Cyber Challenges that Keep HHS' CISO Up at Night

As the top official in charge of IT security for a federal agency thwarting billions of cyberattacks weekly, Christopher Wlaschin knows first-hand the challenges of safeguarding IT systems and protecting at least one-third of Americans’ health information housed within the Health and Human Services Department. Government CIO Media Editor-in-Chief Camille Tuutti talked with Wlaschin, who serves as HHS’ chief information security officer, about some of those hurdles and
how emerging tech helps his agency meet its mission.

**Government CIO Media:** Let’s talk about your office and how you keep up with all the cyber challenges out there. What are some of the obstacles you have to deal with?

**Chris Wlaschin:** HHS is, as you know, 11 operating divisions from the Food and Drug Administration to the National Institutes of Health to the Centers for Disease Control and Centers for Medicare/Medicaid and the Indian Health Service and a number of others. At each of those organizations, there are very talented cyber professionals.

We meet frequently. We operate as a team. We act in unison, when it comes to protecting HHS data, assets and people.

Recently, we undertook an outreach effort to help the health care and public health sector to become more cyber aware and cyber resilient. So, it’s a day-to-day challenge and a huge job. I absolutely cannot do it myself, so I rely on some very effective team members to help me understand the challenges that HHS and the public health sectors face.

**GovCIO Media:** In your role, what do you see as the greatest difficulties new technologies pose for your office at HHS?

**Chris Wlaschin:** The security organization tries to view new technologies as opportunities rather than roadblocks. Security should be an enabler of business and mission functions, not a roadblock to the adoption of new technologies. We work
very hard with our business owners, with our system owners, with the groups that want to bring new technologies to HHS, to understand their value first, how they positively affect the mission and then what, if any, risks they may pose — and then work with the business owners, vendors and others to understand and mitigate those risks.

So, we welcome new technology, to understand that’s the way of the future. That’s how government gets more agile, more responsive to public demands for our services, and we welcome that opportunity, but we do so with the position that we want to understand and mitigate the risks as they present themselves.

GovCIO Media: With the fast-evolving nature of technology, how has your approach to health information and data security changed?

Chris Wlaschin: Well, I get a great deal of input from industry, from the health care sector and my own team on technology innovation. HHS has a security design and innovation team that evaluates new technology and looks for opportunities to bring them into the HHS environment, to help HHS be more effective.

The creation of this team has really enabled us to interact more closely than ever before with vendors, with industry and with the health care sector, to understand our customers, what our stakeholders are seeing, and to make sure that HHS stays abreast and aware of evolving technologies, so we can bring the absolute best, most cost-effective services to our stakeholders.

GovCIO Media: One of the hottest topics in the recent years is AI. Is that something that plays a role in making processes more efficient?

Chris Wlaschin: I am excited of the promise of artificial intelligence and what it can do. When you think of the number of cyber threats that HHS distends every day, every week, every month, it’s in the billions. And there is no way we can hire enough cyber analysts to take a look at each one of those threats and react to it. Artificial intelligence, cyber defenses operating at machine speed bring great promise to defending HHS and the government at large from major cyber threats.

The other area of AI that I am excited about is process improvement. HHS is currently piloting, along with some industry partners, the insertion of artificial intelligence as it applies to process improvement. We think there is a great opportunity for using AI to conduct repetitive, administrative, procurement and
even contracting processes, not major decisions but processes to enable our scarce and valuable government employees to focus on the most important decision points, letting AI do the background work of moving workflows through the agency.

**GovCIO Media:** One of the tougher things to solve is finding that balance between innovation and security. How do you encourage both? Is there any tension between the two?

**Chris Wlaschin:** There is creative tension between innovation and security. Here is what I mean by that: Government needs to be more agile and more cost effective. We need to bring our products and services to market in the same rapid way that industry does. Innovation provides a rapid insertion of technology processes that go against traditional government procurement acquisition and security rules.

For many years, we have taken all the time we needed to evaluate innovative technologies and processes. And we’ve come to find that our processes are too slow, and we are not reacting fast enough. I like to call that tension between innovation and security a positive thing, a creative thing, because it makes both sides of the coin — innovation and security — work closer together to make sure that any new software applications, hardware, or cloud technologies are brought in just as quickly as they can but with security in mind.

**GovCIO Media:** Is there a role for the private sector in achieving the Office of the CIO's goals?

**Chris Wlaschin:** Yes, I am a firm believer that government cannot do this alone. We absolutely must rely on our private sector partners, our vendors, our strategic stakeholders, to deliver on the promise that the government is supposed to provide to our citizenry. Agile, cost-effective, secure applications that protect our citizens’ data, and delivers the services that they need from government. Government cannot do this alone. I see public-private partnerships between government and industry growing to deliver the services that the citizenry demand of us.

**GovCIO Media:** On top of that, are there certain private sector best practices HHS and your office could employ?

**Chris Wlaschin:** Private sector is really the master of best practices, when it comes to cybersecurity, innovation, delivery of cybersecurity services. Private sector has made great leaps and strides in advancing cloud security, cloud
availability and cloud privacy, and the government could learn from what the private sector is doing there.

HHS has significant initiatives around the rapid adoption of cloud environments in our Federal Risk and Authorization Management Program. The private sector is working closer with the National Institute of Standards and Technology, closer than ever before, across a variety of sectors, not just health care, to understand the risks that cyber, malware and cyber activities present against government organizations.

The private sector has thought through some of those things and is sharing best practices with HHS. Our recent partnerships with organizations like the National Health Information Sharing and Analysis Center and iTRUST tell me that the private sector is banding together. They are sharing information about cyber threats and when they share those with the government, together we all become stronger.

**GovCIO Media:** What are some of the ongoing or upcoming initiatives you are most excited about?

**Chris Wlaschin:** I am very excited about the Modernizing Government Technology Act that was recently passed. I think that we finally have the motivation and funding from the administration and Congress to make big changes to the way government manages technology, to reduce our reliance on legacy applications and infrastructure that cannot be supported any longer, so that we can become that more agile, more responsive government we have been talking about for years.

I am also excited about the focus on protecting our high-value assets first. Those applications, those databases that contain our most sensitive data, are the focus of our security technology investments. I like the fact that the government is rallying around the [Homeland Security Department] program for HVAs and continues to use diagnostics and mitigation programs to really focus cyber investments where we need it the most and where the highest risks are. So, those two initiatives alone — HVAs and continuous diagnostics and mitigation — will give us plenty to do in FY18.

*This interview has been edited and condensed for clarity.*

[View printer friendly version](#)

Federal Cybersecurity

cyber