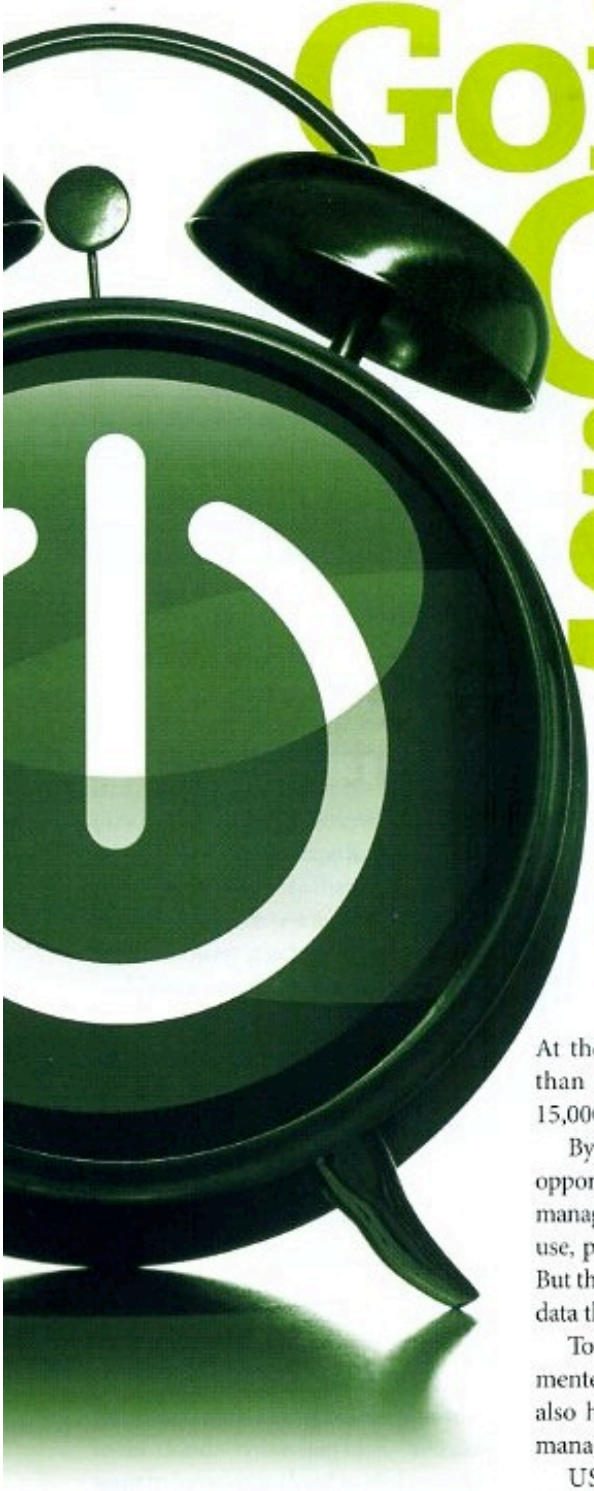

Going Green, Staying Secure

Striking a balance between smart energy conservation and critical information assurance proves a challenging but attainable goal.

By Logan Kugler

At the Agriculture Department, more than 100,000 employees work from 15,000 locations worldwide.

By sheer volume alone, USDA has the opportunity to reduce costs by improving management of its desktop systems' power use, points out CIO Christopher Smith. But the department also must protect the data that trickles down to those systems.

To aid in this process, "we have implemented an endpoint security tool that also has the capability to monitor and manage the power settings," Smith says.

USDA, like other agencies, has found that to be both green and secure demands tweaking IT power and security strategies in tandem.

"We have a very federated model in agriculture," Smith says. "We have a lot of business lines and CIOs running their own local area networks and connecting into our wide area network. One of the first things we want to ensure as we strive to reduce our carbon footprint is that we're not reducing our security posture in any way."

With the administration mandating reductions in energy consumption and greenhouse gases, IT organizations across the government are focused on how their systems consume power. Given their extensive deployment, end-user devices are obvious targets, and, say Smith and others, meshing power monitoring with security best practices requires setting well-conceived configuration policies for both.

More Facts, Fewer Myths

At the Energy Department, the growth of good power management practices has dispelled some myths when it comes to managing device security, says DOE spokeswoman Katinka Podmaniczky.

"A common concern was that power management would not allow IT personnel to install patches or improvements during evenings and weekends," she says.

But wake-on-LAN functionality now allows IT staff to make needed security changes and still achieve energy savings.

CLOCK: MIKE KEMP/GETTY IMAGES

"Implementation of more sophisticated network software programs makes compliance easy since individuals can no longer override power settings," Podmaniczky adds.

At DOE, the "cybersecurity staff became very supportive of power management programs once they understood how their access is preserved," she says. "Power management can actually aid cybersecurity — a safer computer is one that is turned off rather than one running unattended at night and on weekends."

Barbara Kuehn, overseas operations manager for global IT at the State Department, says State posts abroad have implemented desktop power management solutions by working closely with the department's IT security teams to ensure proper arrangements for patching and scanning desktop systems at appropriate off-peak times.

"During the wake-up windows, patching and scanning can occur and, once complete, the desktops can be shut back down," she says. "This allows security to remain in place in a timely fashion as well as avoiding interruption of business operations."

A critical first step for aligning configuration settings for security and power monitoring hinges on obtaining an accurate picture of how much energy an organization currently uses.

In addition to energy usage data, organizations also need to look at operational data such as staffing schedules, processing schedules and weather data, suggests Rhonda Stratton, a project manager at Johnston McLamb systems consultants.

"When you combine these, you can see what's impacting your energy usage," Stratton says. Does the agency have shifts running at peak use times, which can drive up utility expenses? Can the agency adjust shifts? Can it take advantage of opportunities available through the use of virtualization and thin clients? These are all questions to explore, Stratton says.

Beyond the Desktop

When it comes to power management, security can be a factor for systems other than end-user devices.

For large organizations, processing and computing are often handled in distributed environments, which can lead to costly power bills, says Mark Rasch, director of cybersecurity and privacy for CSC.

"What you can do is take all of the energy-intensive processes — the processing, the storage, and the transmission of data and information — and you can locate them in a server farm," Rasch says. "Then you locate that server farm in a place close to cheap or renewable energy, someplace close to a hydro plant, a solar plant or a new coal plant."

But, Rasch adds, security issues can arise based on the location of the inexpensive energy. "Let's say that the lowest cost is in North Korea or China or Libya. You don't want your critical data to be stored and processed in countries that have hostile regimes or that are hostile to your interests."

State understands this dilemma well. In selecting a site for its overseas data center, State was constrained to locations approved in the Defense Department's Base Realignment and Closure plans, Kuehn says.

Based on expected growth, State determined it would need at least 12 megawatts of power over the next 20 years. Another consideration was a location that would allow for ambient cooling, and a final consideration was the cost of the land.

"Our chosen location did not have a hydro or wind option; however, it is standard practice for the department to purchase clean energy as a percentage of the total required energy," Kuehn says. "So, while we will not be generating power through green mechanisms, we will be cooperating with the local power company to purchase a certain amount of power generated using wind, solar, etc."

50%
The percentage of total PC power consumption saved with a well-managed power program for 25,000 PCs

SOURCE: USDA Green IT Strategic Plan

Consolidated Approach

Ultimately, says USDA's Smith, agencies must spend more time thinking about interdependencies across systems and across agency lines of business. When it comes to power management, "the greatest return on the highest sustainable practices, whether commercial or government, is really going to become that synergy across multiple areas — facilities, IT, security, fleet. To me, that is the Holy Grail as we move forward." FT

JEFFREY COOLIDGE/GETTY IMAGES

More Ways IT Can Help Dial Down Power Use

To achieve efficiencies, the State Department's Barbara Kuehn recommends that IT and facilities managers place emphasis on the following areas:

- **Construction:** When designing new buildings and retrofitting existing structures, be sure to include modern, energy-efficient subsystems.
- **Monitoring:** As new facilities are built, include extensive utility and consumables monitoring systems that can support automatic reporting.
- **Printer Management:** Although not a new concept, switch from local printers to networked printers and default to duplex printing.
- **Video Conferencing:** Whenever possible, forgo live meetings and conduct them instead via video conference.
- **Organizational Culture:** Develop an extensive communications plan that details how end users can improve their personal energy footprint. The objective is to change the attitudes and practices of individual federal workers in regard to the consumption of energy and resources at work — and at home.