

## ■ THE GRILL

## James Allen

The FEC's 'nerdy data guy' talks about maintaining **security**, the flow of **campaign finance** information and **the public trust**.



PHOTOS: DAREN HIGGINS

**T**HE Federal Election Commission (FEC) is charged with tracking, reporting on and investigating anything to do with presidential and congressional campaign finance. A big and relatively new part of its charter is to provide campaign finance data to citizens via its Web site.

James Allen, who manages IT infrastructure for the organization, discussed what it takes to keep up with the ins and outs of campaign finance. As he says, "I'm the nerdy data guy, not a politician."

**You've got a data center at the FEC in Washington, and you contract with an external vendor to run servers for you out of Waltham, Mass., and Herndon, Va. How do all these pieces work together?** Here at the commission, we have a small data center — roughly 90 servers, a mixture of Unix and Windows. Our Unix systems handle

Oracle databases; the Windows servers handle file shares, SQL databases, the Lotus Notes e-mail backbone and various support functions for the commission. I have a staff of four people to make sure all our internal servers are operational, have the proper storage and that patching is maintained. Another group of people deals with desktop issues.

Our vendor, Savvis, hosts servers for us in Waltham that handle the public-facing aspects of what we do — the data we provide the public. So they maintain our Web servers, database servers and application servers. They have round-the-clock staffing, which we do not have here, and they provide patching and keep the servers operational. They manage our network down to the core switch here at the FEC, and we have biweekly technical meetings to go over any issues.

In Herndon, there is a separate set

## Dossier

**Name:** James Allen

**Title:** Infrastructure branch manager, IT division

**Organization:** Federal Election Commission

**Location:** Washington

**Favorite nonwork pastimes:** Kayaking, hiking and reading

**Philosophy in a nutshell:** "Always do your best. Don't give up."

**Four people he'd like to invite to dinner:** Albert Einstein, Werner Heisenberg, Mahatma Gandhi and Stephen Hawking

**Favorite vice:** "An occasional glass of wine."

**Great read:** *Cryptonomicon*, by Neal Stephenson



**“Thirty years ago, I could manage all the hardware myself. It’s gone from a one-man operation to a three-ring circus.”**

of servers that acts as our back-end database. These take information from the various House and Senate committees that report on campaign finance. The public doesn’t see this data as it appears here; this is the “raw” information that our analysts take and look into. We have a T1 line to the Senate so they can file their reports securely and quickly.

After the data has been cleared by our analysts — and we have a 48-hour turnaround time — we post it on the public Web site.

**Do you consider your hosted services to be cloud computing?** No, because we have specific servers that run our site, and we own those servers. Savvis just manages them for us. It’s cloud computing only if I can connect and use a service with no regard to where that service may be emanating from. Savvis has talked to us about cloud computing, and that is very interesting to me. I can see it from a disaster recovery perspective. If I can contractually request services, and I get those services as specified in the contract in a secure manner, then that’s fabulous.

But the FEC doesn’t allow anything other than FEC operations on our systems. So I might have to look at a private cloud-computing model with

only the FEC on it. That might be prohibitively expensive, though.

**Tell us more about your Web portal. Who developed it? Who maintains it?** The Web site has been around for many years. It came into being almost as soon as the Web was available, sometime in the mid- to late 1990s. The Web site has gone from a pretty standard noninteractive site to a much more robust site. A lot of that is due to Alec Palmer, our current CIO. He’s very Web-savvy, and he’s interested in putting as much data out to the public as he can. And he wants to put the data out there in more interesting ways than we have hitherto done.

Before, there were flat files, and it was harder to dig for that summary information you may have wanted. Alec’s the one who pushed for the map application — those beautiful bubbles on our home page. He’s assembled a tremendous staff of very talented programmers and enterprise architects and others. Savvis is hosting the Web site; they give us a secure environment to work that magic. But all the programming is done from the FEC.

**How have IT operations changed in the 30 years you’ve been at the FEC?** It’s become much more complex, and at the same time we’ve really reached out to provide more and different kinds of data to the public. Years ago, if you wanted to get information, you had to come to our office here in Washington to do research. Over the years, we developed a process so people could dial in over a modem and view reports; this was pre-Internet. Now it’s all done via the Web, and we’ve vastly expanded the ability for citizens to do queries about who’s getting what money and from where. You can really drill down into the details about which PACs or corporations are giving money to candidates, to see what the candidate really believes in.

This has required us to move from a

single-tier database into a multitiered system. But the graphics are definitely much better than they were. And 30 years ago, I could manage all the hardware myself. It’s gone from a one-man operation to a three-ring circus — with a lot more knowledge and skills required.

When I first started at the FEC, the security implications were nowhere near what they are now. You just didn’t hear of anyone hacking into databases back then — it was a rare occurrence. Now we have to run virus protection software, configuration management software, firewalls and router rules, and intrusion detection/prevention. All of these are necessary to protect and ensure that all of the information we pump out there is accurate and not being defaced or changed by some miscreant.

**What is Savvis’ role in security, and what is the internal role?** Savvis monitors our network very closely. They run [intrusion detection] across the network and let us know if there’s been any attempted scanning or anything amiss on our servers or network. We run checks internally for issues that would be within the commission itself — an employee looking somewhere they shouldn’t, for example. We can detect that here.

Nothing’s happened recently, but you’re always having people scan your network. That’s why you have to monitor it so closely. It’s a sewer out there; there are thousands of viruses, so we have multilayered virus protection. When something comes into our mail router, it’s scanned for viruses, then it’s scanned again in software that Savvis uses, then it’s scanned again when the e-mail hits our internal systems.

We’ve been fortunate, but there’s a huge amount of effort in ensuring that nothing happens. Because once something does, it’s very difficult to regain the trust of the public. We have not had that happen, thank God.

— Interview by **Johanna Ambrosio**



www.savvis.net