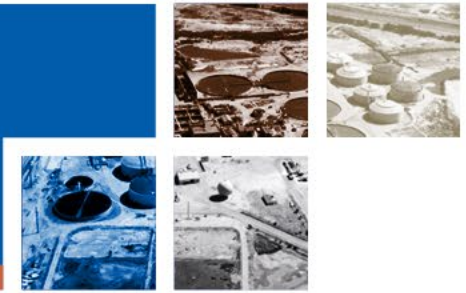


- Emergency Management
  - Ensure available resources are identified and engaged in the event of an emergency
  - Collaborations with local agencies and municipalities
  - Minimum of two emergency response drills per year





# Current Situation



- Security
  - Manage third-party security service provider
  - Preparation for expansion of Security requirements
  - Oversee Security Committee (Physical and Cyber Threats)



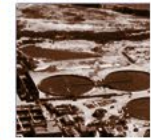
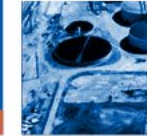
# Proposed Future Policy Statement



Continue to administer existing programs that ensure the safety, health, and security of the workforce, and proactively plan for emergencies to ensure continuity of operations.

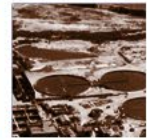
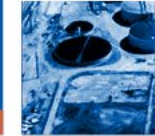
Proactively monitor the changing work environment and requirements to implement new programs that address future vulnerabilities. Improvements will be measured using leading metric indicators and reported to the workforce to foster employee engagement.

# Initiatives to Support Policy



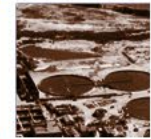
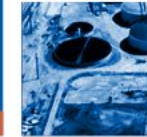
**Safety Initiative:** Complete outstanding safety projects, improvements, and corrective actions to apply and obtain Cal/OSHA Voluntary Protection Program (VPP) status; and continue to foster a culture where employees are accountable for their safety as well as the safety of others.

# Initiatives to Support Policy



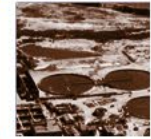
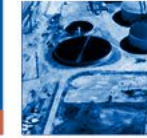
**Emergency Management Initiative:** Support facility and countywide emergency preparedness, response, and recovery efforts by partnering with entities, such as, the Water Emergency Response Organization of Orange County, Orange County Sheriff's Department, and local fire departments to plan and continue to conduct disaster preparedness training and exercises.

# Initiatives to Support Policy

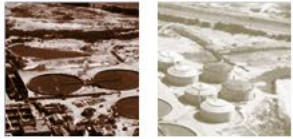


**Security Initiative:** Continually identify and assess vulnerabilities and implement solutions through the Security Committee and third-party assessments. Prevent/mitigate security breaches using physical security systems such as video monitoring, access control, and armed security patrols.

# Policy Question



***Is OCSD properly prepared to ensure the safety, health, and security of the workforce and have we adequately planned for emergencies?***



**Questions?**



# Cyber Security

Book Page: 273

Presented by Lorenzo Tyner  
*Assistant General Manager*



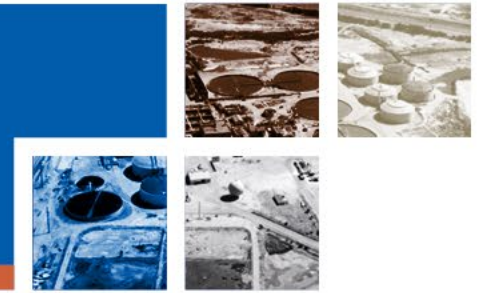


# Policy Question



***Has OCSD properly prepared for the increase in cyber security threats faced by today's government agencies?***

# What we're protecting?



## Industrial Control Network

- Remote control or monitoring of Plant assets - 370,000 electronic input and output data points
- 23 SCADA servers and 151 workstations
- 160 Programmable Logic Controllers (PLCs)
- 6 Terabyte of Data and 69 network switches

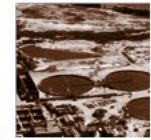
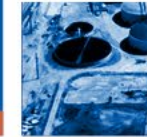
# What we're protecting?



## Office Network

- 310 Servers & 1,000 workstations and laptops
- 2 petabytes of data and 100 network switches
- Enterprise software applications
  - Financial Systems, Maximo Asset Management System, Laboratory Information Management System
- Personal identifiable information

# Current Cyber Security Threats



- Business Email Compromise (BEC)
- Ransomware
- Attacks on Critical Infrastructure

# Business Email Compromise



- 91% of cyberattacks start with email
- 5-20% of emails are suspicious
- 50 to 80% increase in attacks each quarter
- 2,370% increase in losses due to BEC

Insurer Slapped with \$2.2 Million HIPAA Settlement

*The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*

Everyone Is Falling For This Frighteningly Effective Gmail Scam

Russian hackers targeted just one Yahoo employee in order to breach 500M accounts

Coupa Software HR employee sends W-2 forms for all 2016 employees to an attacker posing as CEO

Seagate sued by its own staff for leaking personal info to identity thieves

Sources:

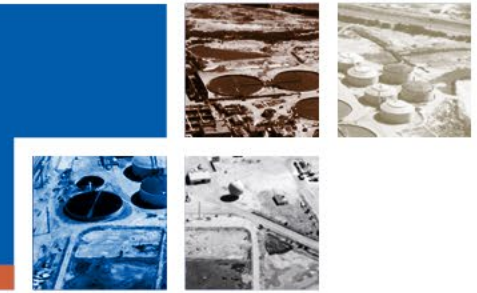
VALIMAIL, PhishMe, Proofpoint's Human Factor Report, FBI

# Recent OCSD Attacks



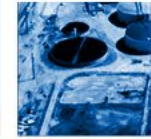
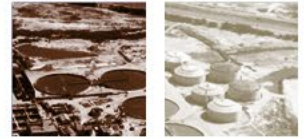
- Email spear phishing campaigns that appear very credible with OCSD logo, targeted at EMT, Managers, and specific business functions
- Voicemail attachments noting that you have several missed calls. Attachment leads to a phishing website to steal user credentials.
- False attempts to get users to change their password
- Phishing emails that disclose previously used passwords acquired from outside breaches to lure the recipient to open a malicious file

# Security Assessments



- Department of Homeland Security assessment
- Design Architecture Review
- Network Architecture Verification and Validation
- Microsoft Active Directory Security
- Microsoft Security Incident Management
- Microsoft Securing Lateral Account Movement
- Office 365 Security assessment
- CIS Top 20 Security Controls

# Defense in Depth



- Network Firewalls
- Intrusion Prevention System
- Web Filtering Gateway
- Next-gen Anti-malware
- Patch Management
- Backups
- Security Awareness Training





# Security Awareness & Training Program



- Multiple phishing security tests per month
- Quarterly security training videos
- Communicate cyber security best practices and tips
- Implemented Industrial Control Systems (ICS) Engineer Security Training
- Implemented Software Developer Security Training

# Critical Security Controls



## Basic CIS Controls

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

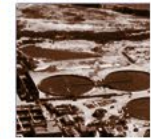
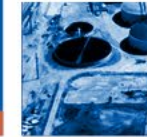
## Foundational CIS Controls

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

## Organizational CIS Controls

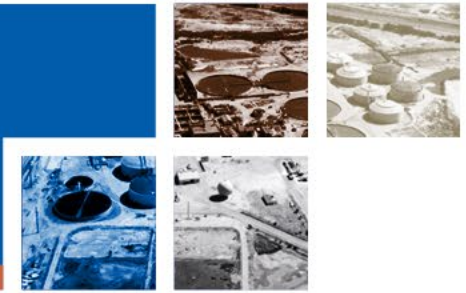
- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

# Best Practices



- Defense in Depth strategy
- Security Training and Awareness programs
- Patch Management processes
- 3-2-1 Backup Strategy
- Critical Security Controls and Frameworks
- Incident Response
- Sensitive Data Classification and Handling Policy
- Develop close relationship with Operational Technology

# Policy Statement



The Sanitation District must maintain adequate cyber security (information technology security) techniques that protect computer assets, networks, programs, data, and industrial control equipment from unauthorized access or attacks that are aimed for exploitation.

# Initiatives to Support Policy



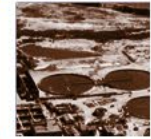
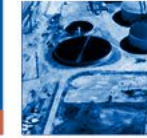
**Initiative:** Conduct various Incident Response tabletop exercises to determine the organization's ability to respond to a targeted cyberattack and to improve the quality of the response, should an attack occur.

**Initiative:** Evaluate, enhance and monitor network security including activities to protect the usability, reliability, integrity and safety of the network by developing Security Operations Center (SOC) capabilities that support continuous monitoring and is responsible for the continuous threat protection process.

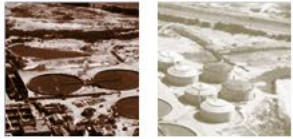
**Initiative:** Conduct a comprehensive third-party cyber security operations assessment (Red Team). A thorough Red Team engagement will expose vulnerabilities and risks regarding:

- Technology — Networks, applications, routers, switches, appliances, etc.
- People — Staff, contractors, departments, business partners, etc.
- Physical — Offices, warehouses, substations, data centers, buildings, etc.

# Policy Question



***Has OCSD properly prepared for the increase in cyber security threats faced by today's government agencies?***



**Questions?**



# Real Estate and Property Management

**Book Page: 277**

**Presented by Lorenzo Tyner**  
*Assistant General Manager*





# Policy Question



***Should the OCSD develop in-house  
Property Management/Real Estate  
resources or continue to outsource  
specialized services as needed?***

# Sanitation District Assets



**OCSD has more than \$11 billion in assets**

- Most of these assets are directly related to the plant or physical infrastructure.
- However, OCSD owns considerable real estate, property rights, and easements.
- OCSD owns and maintains real estate for the specific purpose of supporting its operations. OCSD does not purchase for speculation or investment purposes.

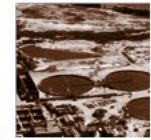
# Recent Property Activities



## **In the last three years, OCSD has been very active**

- In February 2017, OCSD purchased two the properties each approximately 25,000 square feet. This will be the location of OCSD's future headquarters building.
- In March 2018, OCSD purchased a commercial office building that currently houses OCSD's Resource Protection Division with 37 staff, as well as nine commercial tenants.
- In August 2018, OCSD purchased 3 commercial/industrial properties with a combined total of 66,000 square feet. This will be part of the new Headquarters parking compound. When purchased, the properties were leased to a total of 8 tenants.
- In April 2019, OCSD sold its Garden Grove commercial/industrial building. This building has been leased to the same tenant since 2011 and had generated more than \$1.6 in revenue prior to its sale.

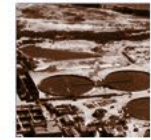
# Recent Property Activities



**In the last three years, OCSD has been very active**

- Edinger Pump Station (Huntington Beach)
- Bay Bridge Pump Station (Newport Beach)
- Western Regional Sewers Project (Denni Street, Cypress)

# Recent Property Activities



## Upcoming Activities

- Yorba Linda Pump Station (Fullerton)
- West Side Pump Station (Rossmoor/Unincorporated area)
- Miller-Holder Trunk Sewer on Rhone (Huntington Beach)
- Mass Annexations in our Service Area

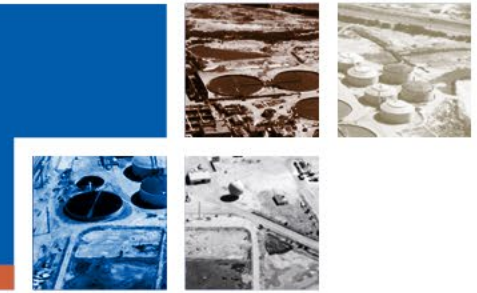
# Other Property Activities



## OCSD is often involved with other agencies

- OCSD has leased two of its vacant buildings to the Fountain Valley Police and Fire Departments for training exercises.
- The Fire Department runs nighttime training exercises and has numerous joint sessions scheduled with the City of Huntington Beach Fire Department between October and May.
- Before the Doig Drive building was leased, the City of Garden Grove's K-9 unit utilized that commercial/warehouse for drug sniffing exercises with their elite team of canine officers.

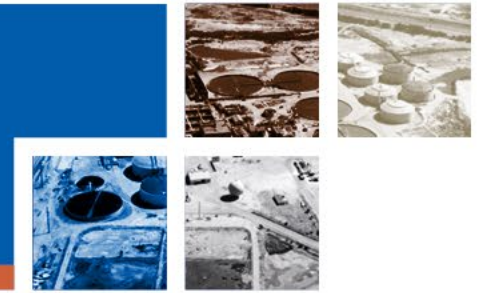
# Property Rights and Easements



## **OCSD has just begun to assess all its property rights**

- OCSD has a vast array of property rights including ownership in fee, easements, permits, perpetual encroachment permits, licenses and leases, as well as shared utility corridor rights, and public rights-of-way.
- OCSD is working with an outside consultant to map, label, and quantify all property rights and encumbrances inside and outside of the plants.
- This is about 50% complete and we hope to complete the project by the end of December 2019.

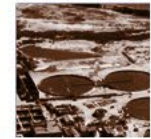
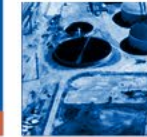
# OCSD Resources



- OCSD maintains minimal staff that currently manages its Real Estate or Property Management activities.
- Staff is familiar with general issues in this area
- OCSD utilizes General Counsel as needed
- To date, OCSD has made a conscious decision to use in-house generalists and general counsel for its day-to-day needs instead of building property management infrastructure and adding staff.
- OCSD has relied on specialized contracted resources when specialized support is required.



# Initiatives to Support Policy



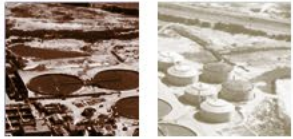
**Initiative:** Complete work with an outside consultant to map, label, and quantify all property rights and encumbrances inside and outside of the plants.

**Initiative:** As part of the 2020-21 budget process, add in-house professional real estate and property management staff to ensure comprehensive management of OCSD's significant real estate and property rights.

# Policy Question



***Should the OCSD develop in-house  
Property Management/Real Estate  
resources or continue to outsource  
specialized services as needed?***



**Questions?**