Facility XXXX Site Security Survey   Date: 10/9-10/10/02

(A) Perimeter Security			
Feature	Yes	No	Comments
DELAY/DETER			
Site Boundary			
Fence (Height and Construction)			None of the critical facilities have protective fences.
Outriggers			
No Trespass Signage			
Vehicle Barriers			
Employee Gate			
Shared Gate			
Back Gate			
Geographic Barriers (i.e. water)			
Vegetation			All critical facilities are surrounded by pavement with the exception of the PFP metering building. This building is on a golf course and grass is kept mowed
Inside the Site			
Buildings			
Restricted Access Areas			The areas are kept locked or are in manned facilities
Fences and Walls			
Target Areas			
Enclosures around critical areas			
DETECTION/ASSESSMENT			
Sensors – fence (security)			
LIGHTING			
Dark areas? Glare?			Very poor lighting is present at facilities. Lighting is limited primarily to just over doorways.

NARRATIVE SUMMARY – Section A Perimeter Security

Perimeter security is non-existent at all of the critical facilities. The only security measure at any of the facilities are a single locked door separating an intruder from the critical asset. Only at PFP main building are any full-time personnel present.

(B) Access Controls / Systems			
Feature	Yes	No	Comments
ACCESS/EGRESS POINTS			
Personnel – Employee Vehicle Portal			No control, open roadway to parking
Personnel – Contractor Vehicle Portal			Contractors use employee parking areas
Vehicle portal			No control, open roadway to parking
Visitor Control			
Personnel access / control			Locked exterior door on smaller buildings, operating personnel at PFP main building
Vehicle access / control			No control, open roadway to parking
Confidentiality Agreements			
ID Checks			
Employees			
Badges issued?			Badges issued but not worn
Displayed at all times?			
Photo?			
Visitors			
Visitor badge issued?			
Displayed at all times?			
Reconciliation of visitor badges?			
Vendors ID checked or badge issued			
Contractors ID checked or badge issued			
Chemical delivery driver			
ACCESS CARDS			

Type of System - None		**System 1**	**System 2**
Card Technology		None	
Accountability		None	
Card Access Areas		None	
Card Distribution		None	

INTRUSION DETECTION			
Fence Sensors, Door and Hatch Sensors, Motion Detection			None installed
Monitored by service provider or internally?			
Response capability			
KEY CONTROL			
Accountability			There is no key accountability
HR Dir Plant Manager Safety/Security Mgr Other:			
Are keys signed in and out?			
Keys are Requested from?			Supervisor
Keys are Reproduced by?			Keys are freely reproduced by any locksmith in town
Key Log?			
Secured doors noted			
Unsecured doors noted – if yes, where?			
SIGNAGE AT ENTRANCE			
Weapons Policy			
Subject to Search			
CONTRABAND DETECTION			
Searches			
X-ray, metal or other detection			
Prohibited articles (i.e. weapons)			
PARKING			
Locations? Inside or outside the perimeter or protected area?			Parking is in uncontrolled areas.
Controls / restrictions			There are no parking controls
TRAFFIC FLOW			
Access prohibited or restricted within the site or facilities			

NARRATIVE SUMMARY – Section B Access Controls

The only security measure at any of the facilities are a single locked door separating an intruder from the critical asset. Only at PFP main building are any full-time personnel present.

(C) Security Force Management			
Feature	Yes	No	Comments
GUARD SERVICE			
Type of Guards			
Proprietary Contract			N/A
Armed Unarmed			N/A
Stationary Mobile			N/A
Guard Contractor Company			N/A
Guard Supervisor(s)			N/A
Guard Staffing / Shifts			N/A
Guard Locations			N/A
Means of Communication			
Silent Alarm Hand held radio Telephone Other: Pager			N/A
Direct lines to monitoring station			N/A
Direct lines to LLEAs			N/A
Guard Equipment			
Weapons Flashlight Other: _____			N/A
Training			N/A
EMT Other: __			N/A
Post Orders?			N/A
Daily Log?			N/A
Incident Reports?			
Conduct Safety Briefings?			
Evacuation Procedures?			
Bomb Threat Procedures?			
Contact with Local Law Enforcement?			

NARRATIVE SUMMARY – Section C Security Force Management

There is no force management in place

(D) Video Surveillance System			
Feature	Yes	No	Comments
CAMERAS			
Number of Cameras			A single PTZ camera is in place at the CS reservoir
Type of Cameras			
Color Black & White			Color
Camera Coverage			
PTZ Stationary			PTZ
MONITORS			
Number of Monitors			Monitors by a private service during the day, police at night
Type of Monitors			
Color Black & White			
Single Screen Quad Screen			
Continuous Time Delay			
Quality of Coverage – Daylight			poor
Quality of Coverage – Night			Extremely poor
RECORD CAPABILITY			
Type of Recording			
Analog Digital			N/A
Real Time Delayed			
Motion Continuous			
Color Black & White			
Tape Changes			
Hourly Daily Weekly			N/A
Tape Storage / Rotation			
Daily Weekly Monthly			N/A
Tape Accountability			
Guards Security Mgr Other: ___			N/A

NARRATIVE SUMMARY – Section D Video Surveillance System

The video surveillance is so poorly situated for protection of critical assets that it is unlikely to aid in detection or assessment. The single camera is more likely to be used at night to apprehend drug deales.

(E) Information Security

	Yes	No	Comments
Locations of Fax Machines and Printers – secured?			
SCADA Network Access – modems connected to LAN workstations			Not at this time but planned for future
Computer file storage			No storage kept
Laptop Security – locks			
Library file storage – secured room/cabinets			
Lab Notebook storage – secured?			
Mail distribution and control – secured?			

NARRATIVE SUMMARY – Section E Information Security

Information security at the plant is accomplished by connecting on-line only when the SCADA contractor calls and requests that the telephone line be switched on. The Contractor uswes a password to take control of the system for diagnostic work and downloads. No confidential material is kept on plant PC's.

(F) SCADA Control System

Feature	Yes	No	Comments
COMMUNICATIONS			By modem
Link to an external off-site system			By modem
Encryption			
Lock and sensor communications rooms			
Supervised lines			
Authentication			
Redundant systems			
COMMERCIAL HARDWARE AND SOFTWARE			
Current security patches			
Strong password			
Audits			
Monitor unusual use			
APPLICATION SOFTWARE			
Configuration control			
Trusted source			
Documentation			

	Yes	No	
Thorough testing			
PARAMETER DATA			
Validate value and effect			
Configuration control			
Read only			
Authenticate write privilege			
SUPPORT INFRASTRUCTURE			
UPS			
Automatic switch to backup			
Environmental controls			
SECURITY INTRUSION DETECTION			
PFP buildings			
CS buildings			
Monitoring and Response capability			

NARRATIVE SUMMARY – Section F SCADA Control System – Security Intrusion Detection

Security is controlled by disconnecting telephone line to system

(G) Other			
	Yes	No	Comments
PROCESS SAFETY FEATURES			
Fail-Safe valves			
Sensors and Indicators			
Limit switches			
Relief or check valves			
Manual or Automatic Shutoffs			
Alarms and procedures			
Emergency Air Supply			
Emergency Power			Diesel back-up for pump power.
Rupture Disks			
Flow-limiting Equipment			
Inhibitor addition			
Process Area monitors			
Perimeter monitors			
MITIGATION FEATURES (ACTIVE, PASSIVE)			
OTHER AREAS TO CONSIDER			

NARRATIVE SUMMARY – Section G Other