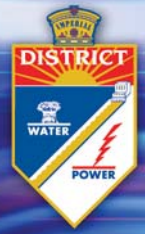


Currents

Imperial Irrigation District

Protecting the flow of progress.



News for district employees

August 28, 2009

Sign up for energy's new SwingShift program

■ Tool will allow district to better prepare for emergencies


IID has a new tool to manage electric use during periods of peak energy demand. Dubbed "Energy SwingShift," the program allows IID to manage usage and lower overall demand on the system in time of need.

Energy SwingShift



"By cycling air conditioners and shutting off pool pumps and electric water heaters, IID can make a significant reduction in the amount of load we need," said program manager Darrin Marquez. "In an emergency situation, this will help us keep the system stable and avoid the need for emergency load shedding procedures."

Demand response programs are used by utilities nationwide to reduce energy demand. In addition to boosting system reliability, reducing peak usage also helps lower IID's operating costs by eliminating the need to purchase costly energy on the spot market.



Strategic Plan Objective
Develop an integrated energy resource plan

Demand response programs can be structured in many ways. IID customers will be paid an incentive of \$5 for air conditioners, \$3 for pool pumps or \$2 for electric water heaters each time the utility cycles back their systems.

Depending upon the customer's choice of technology options, some participants will receive a free programmable thermostat.

"Contrary to what you might think, participating in a demand response program does not mean sacrificing comfort," Marquez added. "For instance, air conditioning units are not turned off; instead, they are cycled for brief periods. The net effect of several small-cycling events creates a substantial reduction in overall electrical demand."

Some restrictions apply. Presently, the program is available to single family residences or small businesses.

Employees are encouraged to participate, too.

Anyone wishing to sign up may call (866) 540-4319 to enroll and schedule an installation appointment.



Strategic update

This week (Aug. 24-28) General Manager Brian Brady conducted brown bag meetings with employees at Valley Plaza, the steam plant and La Quinta.

One meeting remains scheduled: 12-1 p.m. Tuesday, Sept. 1 at River Division.

Following the employee brown bag meetings, Brady will hold similar meetings with middle management.

Budget coordinator Diana Rosas, who is engineering the brown bag meetings for the general manager, said a number of issues have already been resolved and others are being looked into.

The next update on the district's strategic plan will be conducted during a special workshop, which is open to the public, and scheduled for the Sept. 29, from 3-5 p.m. in the Condit Auditorium, El Centro.

It's CIPS for physical and cyber protection

Since this spring, critical infrastructure protection standards awareness training has been conducted throughout the district to educate staff regarding North American Electric Reliability Corporation standards and security measures necessary to

See **SECURITY**, back page

Electricity Sector Threat Advisory Levels

Physical

Cyber

ELEVATED



Significant Risk of Terrorist Attacks

ELEVATED



Significant Risk of Terrorist Attacks

SECURITY (continued from front page)

protect physical and cyber assets. In accordance with these standards, entities are required to continue to provide sound security practices and reinforce security awareness on a quarterly basis.

The current threat level for the energy sector remains elevated for both physical and cyber assets.

The recommended security measures at this threat level are in addition to those required for the green (low) and blue (guarded) threat levels listed below:

Green (low) physical security measures:

1. Ensure normal security operating standards and procedures are in place and operational.
2. Train security staff and key personnel on all aspects of the response plan and specific pre-planned operating standards and procedures.
3. All visitors should be approved before being allowed to enter a critical facility or access a critical system.
4. Stop individuals not known or otherwise approved to determine indentify and reason for presence and take appropriate action, such as issuing a badge or removing the individual from property.
5. Conduct routine maintenance and inspection of electronic security equipment to ensure good working order at all times.
6. Periodically post or issue workforce awareness messages and conduct tabletop exercises as appropriate.
7. Review and update all security, threat, and disaster-recovery plans at least annually.
8. Report any unusual or suspicious activity observed by critical facility personnel or contractor to security or facility management staff.
9. Address security topics at employee meetings to increase security awareness.
10. Annually audit electronic or other access programs for critical facilities to ensure proper access authorization.
11. Ensure proper training of hazardous materials, security and emergency response personnel.
12. Identify critical facility long-term and short-term security measures as appropriate: electronic security systems, close nonessential perimeter/internal portals, physical barriers, fencing, lighting, security surveys, vulnerability assess-

ments, availability of security resources (contract/proprietary); law enforcement liaison, availability of essential spare parts of critical facilities.

Blue (guarded) physical security measures:

13. Communicate heightened security threat level to all personnel and contractors at critical facilities and non-critical facility personnel.
14. Monitor all deliveries, particularly deliveries of combustible materials such as start-up fuel, diesel and gasoline.
15. Review operational plans and procedures to ensure they are up to date.

16. Provide local law enforcement agencies any information that would support the ability to provide assistance.

17. Monitor conditions and be prepared to escalate to higher level or de-escalate to a lower threat level.

Yellow (elevated) physical security measure:

18. Increase the surveillance of critical facilities
19. Ensure all gates, security doors and security monitors are in working order and that visitor, contractor, and employee access controls are enforced.
20. Notify critical and on-call personnel of the elevated threat level.
21. Establish and assure ongoing internal and external communications and coordinate the organization's action plan with local, state/provincial, and federal law enforcement agencies.
22. Review operational plans and procedures and ensure they adequately address the terrorist threat associated with reason for the elevated threat level.
23. Indentify additional business and site-specific measures as appropriate.
24. Monitor conditions and be prepared to escalate to a higher level or de-escalate to a lower threat level.

In June, the district indentified the systems operation center and distribution operation center as critical assets. As such, the above security measures will continue to be enforced to ensure compliance with CIP standards and current threat level security procedures.

For more information about IID's physical security plan, please contact the Security Claims and Investigations section at Ext. 7413 or the internal NERC CIP standards reliability compliance office at Ext. 3354.

