Four Ways that the Cloud Benefits Federal Energy Management

by Brandy Moore and Ellen Kotzbauer

Executive summary

Federal agencies have been challenged to adopt a “cloud-first” strategy for computerized applications, including those that run facilities energy management. However, many are reluctant to embrace the cloud due to issues surrounding cybersecurity, loss of control, and staff expense increases. This paper explores why moving energy management to the cloud is a safe, smart move that reduces cost and improves resiliency, efficiency, flexibility, and accessibility.

998-2095-02-06-15AR0

Schneider Electric

Introduction

Federal agencies are under pressure to cut costs and increase resiliency. In order to achieve these goals, special emphasis has been placed on energy management and migration of IT solutions to the cloud. An array of executive orders, congressional acts, strategies, and guidelines (see **Table 1**) are key drivers behind these particular initiatives. An array of executive orders, congressional acts, strategies, and guidelines (see **Table 1**) are key drivers behind these initiatives. The Energy Independence and Security Act of 2007, for instance, called for a 30% reduction of energy usage by 2015. Executive Order 13514 from 2009 mandates a reduction of 28% in Scope 1 greenhouse gas emissions by 2020. Specific to the "cloud" are the 25 Point Implementation Plan to Reform Federal Information Technology Management (2010) and the Federal Cloud Computing Strategy (2011), both of which mandate that agencies begin to implement a "cloud-first" policy.

One way federal facility managers can accommodate their energy management initiatives and help their IT colleagues achieve the cloud-first strategy is to leverage new cloud-based building monitoring, analytics and control solutions. These systems have been traditionally hosted on site, or "on premise." Despite the distinct advantages over the traditional approach, some agencies have resisted moving to cloud-based facility energy management solutions, largely due to security and IT infrastructure management concerns.

In fact, cloud computing provides an environment that is *more* secure by centralizing data storage and governance, often at a lower cost than traditional computing environments. If the correct cloud model is deployed, systems service delivery speeds can be increased and additional cost savings can be realized. (See **Appendix A** for definitions of the various cloud types). This paper will review four benefits of cloud-based solutions and offer recommendations for how agencies can prepare for a cost-effective migration from traditional, on-premise energy management systems to the cloud.

Table 1
Partial list of federal government mandates surrounding energy management and information technology (with live links)

Energy Management Initiatives	Information Technology Initiatives
Energy Independence and Security Act of 2007	Federal Information Security Management Act of 2002 (FISMA)
Energy Policy Act of 1992	Federal Cloud Computing Strategy (FCCS) 2011
Executive Order 13221: Energy Efficient Standby Power Devices (2001)	25 Point Implementation Plan to Reform Federal Information Technology Management (which includes the Cloud First Strategy) 2010
Energy Policy Act of 2005	Federal Data Center Consolidation Initiative (FDCCI) 2010
Energy Independence and Security Act of 2007	Federal Risk and Authorization Management Program (FedRAMP)
Executive Order 13423: Strengthening Federal Environmental, Energy, and Transportation Management (2007)	National Institutes for Standards and Technology
Executive Order 13514: Federal Leadership in Environmental, Energy, and Economic Performance (2009)	
2013 Presidential Memorandum (Green Button)	

Potential savings

While there has been a major push to consolidate building footprints, the U.S. federal government is still one of the largest owners and lessees of property in the country. According to the 2013 Federal Real Property Report (FRPR), published by the U.S. General

Services Administration (GSA), federal government agencies owned, leased, and otherwise managed over 350,000 diverse buildings at the time of the report. This real estate totaled more than 3.3 billion gross square feet and cost nearly $25 billion annually to operate.[1]

In its "Clean Energy Lead by Example Guide,"[2] the U.S. Environmental Protection Agency (EPA) says that energy represents 30% of the variable costs in a typical office building and constitutes the largest controllable operating cost. The guide also indicates that the lifetime energy cost savings produced by an energy-efficient building could be in the millions, with upward of 35% or more in savings possible in many existing buildings.

According to the Federal Energy Management Program (FEMP), the U.S. government's energy costs for all real estate holdings in 2013 exceeded $7 billion. If the cost-savings metric of 35% is applied, the government could have saved over $2 billion as a result of energy efficiency improvements on its holdings. These numbers do not take into account the reductions in greenhouse gas emissions that would result from lowering energy consumption.

In addition, the January 2014 GAO Report 14-188 asserts that federal facilities are sustaining maintenance and repair backlogs totaling billions of dollars (see **Table 2**). Left unchecked, this results in more expensive repairs, higher operating costs, and diminished performance of the facilities.[3]

Table 2
Selected agencies deferred maintenance and repair backlog estimates

Agency	Financial report estimates (in billions of dollars)	Federal real property profile (FRPP) estimates (in billions of dollars)
GSA	$1.5	$4.7
DOE	$4.7	$5.1
DHS	$0.8 – 0.9	$.9
Interior	$13.8 – 20.2	$14.4
VA	$6.7	$12.5

To achieve energy goals, build a robust framework

To attain the goals of decreasing energy usage and reducing GHG emissions, a government facility – whether it's relatively new or in need of repairs – must implement smarter operations. Energy management solutions that provide monitoring, control and analytics are needed. This allows facilities staff to drive measurable, sustainable savings, to reduce operating and maintenance costs, and to increase resiliency. Such a solution also enables greater adaptability to changes in space utilization and energy needs, which is key as federal agencies consolidate their real estate holdings.

Some federal agencies are already using basic tools to monitor and control their facilities. These tools are not enough, because they do not tap into the analytical, historical, and real-time data that drive improved building energy performance. With modern analytics tools, a more holistic visibility to facility operations is now possible, which better enables facilities personnel to achieve their energy and sustainability goals.

[1] U.S General Services Administration, FY 2013 FRPP Summary Data Set

[2] http://www.epa.gov/statelocalclimate/documents/pdf/epa_lbe_chapter2.pdf

[3] http://www.gao.gov/assets/670/661063.txt

Benefits of the cloud

When choosing energy monitoring, control, and analytics solutions, facilities managers have many options, including cloud-based versus a traditional on-premise solution. With IT managers under the same pressure to undertake cloud computing initiatives as their fellow facilities managers are in regard to managing energy, a cloud-based solution is an important consideration. A cloud-based energy management solution can extend the benefits of an on-premise solution and help cut costs, drive greater resiliency, security, and efficiencies, while also supporting agencies in their first cloud efforts.

Benefit #1: Added security

A top concern of both IT and facility managers is whether or not the cloud environment is secure enough for their applications. A recent Market Connections study states that nearly two-thirds (64%) of federal government IT decision makers and influencers indicated that a secure infrastructure is a top *benefit* of cloud computing. Yet in the same study, 69% of these respondents indicated the cloud is a top perceived risk because of concerns about data leaks, unauthorized data access, and security defects.[4]

"Cloud-based solutions offer higher security and more robust IT infrastructure management than most on-premise solutions."

In fact, cloud-based solutions offer higher security and more robust IT infrastructure management than most on-premise solutions. In its FY2013 Annual Report to Congress: Federal Information Security Management Act (FISMA), the Office of Management and Budget reported that agencies have improved their security posture since FY2012, but weaknesses still exist in such areas as access management, information security continuous monitoring, vulnerability remediation, configuration control, and patch management.[5]

Cloud service providers are keenly focused on these and other security issues, as they are fundamental to their business. Such providers construct robust infrastructures with greater redundancy than many federal data centers, delivering greater availability and reliability. Cloud offerings include advanced security measures with firewall, authentication and authorization, data transmission, and data storage services. Oftentimes these cloud-based solutions include independent third-party security audits at regular intervals and are certified to national and international security standards. When vulnerabilities are discovered, security patches are quickly developed and automatically deployed to all systems.

Cloud service providers also ensure that their offerings meet federal security requirements. For instance, energy management solutions can be run on FedRAMP-certified public clouds, which offer the highest degree of security and privacy through multilevel data security at the application, infrastructure, and data center layers.

Companies like Microsoft and Amazon are creating special government clouds that are FedRAMP-authorized. Microsoft is offering Azure Government, a cloud platform that meets the government's requirements for security. The offer also addresses compliance by providing physical and network isolation from non-U.S. government deployments and specialized personnel screening. Amazon offers the AWS GovCloud (U.S.) with similar security and functionality.

Benefit #2: Advanced technology

Cloud-based solution providers offer newer, more sophisticated technologies and services than what exists within traditional on-premise implementations. A cloud-based energy management solution, for example, offers the following unique technology benefits:

[4] Market Connections and General Dynamics Information Technology, "Cost Reduction Drives Agency Interest in Cloud-Based Services", October, 2014

[5] Office of Management and Budget, "Annual Report to Congress: Federal Information Security Management Act", May 1, 2014.

- Instant access to updates and innovations that keep systems current and on the forefront of technology
- Easier-to-use interfaces that allow universal access, any time, any place and encourage a high rate of user adoption
- Real-time collaboration for individuals across multiple functions, facilities, and regions through easy access to documents and intelligence that is stored in a central, virtual location
- Faster deployments, with implementations taking half the time than what is typical of traditional systems
- Centralized management and reduced maintenance

Benefit #3: Superior data management

Agencies recognize that data management is a key enabler of smart building management. The amount of building energy data generated is massive and will only increase – especially where multiple buildings with thousands of data points are being managed and stored on frequent intervals through a single solution.

The amount of data requires resources and computing power beyond on-premise data management capabilities. Cloud-based solutions, however, have the power and intelligence for rapid analysis of massive amounts of building data – analytical, historical, and real-time. This data helps facility and IT managers make smarter, better-informed energy management decisions, especially when systems are at risk.

Any necessary disaster recovery measures, as well as system backups and restoration processes, are more efficient, because data is instantaneously and automatically replicated. System recoveries are quicker and easier than what is available through on-premise solutions.

Benefit #4: Cost and operational savings

Cloud-based solutions offer a lower total cost of ownership (TCO), as they require a smaller capital investment and drive a shorter payback period. In fact, in the Market Connections study cited previously, 53% of the respondents indicated that decreasing IT operating and infrastructure cost was a top driver of cloud adoption. Also, 59% indicated that a migration to cloud-based services can result in lower capital expenses compared to in-house infrastructure deployments.[6]

"Cloud applications offer a lower TCO than on-premise solutions, because cloud applications are designed to anticipate and address common issues."

In addition, cloud applications offer a lower TCO than on-premise solutions, because cloud applications are designed to anticipate and address common issues. Software patterns such as the node failure, busy signal, and queue-centric workflows represent problems that have already been diagnosed and enable the operation of a more robust environment. Cloud environments are easier to scale. In many cases the lower hardware costs of cloud providers are passed on to customers as lower operating costs so that the cloud offerings can be more competitive. Upgrades to the hardware are performed by the cloud provider on a large scale, providing additional savings.

The cloud-based energy management system model, since it is scalable, enables a federal agency to manage multiple buildings in its real estate portfolio through a single integrated building management system, without having to increase its own data center footprint. A typical federal data center footprint is 50 -100X the energy intensity of an office building. Cloud data centers offer the benefit of a cost-effective, higher data processing density, thereby increasing energy efficiency and decreasing carbon emissions.

[6] Ibid.

Subscription-based software-as-a-service (SaaS) solutions also offer agencies the option to leverage their investment as an operating expense, so they can preserve their capital expense budgets for other projects. Services can be purchased on an as-needed basis, providing further flexibility to cost-constrained departments.

Agencies also fear that moving applications over to the cloud will result in additional internal staff requirements. In fact, more than 68% of federal executives believe they do not have the necessary skills to implement a cloud strategy[7] and 30% think they would need to hire up to 20 new employees for cloud deployments.[8]

The reality is energy management and cloud vendors provide cost-effective expert services that can act as an adjunct to facility and IT staffs. This safeguards internal resources and supplements the agency's cloud and energy management expertise knowledge base.

Energy management in the cloud

In the domain of energy management, several types of cloud implementations are available. The following are summaries of some of the more popular applications.

Automated fault detection and diagnostics. These solutions help provide predictive analytics, ROI-based prioritization of repair and maintenance needs, and accurate reporting of building mechanical systems costs and benefits. Energy savings in the range of 2-30% (with a median of 9%) can be expected when issue resoution actions are promptly pursued.[9] Such tools enhance building performance, reduce operating costs, improve occupant comfort, and optimize energy efficiency through continuous monitoring-based commissioning (MBCx). Automated fault detection and diagnostics (aFDD) and real-time performance monitoring capture building systems information and forward it to secure cloud-based data storage. Advanced analytics engines process building data to diagnose facility performance and identify equipment and system faults, sequence of operation improvements, system trends, and energy usage.

Energy information systems (EIS) and energy data management. These SaaS tools provide energy consumption information to help federal agencies optimize energy use and reduce operating expenses. They enable visibility into energy and resource use across a federal agency. Access to accurate and actionable data is provided to help conserve resources, optimize business performance, and manage an effective sustainability strategy.

A good example of how the cloud is being leveraged for EIS in federal facilities is the Green Button initiative. This service brings ConnectMyData (a recent standard utilized by commercial and industrial customers to access building energy data from utilities) access and connectivity to federal buildings. Sub-metering data from participating buildings is provided to energy management systems. This allows facility managers to monitor usage, track demand and emissions, and gain a better understanding of how their buildings use energy.

The federal program is part of a broader Green Button initiative that was launched in January 2012. To date, a total of 35 utilities and electricity suppliers have signed on to the initiative. These commitments ensure that 36 million homes and businesses will be able to securely access their own energy information in a standard format. This number will continue to grow as utilities in the U.S. voluntarily make energy data more available to their customers in this common, machine-readable format.

[7] http://www.ecommercetimes.com/story/80000.html#sthash.CamFQBit.dpuf

[8] http://www.businesscloudnews.com/2014/02/10/three-years-after-us-cloud-first-mandate-federal-agencies-struggle-with-implementation/

[9] http://evanmills.lbl.gov/pubs/pdf/mbcx-lbnl.pdf

Building environmental controls. Some solutions use web and wireless technology to control HVAC, lighting, and metering. This saves time and energy, and improves human comfort with minimal impact on operations. By providing anytime, anywhere access to building information on a simple user interface, energy costs can be reduced without compromising comfort. These solutions include the ability to centralize monitoring and technician dispatch, as well as the ability to share data across facilities to better track performance and improve operations. Wireless building management solutions can be utilized to increase efficiency in older structures, where the costs of replacing "in the wall" wiring solutions would be too high.

Sustainability management systems. These solutions provide online sustainability and energy management tools for secure access to energy and environmental data, reports, and summaries. They track and manage utility costs and carbon emissions throughout federal facilities, including data centers.

Building a support team

While porting energy management applications to the cloud might seem like an arduous task, a step-by-step process exists that can help. The following recommendations can help expedite the process:

- **Build a team of stakeholders.** Make a list of influencers, decision-makers, and system users from both building facilities and IT. Invite them to participate when the appropriate aspect of the process requires their expertise and support.
- **Define the solution's requirements.** Each agency will have its own unique building facility and cloud requirements. Delineate the objectives, priorities, and other pertinent criteria for a cloud-based energy management system appropriate to the agency's needs.
- **Assess the risks.** For energy management and the cloud, what risks and challenges are of concern? Certainly, security and privacy are top of the list on the cloud side, as well as the required personnel to support such a solution. Develop a comprehensive list by engaging stakeholders in the organization and collaborating with vendors to ensure concerns are addressed.
- **Determine the cloud model that works best.** Some agencies make implementation of a private cloud mandatory. Depending on the resources available, there may be particular service models that work best (see **Appendix A**).
- **Delineate high-priority energy management tactics.** Ascertain which method is more advantageous to the department: adopting various individual modules or deploying a full comprehensive solution. Determine which areas can provide the most return on investment (refer to the previous section that reviews the cloud-based energy management solutions).
- **Create a request for proposal.** For both energy management and the cloud, identify the agency's specific requirements, as well as government mandates, such as FedRAMP. Create a short list and develop a request for proposal.
- **Choose the best solution.** In reviewing requests for proposals, it will become evident which solution providers can best meet the requirements for both energy management and cloud technology.

Use cases

As acknowledged earlier, the federal government is already taking steps to implement intelligent energy management solutions. Here are a few examples:

- The U.S. General Services Administration, as part of their National Deep Energy Retrofit program, installed energy efficiency improvements and renewable energy systems at the Almeric Christian Federal Building in St. Croix, U.S. Virgin Islands. This initiative is making this facility one of the first federal buildings to achieve 100% net

zero energy through an Energy Savings Performance Contract (ESPC). This project guarantees a total of $13 million in energy savings, with savings in the first year of more than $500,000.

- Four U.S. Coast Guard sites in Puerto Rico underwent a $50 million green renovation. The buildings' new systems are redirecting $1 million of annual energy spending from brown power to PV-generated green power. In addition, the systems produce more than five million kilowatt-hours and $1.1 million in annual savings.
- The U.S. Navy is implementing an advanced metering infrastructure (AMI) program to improve energy efficiency by achieving a greater return on utilities management, energy management, and energy security. By integrating its worldwide facilities, the Navy will gain insight into 95% of its electric consumption and 75% of its mechanical consumption (water, natural gas, and steam) to help meet the requirements of cutting its annual $1 billion utility bill by 30% by 2015. In addition, the Navy hopes to leverage AMI to also help achieve its net zero energy goals.
- The VA National Energy Business Center monitors more than 800 buildings and 20 renewable energy systems. It is leveraging Schneider Electric ION advanced meters and the Enterprise Energy Management (EEM) system, an energy information and demand response management system, to monitor and manage facility electricity usage for the center's $500 million annual utility bill. The solution verifies electricity usage and utility billing and identifies potential infrastructure upgrades and opportunities to reduce energy usage.
- GSA Green Button pilot was launched in May 2014 as part of the first deployment of ConnectMyData for commercial users by Pepco. The program utilizes a cloud-based energy management information and demand response management system to provide easy access to energy data for GSA and third-party solutions providers who work with GSA. Integrated with existing advanced metering infrastructures and ION EEM, the solution provides a utility interface for the ConnectMyData service.

Conclusion

Cloud- based services provide an alternative to on-premise solutions and have the advantages of being more efficient, scalable and agile. For energy management solutions, a cloud infrastructure provides the capacity to manage much larger volumes of data without sacrificing security.

Federal agencies need to meet energy and sustainability goals and lower facilities operations costs while adhering to IT efficiency strategies. Moving to the cloud offers a better way to manage energy and operational assets in a manner that is life-cycle cost-effective.

About the authors

Brandy Moore, **CEM, PMP**, is Offer Management Director for Schneider Electric's Global Field Services for Buildings. She is responsible for industry-leading global services strategies, remote technology-driven and traditional service offer development, and worldwide service product launches. She has worked with customers around the globe to introduce and implement cloud-based technologies to improve facility performance and efficiency since 2011. An industry expert, writer, and blogger on high-performance green buildings, energy solutions, and infrastructure solutions, she has held several positions at Schneider Electric, including director of Global Education Solutions prior to joining the services team. A Certified Energy Manager and Project Management Professional, she holds a Bachelor of Science degree in industrial distribution from Texas A&M University.

Ellen Kotzbauer, BEP, is a 24-year veteran of Schneider Electric and has held numerous engineering, manufacturing, and marketing positions in the company. She has worked closely with U.S. federal government customers for the past 10 years and is currently a program manager for U.S. Army Corps of Engineers programs. She has co-authored four white papers and is an active member of several industry associations, including SAME, EFCOG, and AEE. She holds a B.S. in industrial engineering from Northwestern University and is a certified Business Energy Professional (BEP).

Acknowledgment: A special thanks to Nick Gayeski, CEO and co-founder of KGS Buildings, a leading building performance management company focused on advanced analytics for intelligent buildings. KGS is a Schneider Electric Ecostruxure Technology Partner, a Microsoft Partner, and an early adopter of the Azure cloud platform in 2010. Nick holds a master's degree and a Ph.D. from the Massachusetts Institute of Technology.

Appendix A

Definitions of "cloud" types (as described in the NIST's Federal Cloud Computing Strategy)[10]
Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (such as mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public). These remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (such as cloud bursting for load-balancing between clouds).
Cloud computing can also categorized into service models. These are defined by NIST to be:
Cloud Software as a Service (SaaS). The model uses the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (for example, web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Cloud Platform as a Service (PaaS). The capability provided to the consumer is the ability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (such as host firewalls).

[10] http://www.cloudbuyersguide.org/the-guide/