EAST BAY MUNICIPAL UTILITY DISTRICT

# Critical Infrastructure Protection-Attacks-Response


Steve Frew – EBMUD

CUEA Board of Directors

Chair – Water/Wastewater Committee

Member, Strategic Planning Committee


California Utilities Emergency Association (CUEA)
Annual Conference 2016 - Pasadena

# Agenda

- Overview of Recent Crime affecting Critical Infrastructure in the Bay Area
- Reporting Crime to Police or Sheriff's Office
- Connecting the Dots - Investigations
- State Law vs Federal Law – Investigation and Prosecution
- Discussion - Q and A

# Our Panel:

FBI – Special Agent Kyle Biebesheimer

EPA – Criminal Investigations – Scot Adair

LAPD/JRIC – Detective Kurt Wong

JRIC – Critical Infrastructure Assessor (CIA) Andrew Carlson

JRIC – CI/KR Analyst Nate Watson

US DHS – PSA Richard Scott Mitchem

# Prelude:

- SUMMARY of real cases
- EXAMPLES that could affect any of us
- SOLUTIONS you can begin today….

# Recent Infrastructure Attacks

- PG&E Metcalf substation in San Jose on April 16, 2013.
- Radio Tower in San Ramon, July 30, 2013
- Fiber optic lines cut in Berkeley, Fremont, Walnut Creek and San Jose, July 6, 2014,
  - February 2015 cables were cut again in Fremont
  - June 2015 cables cut again in Fremont and Walnut Creek.

# More Fiber Optic Cable Cuts

- 7-6-14 Berkeley
- 7/6-14 at 11:39 PM Freemont
- 7/6/14 an hour later Walnut Creek
- 7/6/14 30 minutes later again in Freemont
- 7/7/14 in San Jose
- 2/24/15 - 11:30 PM - 2 more cable cuts in Fremont

# Cable Cuts Cont'd

- 6/8/15  in Alamo
- 6/8/15 (again) in Fremont;
- 6/9/15 in Walnut Creek
- 6/30/15 - Along I-80 and Highway 24, Oakland to Berkeley, Wave Broadband case affected cable service in Alameda County, SF and Sacramento area
  - Affected Internet wholesalers
  - Internet, television, and phone service impacted
  - Slowdown on cloud computing service
- 9/14/15 10:30 PM  - Altamont Pass - ATT offered $250K reward for information

# Alameda County Water District

- May 21, 2015 early AM hours
- Suspects vandalized (cut) an inflatable Dam
- 50M gallons of water dumped into Alameda Creek and into the Bay
- Scot Adair will discuss this case shortly…..

# Petroleum Pipeline Tampering

- 6/2/15 1:21 AM - in Albany near Eastshore Highway
- 6-3-15 9:15 PM in Alamo near the Iron Horse Trail, 9:15 PM
- 6-3-15 in Albany (again) near Eastshore Highway
  - In each case - cut locks on vault hatches, cut and removed locks and lock-out-tag-out chains and inside vaults

# Tampering with Public Water System - EBMUD

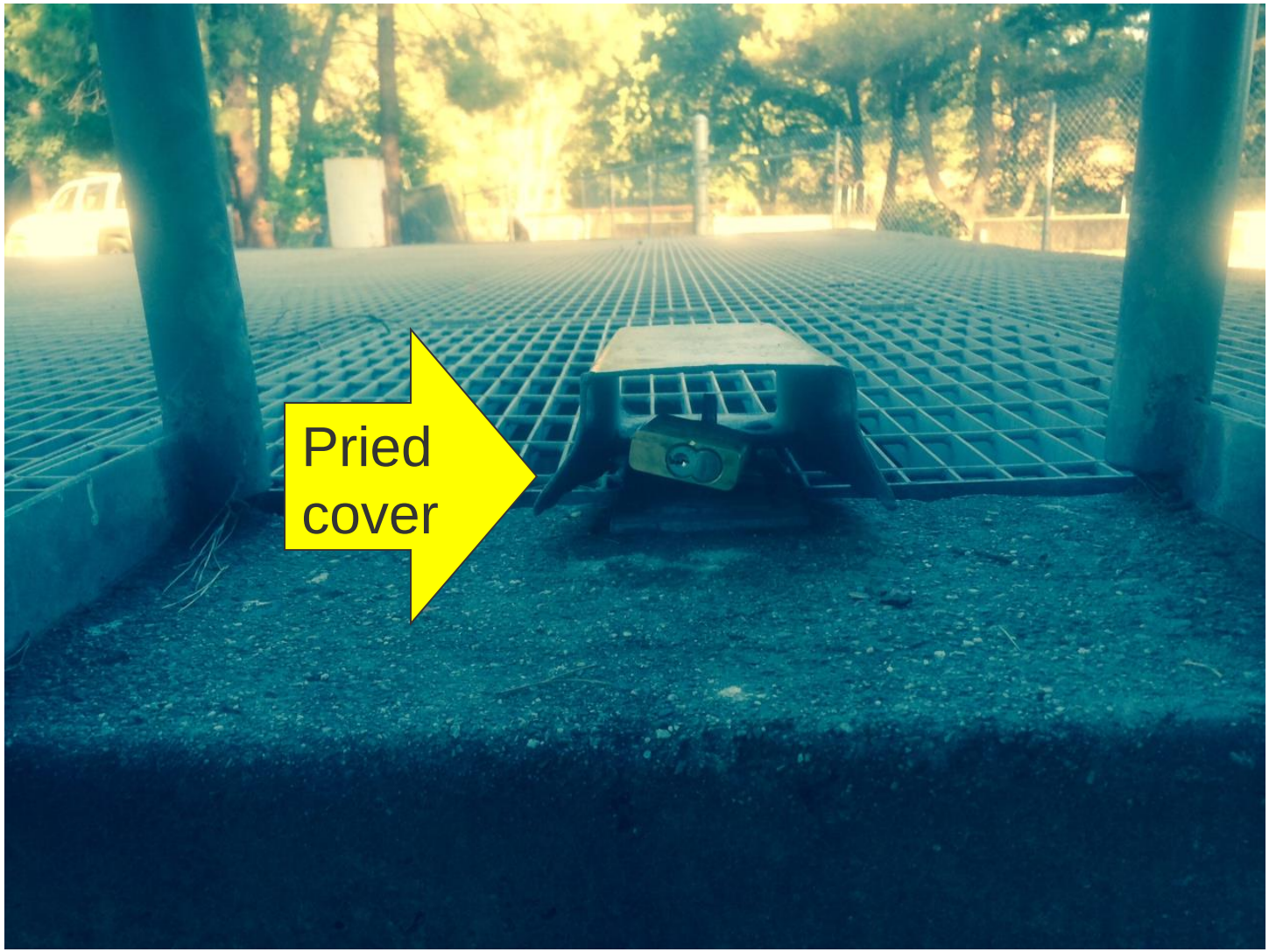
Walnut Creek WTP, Sunday, June 6, 2015 about 9:00 PM

- Two under-ground vaults behind WC WTP along Diablo/Briones Trail - locks cut on vault hatches
- In one, no damage
- In the other, one valve turned slightly on, the other turned completely off – shut off raw water intake to the plant, shut down the plant.

# WC WTP Cont'd

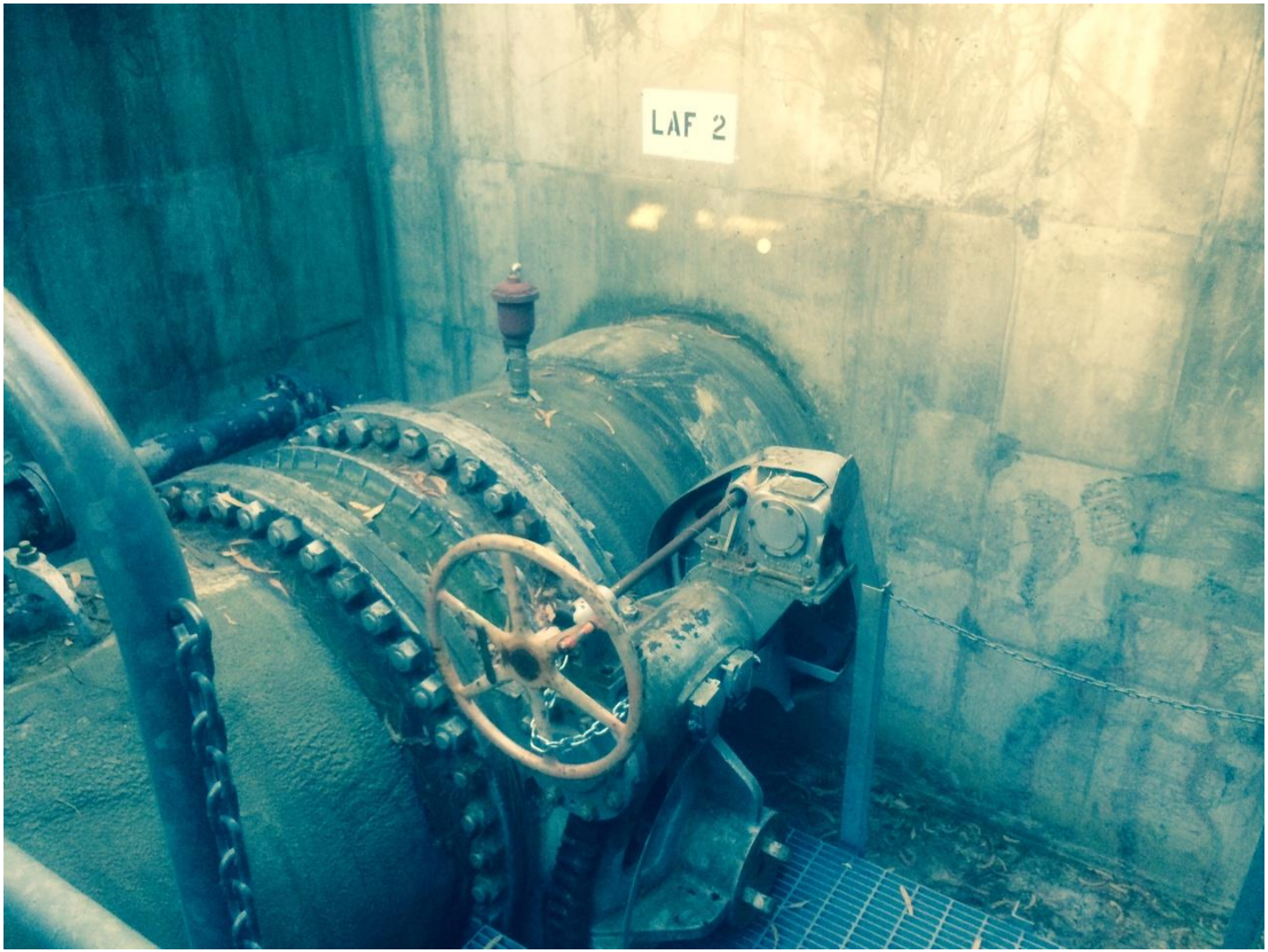
- Reported to Walnut Creek police and to District Security and Operations dispatchers
- Aqueduct and Water Treatment systems affected
- WCPD responded that night – lead agency investigating
- Following day, EPA Criminal Investigations Unit, and by Thursday of that week FBI assigned

# BEFORE - Padlock – pried - cut



# AFTER - New Puck Lock & Protective Hasp – Can't cut!

# Valve Was Tampered With



# Report Crimes Affecting Your Infrastructure

- Report to local police or Sheriff
- TELL THEM if the crime affects your Critical Infrastructure – and what SECTOR it is
- Try NOT to touch things and if you MUST use latex gloves, in layers - PROTECTS EVIDENCE
- Preserve and protect the scene of the incident for law enforcement

# What CRIME is it?

- California Penal Code
  - PC 459 Burglary
  - PC 487 Grand Theft
  - PC 488 Petty Theft
  - PC 594 Vandalism
- California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. (California Civil Code s. 1798.29(a) and California Civ. Code s. 1798.82(a))
- Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. (California Civil Code s. 1798.29(e)and California Civ. Code s. 1798.82(f))

# State Crime Vs Federal Crime

- What THRESHOLDS trigger FEDERAL attention/investigation?
- How familiar are city police and county sheriff's with what federal laws apply and how they can get to them?
- As the owner of the infrastructure YOU should know and be able to help them
- Here is an example from the WATER SECTOR:

# Example – Water Sector - Tampering

- Tampering with a Public Water System in covered under federal law, under the Bio Terrorism Act of 2002, carries serious fines and prison penalties
- Title IV, US Code The Safe Drinking Water Act

- Sec. 300i-1 - Tampering with public water systems
- Sec. 300i-2 - Terrorist and other intentional acts
- Sec. 300i-3 - Contaminant prevention, detection and response
- Sec. 300i-4 - Supply disruption prevention, detection and response

# Who Do You Call?

Reporting (when it happens)

- Police/Sheriff
- Your Joint Regional Intelligence Center (JRIC) or Joint Terrorism Task Force (JTTF)
- EPA Criminal Investigations (Water Sector)
- FBI (terrorism – interstate crimes)

# Meet Your Resources

Now let's hear from each of our panel members:

First Special Agent Kyle Biebesheimer, who was assigned to look at potential connections between all of these cases…

# FBI/Joint Terrorism Task Force

- Overview
  - 56 FBI Field Offices nationally
  - In California, four separate Field Offices:
    - Los Angeles
    - San Francisco
    - San Diego
    - Sacramento

# FBI/Joint Terrorism Task Force

- CT/JTTF
  - Agents and TFOs
  - IT and DT Squads
  - Acts of “terror”
    - fed. crime of force/violence against person/prop.
    - influence change
    - ties to foreign power*

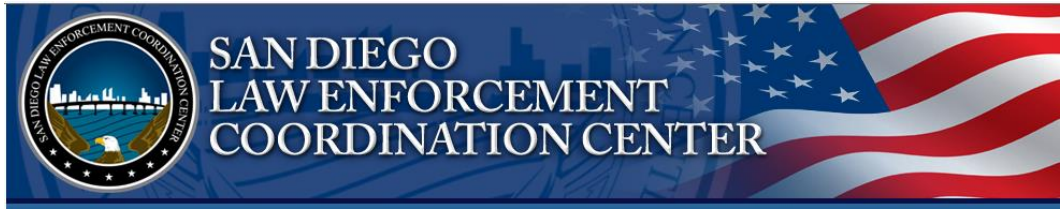

# Sharing Information

- Fusion Centers
  - Monitor regional, national trends
  - Disseminate intel bulletins to local, state, and federal LE; and private sector partners
  - Essential link in the information sharing process

EBMUD








# Five California Fusion Centers:

San Francisco, Los Angeles, Sacramento,
Orange County, and San Diego

# “Connecting the dots”

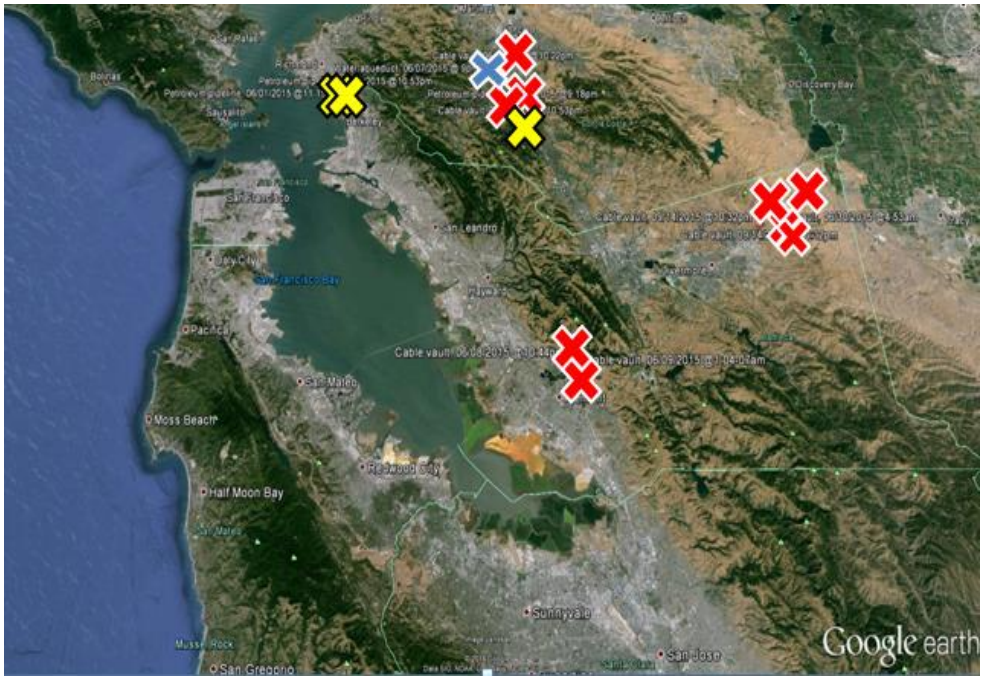
- Rise in bay area crimes targeting infrastructure, 2013-
  - Electrical (1)
  - Communication (17)
  - Petroleum (3)
  - Water (2)

# “Connecting the dots”

- My investigation
  - Initial focus on severed fiber optic cables
  - Shared info with fusion center
  - Fusion center shared info regarding water and petro

# “Connecting the dots”

- My investigation
  - Met providers; toured crime scenes
  - Uncovered 20+ (related?) attacks on critical infrastructure
  - Partnered with local LE
  - Multiple federal violations on point



# Conclusion

## Takeaways

- Information sharing was key
- Fusion center provided necessary link
- Established LE-utility provider liaisons for future use

## Misconceptions

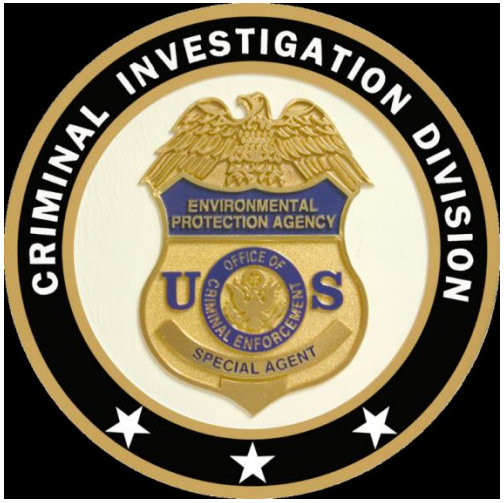
- All LE share information with each other, all the time—FALSE
- All FBI/JTTFs share information with each other, all the time—FALSE
- All infrastructure crimes can be prosecuted federally--FALSE

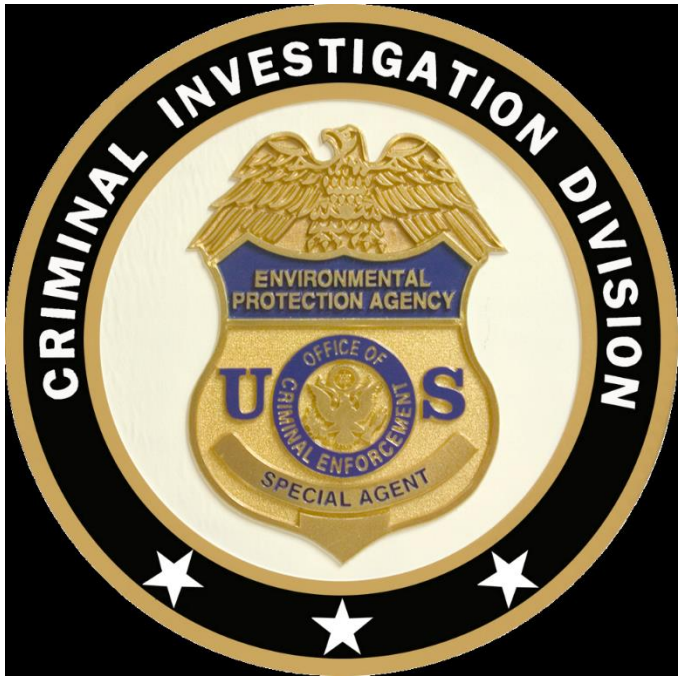
# Next, Scot Adair
# EPA Criminal Investigations

## United States Environmental Protection Agency

## Criminal Investigation Division

## Region 9




CRIMINAL INVESTIGATION DIVISION
ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF CRIMINAL ENFORCEMENT
U S
SPECIAL AGENT

- EPA-CID consists of approximately 160 Special Agents
  - Agents are sworn federal law enforcement officers
  - Make arrests and execute warrants
  - Carry firearms
  - Investigate a variety of environmental crimes

# SAN FRANCISCO AREA OFFICE
## EPA-CID Region 9

- Cover CA, NV, AZ, HI, and the Pacific Islands
- 1 SAC and ASAC
- 15 SAs
  - 4 in San Francisco
  - 2 in Phoenix
  - 1 in Sacramento
  - 4 in Los Angeles
  - 2 in San Diego
  - 2 in Hawaii

UNITED STATES EPA-CID

# CRIMINAL ENFORCEMENT OF FEDERAL ENVIRONMENTAL LAWS

- Knowing or negligent behavior
- Significant and most egregious violators
- Involve lengthy, complex investigations
- Potential for fines and/or incarceration

# FEDERAL STATUTES ENFORCED

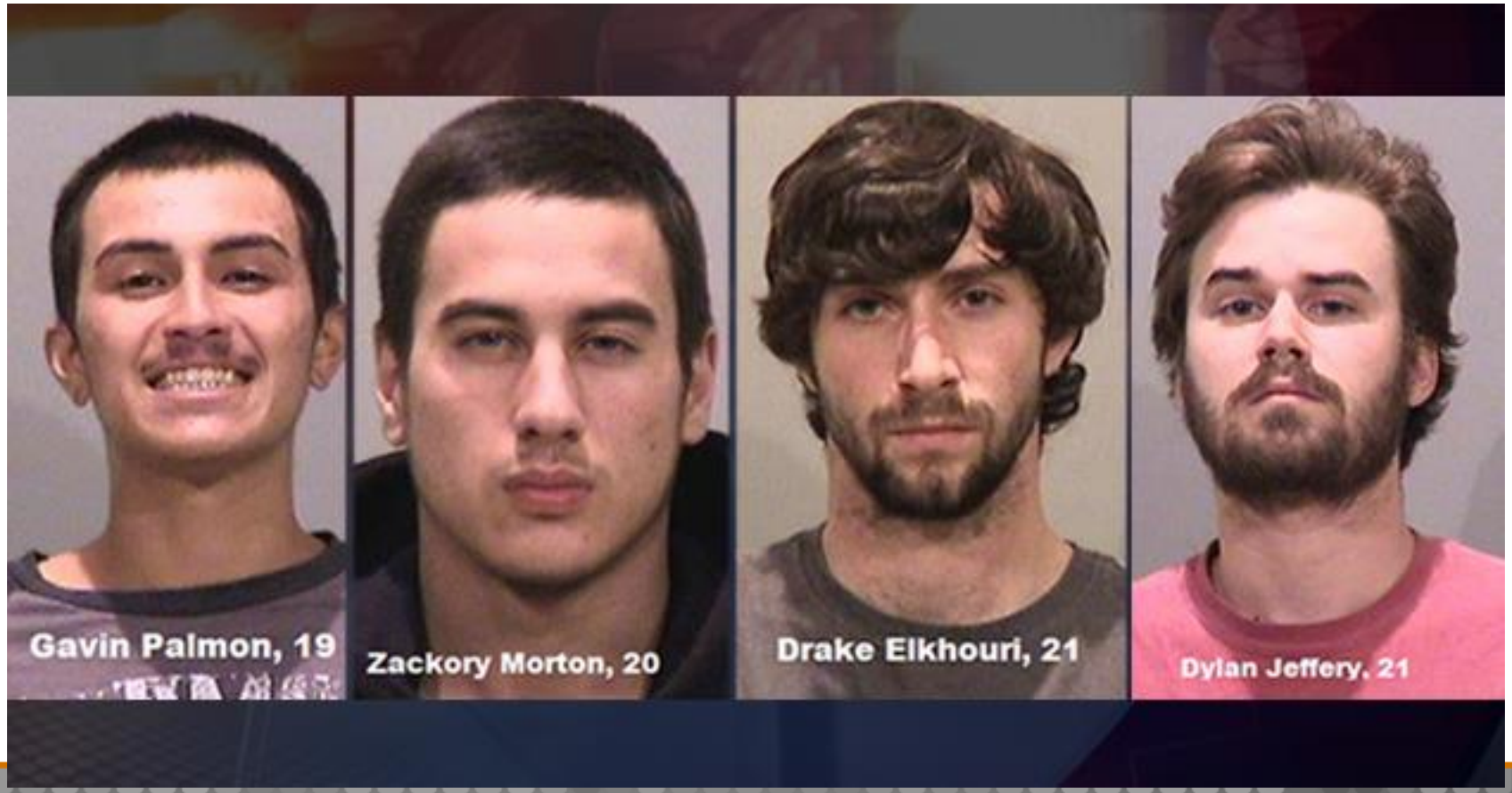
- RCRA
  - Hazardous waste management
- CERCLA
  - Superfund
- CWA
  - Surface waters
  - Sewers
- FIFRA
- SDWA
- CAA
  - Asbestos
  - Stationary Sources
  - Mobile Sources
- EPCRA
- TSCA
- Title 18 U.S.C.
  - False Statements
  - Conspiracy
  - Mail Fraud
  - Wire Fraud

# SAN FRANCISCO AREA OFFICE
## EPA-CID Region 9

- EPA CID
  REGION 9
- Office : Main
- (415) 947 8713

Environmental Protection Agency
Criminal Investigation Division

# Fremont Dam Incident – May, 2015



Environmental Protection Agency
Criminal Investigation Division

# Fremont Dam

- **Background**:
- Alameda County Water District services 348,000 customers
- Union City, Newark, and Fremont
- Water supply – local aquifers and Hetch Hetchy
- Alameda Creek used to impound untreated drinking water behind inflated rubber dam (ACWD Dam #1)

Environmental Protection Agency
Criminal Investigation Division

# Fremont Dam

Environmental Protection Agency
Criminal Investigation Division

# Fremont Dam

- **Incident**:

- 3:00am, May 20, 2015, video captures images of three males on site at dam, behind trespass signs.

- 1:00am, May 21, 2015, video again captures image of three males behind trespass signs.

- 12 lateral cuts and 1 large vertical cut in dam. Approximately 49 million gallons (150 acre feet) of untreated drinking water lost to San Francisco Bay.

Environmental Protection Agency
Criminal Investigation Division

# Fremont Dam

Environmental Protection Agency
Criminal Investigation Division

# Fremont Dam

Environmental Protection Agency
Criminal Investigation Division

# Fremont Dam

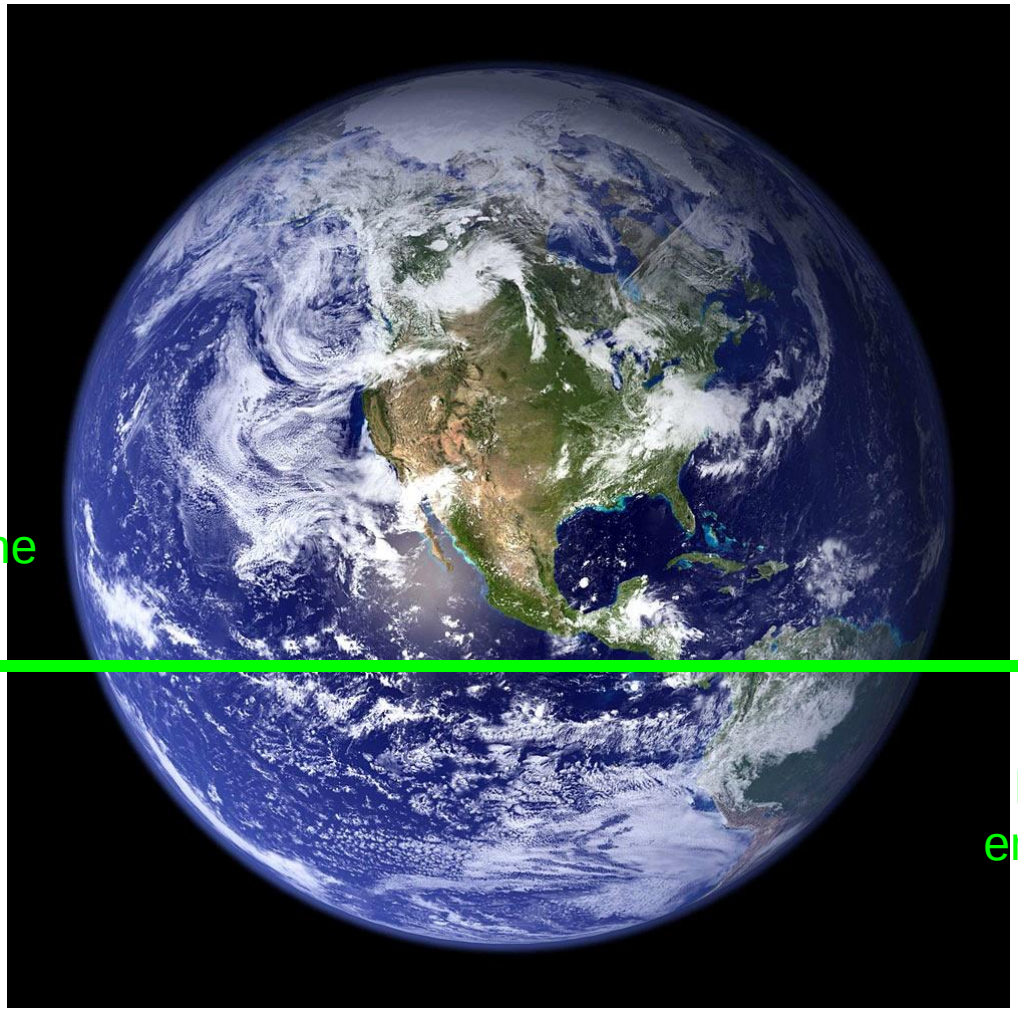
- **Investigation**:
- Fremont Police Department actively investigates crime – 60 months.
- Video sources, cell phone activity, witness statements
- EPA-CID: Consult with Fremont PD, ACWD, Department of Justice
- Social Media monitored

Environmental Protection Agency
Criminal Investigation Division

# Fremont Dam

- **Arrest/Charges/Adjudication**:
- November, 2015, four individuals arrested and charged with felony vandalism.
- Elkhouri plead guilty to single felony vandalism charge – sentenced to one year in county jail.
- Other three – misdemeanor trespass pleas. Time served

The thin green line



Between you and environmental crime

# Next, LAPD Detective Kurt Wong

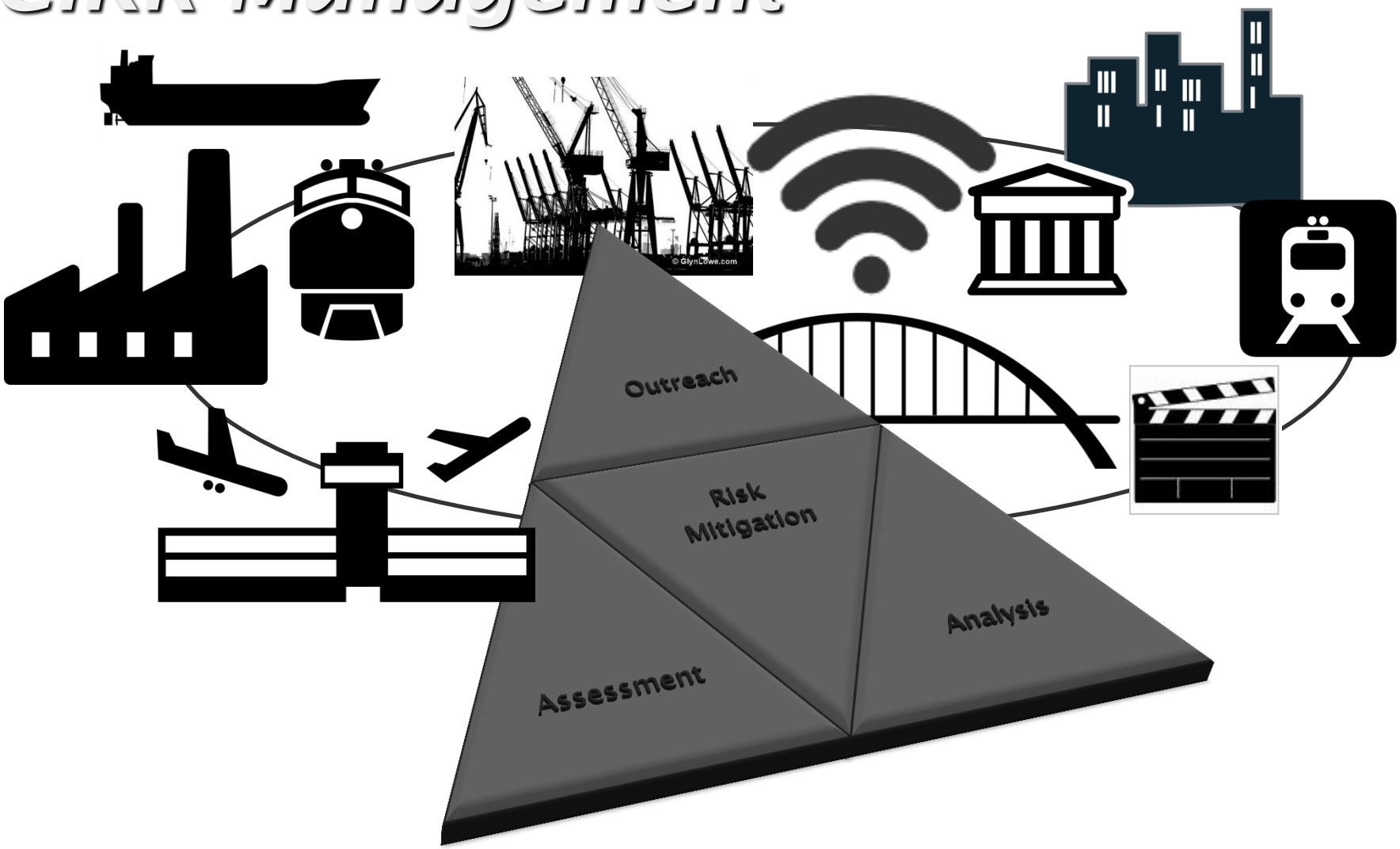
- Kurt Wong, Detective, LAPD and Los Angeles Joint Regional Intelligence Center (JRIC)
  - Andrew Carlson, Critical Infrastructure Assessor
  - Nate Watson, CI/KR Analyst
  - Richard Scott Mitchem, Protective Services Advisor, US DHS

# The Joint Regional Intelligence Center

## *Critical Infrastructure Protection Working Group (CIPWG)*

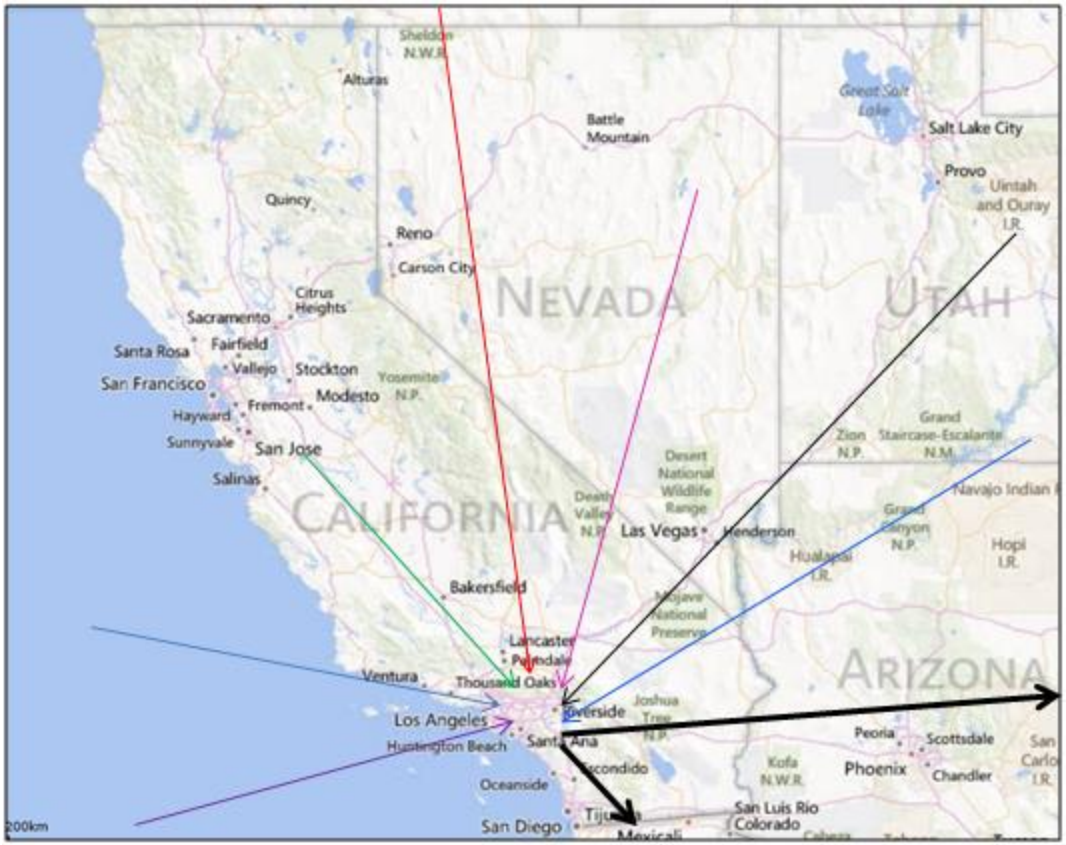
Los Angeles · Orange · Riverside · San Bernardino · San Luis Obispo · Santa Barbara · Ventura

# CIKR Management



# Lifelines and Supply Chains

- Infrastructure within the region has national significance; some assets are essential to the national supply chain



# Security Vulnerability Assessment

The ultimate objective

- Develop the most effective mitigation measures to achieve the desired levels of protection

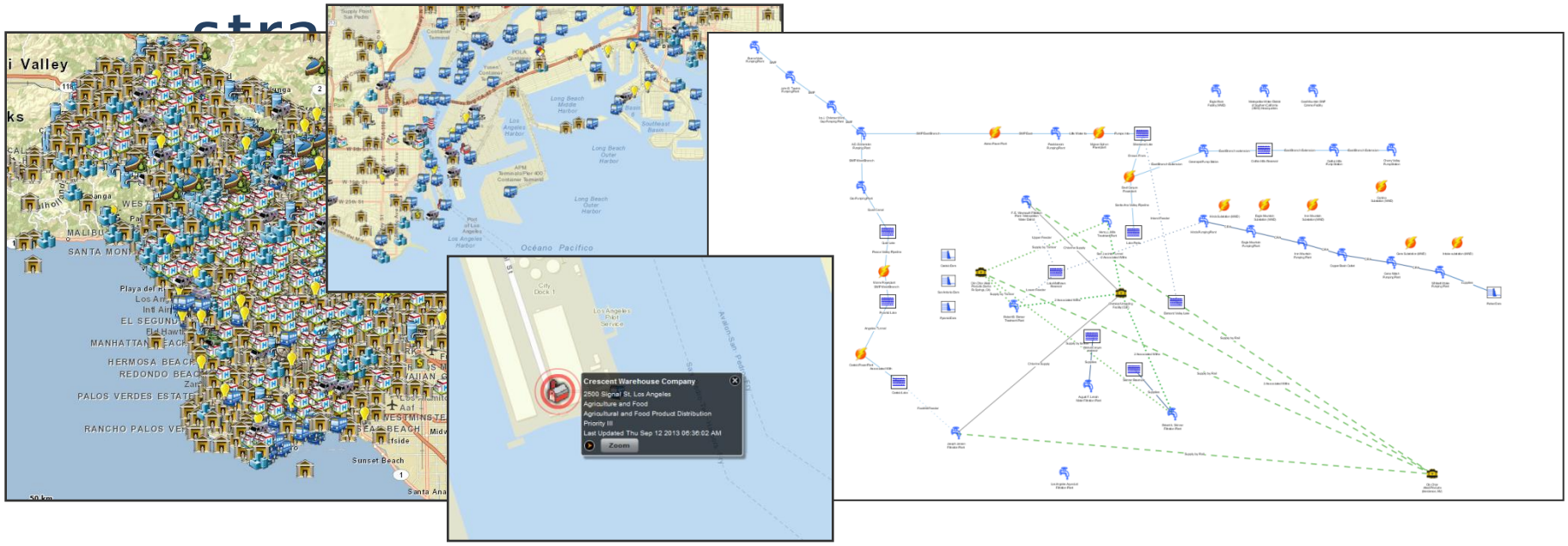
# Security Vulnerability Assessments

- Department of Defense and Department of Homeland Security Guidelines
- Non-regulatory and provided at ***NO COST***
- No “check-ups” on implementation
- Focus on “low-cost”/ “no-cost” options
- Objective “unbiased” perspective
- Enhance overall security and vulnerability awareness

# CIKR Analysis

The ultimate objective

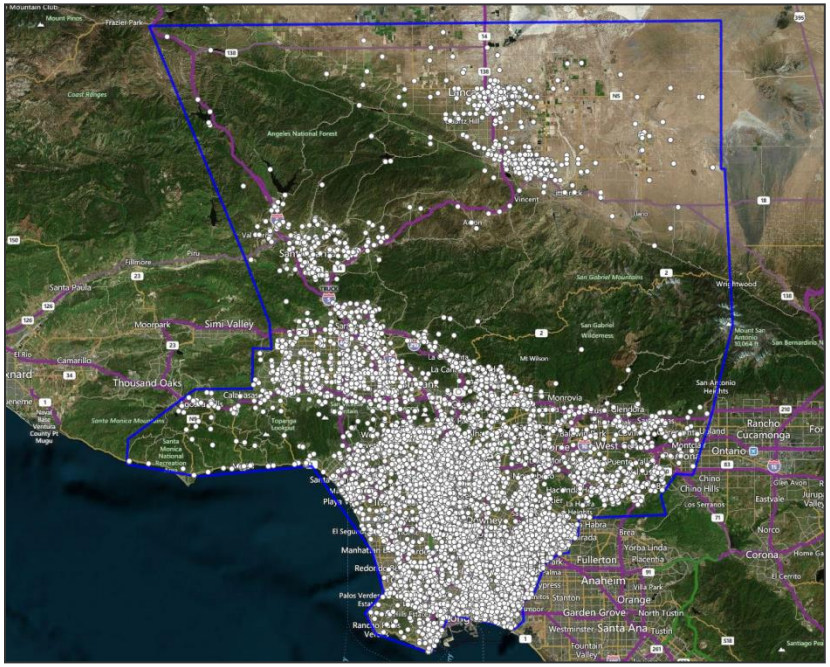
- Develop databases, tools, and products to guide risk mitigation stra

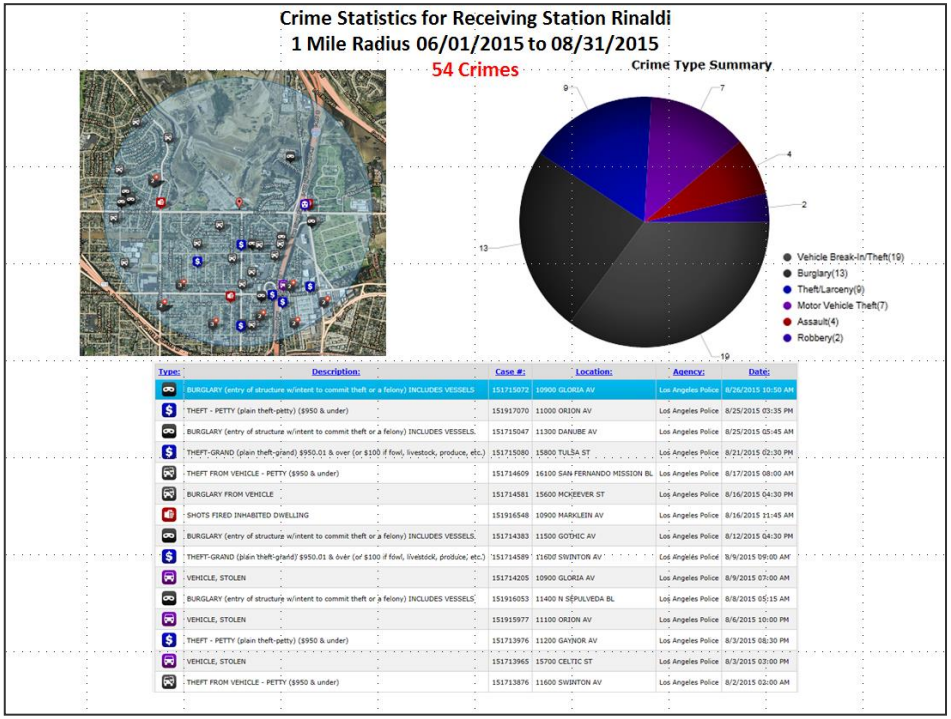


# CIKR Analysis

And

- Develop site specific analytical products to inform our internal and external stakeholders



# Outreach

Cultivating contacts

- Trusted relationships built through unbiased and security advice and support
- InfraGard Los Angeles
- Sector specific engagement with industry groups

# Questions ?

JRIC CIPWG

JRICCIPCELL@JRIC.ORG

# Take-Aways:

- Meet with Kyle, Scot, Kurt, Andrew, Nate and Richard, and share contact information here TODAY
- Reach out to your police and sheriff's offices locally to introduce them to YOUR infrastructure SOON
  - Provide Tours & Presentations about YOUR organization to your first-responders
  - Learn what you can do to help them respond to and enforce laws applicable to your infrastructure (signage – reporting procedures)

# Thanks to our Panel on Critical Infrastructure Protection

- Now let's open the floor to questions for our panel members