

Highlighting the career of outstanding ISSA members...

Marc Noble

ISSA Public Service Award 2007

The ISSA Public Service Award recognizes an individual's contribution to the information security profession in the areas of public service, programs, legislation, public affairs, and public awareness of information security issues.

Marc Noble certainly exemplifies this award, retiring earlier this year after 30 years of U.S. government service, his most recent position being Chief Information Security Officer of the Federal Communications Commission, as well as his tenure in the ISSA, currently president of the Northern Virginia chapter. Let's hear his story.

In 1991, I was a computer programmer looking to do something different. I moved to the Court Systems Branch in the federal judiciary, working in the areas of information security and quality assurance, both of which were new to me. I dove right in, reading a lot in both areas and really developed a fascination in the security side. There was no security office at the time, and I was soon tasked with setting up a security program at the U.S. Courts.

Having a technical background and starting a program from scratch was a real challenge. I certainly took up that challenge and did my best to move the judiciary forward, but dealing with a very decentralized, flatly managed organization proved to have some serious difficulties. But I did have a positive impact, and a lot of the core units soon knew who I was. When they had problems, they'd call me up.

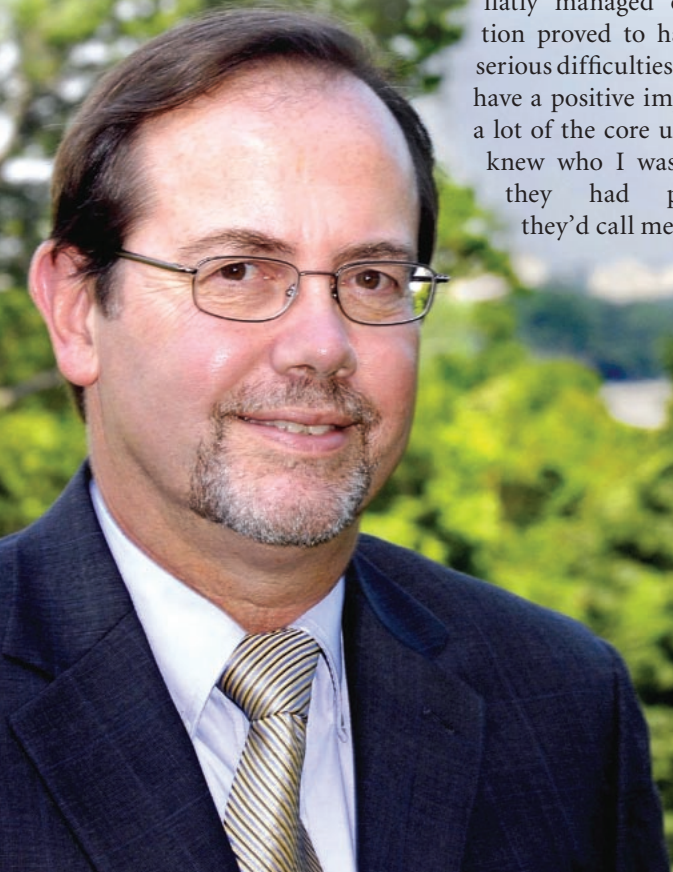
One of the key things I think any security person should be aware of, especially a chief of security, is making sure that you know who your clients are, making sure they know who you are, and making sure they know you are concerned about them.

I've always advocated communication. An excellent tool is to have some type of newsletter, which does an unbelievable job of communicating out to your community who you are, what you're about, and how you're trying to help. You shouldn't be trying to say "don't do this" or "don't do that." Give them good working, practical knowledge of how to protect themselves. That really goes a long way towards getting buy-in for a security program.

I ended up getting invited out a number of times to U.S. Court units just by having good communications with them. They thought I was on their side. *Well, I was on their side.* I think they honestly believed I was really working for them, with their interests in mind. That's the one thing we all have to work at. Make sure our clients know we are working for them. This has worked for me, and I think it's an excellent way of selling security. I took a lot of jobs going through college. One was being a sales clerk. Lesson learned: you are working for your client. If you want to make a sale, the client needs to be sure you are working for them, giving them the best value for their money. It works for security as well.

Also during my time with the U.S. Courts I pushed the development and laid the groundwork for the incident response capability. It was an interesting work environment, trying to get 300 organizational units with aversion to central control to be able to report in, when what we were developing sounded like central control to them. We got it done, and to my knowledge it is still working today.

In 1997, I was invited to join the Federal CIO Council's Federal Best Security Practices Committee, and we developed the document *Proposed Plan for the Federal Best Security Practices Program for CIO Council* and a small website as a test bed for setting up best practices in the government. Eventually the National Institute of Standards and Technology (NIST) set it up as the *Federal Agency Security Practices* website. So they just changed the name and used some



of the practices we worked on. That's been a lasting legacy I can proudly say I took part in. I feel that if we can help others get better, that's what we should do.

The FCC

My last move in government was in 2002 when I became the associate CISO at the FCC. As associate I was being schooled and groomed to take over the full position if necessary, and after two years I stepped into the position of Chief Information Security Officer of the Federal Communications Commission. What an absolutely outstanding experience. Everything I'd read about setting up a program, I was now able to actually do, really providing leadership in moving forward, moving the program in the way a program really should be set up. It was a good program, but I wanted it to be deeper in looking at the security problems of the agency.

I pushed my staff to begin looking at security problems before implementation of a system or application rather than afterwards. I got us involved in the *development* of applications and systems, giving advice to our clients on security problems they should think about *before* final development. I felt I made a real impact in moving the security program forward, providing the FCC with a much better security stance.

I also paid a lot of attention to what the Office of Management and Budget (OMB) was telling the agencies at the time and the directions they wanted to go. One thing they were pushing was that a system should be checked from the very beginning to make sure proper settings and configurations were correct and appropriate for building upon – before installing applications. About a year before the OMB came out with the Federal Desktop Core Configuration, I had been pushing my staff in that direction. Granted the systems staff was not too happy at times because they felt the tools we were using weren't the best – I certainly agreed – but I convinced them that in the long run they'd be much better off and it would help the FCC. They bought into it. Consequently, by the time the FDCC came out, when the FCC did the test to find out how we were doing, we were at an amazing 95% compliance. We did something right!

The ISSA

In addition to working a normal job, I am always looking for opportunities to get involved in the greater community. I was a history/political science major and my feeling has always been that we should all – and there's a particular responsibility for security professionals – get involved in public service and public affairs. It's what we are about, protecting the public, helping the public understand their need for privacy, for protecting themselves online. I think it behooves us as security professionals to go out as much as possible and talk with people outside our profession to make sure we are providing good service to our community.

I got involved with ISSA in 2001. I was looking for an outlet for doing something – my wife asks me why I do so many jobs where I don't get paid – No apologies, I just like to do it.

ISSA Northern Virginia (NOVA) chapter had an open house. I went to it; met some good people; got invited to speak at a conference for certification and accreditation. Someone said I should run for office and I ended up secretary. Did it for two years, then VP for membership for a year, and just recently became president. I find the ISSA to be an excellent outlet for keeping up with security issues and meeting great people with whom I have a lot in common. And our chapter is always looking at ways to benefit the community.

One of the things ISSA-NOVA is working on – and I am very proud of – in conjunction with the (ISC)² Government Advisory Board is to develop a scholarship and assistance program to assist returning veterans to receive training and positions in the information security industry. We are looking at something that will provide them IT skills, and if they have IT skills perhaps get them interested in information assurance. Certainly there is a large need these days. It's not as far along as I'd like, but we are still making progress and developing a program to help our veterans.

Another thing we did this year was set up a scholarship fund in honor of one of our founding members, Laurie McQuillan, who died of cancer last year. A lot of folks talked about doing something for her, and I'm the kind of guy that says "let's do it." I talked with George Mason University, where she earned her master's, and we set up a scholarship fund. ISSA-NOVA is now working diligently to fund it and build it to be a perpetual fund for information assurance students at GMU.

Just recently ISSA-NOVA agreed to promote National Cyber Security Awareness Month,¹ a national campaign focused on educating the American public, businesses, schools and government agencies about ways to secure their part of cyberspace, computers, and our nation's critical infrastructure. We are going to be putting it on our website (by the time you read this) – *Protect Yourself before You Connect Yourself*, linking to other organizations to get the message out: 10 things to do to protect yourself, what to look for with computer viruses, and the like. We have to find better ways of communicating with the public to make sure they know how to protect themselves online. As a security professional, I continually hear stories that will curl your hair about people who got their bank accounts drained, and how cavalier people can be, thinking nothing is going to happen to them.

Well, it's been a great run. I just retired from the government after 30 years. It was a good career, and I learned a tremendous amount. They gave me great opportunities to learn and develop leadership skills. One reason I have taken my new position at MITRE was so I could continue to work with the government, hopefully protecting the taxpayers by giving good advice to our government on how to operate efficiently and securely.

Thank you, Marc, you certainly embody the spirit of ISSA's Public Service Award – ISSA Journal.

¹ <http://www.staysafeonline.info/events/index2007b.html>.