

CGI INITIATIVE FOR COLLABORATIVE GOVERNMENT'S

Leadership

WINTER 2012

Cybersecurity and Mobility:

Securing the Mobile Frontier

Gen. Keith **Alexander**
USCYBERCOM & NSA/CSS

Dr. Edward **Amoroso**
AT&T

Gregory **Garcia**
Banking/homeland cyber executive

Lt. Gen. Susan **Lawrence**
U.S. Army

Dr. Peter **Levin**
Dept. of Veterans Affairs

Christopher **Painter**
Dept. of State

Gregory **Schaffer**
Dept. of Homeland Security

Teri **Takai**
Dept. of Defense



Initiative for
Collaborative Government

WWW.COLLABORATIVEGOV.ORG/LEAD

Table of Contents

Editor's Note	3
Securing the Mobile Frontier <i>By Barbara Fast</i>	5
Leadership - Resilience - Flexibility – Communication <i>Insights from Gen. Keith B. Alexander, USCYBERCOM & NSA/CSS</i>	9
Securing the Airwaves <i>Leadership Profile of Dr. Edward Amoroso, AT&T</i>	16
Racing for the Advantage <i>Leadership Profile of Gregory Garcia, Banking / Homeland Cyber Executive</i>	22
Connected for Battle <i>Leadership Profile of Lt. Gen. Susan Lawrence, U.S. Army</i>	28
Open Warfare <i>Leadership Profile of Dr. Peter Levin, Dept. of Veterans Affairs</i>	33
Global Cyber Sleuth <i>Leadership Profile of Christopher Painter, Dept. of State</i>	40
Running the Rapids <i>Leadership Profile of Gregory Schaffer, Dept. of Homeland Security</i>	47
Chain of Security <i>Leadership Profile of Teri Takai, Dept. of Defense</i>	52

Editor's Note

Welcome to the Winter 2012 issue of the CGI Initiative for Collaborative Government's executive journal, Leadership.



Andrew McLaughlin

Leadership gives voice to thoughtful executives who are creatively and effectively addressing the most important issues confronting the United States and the globe. Each issue focuses on a theme that challenges leaders in every organization, featuring profiles of executives whose practical insights and observations are born of success and are applicable across the government, private and nonprofit sectors.

This issue focuses on “Securing the Mobile Frontier.” To set the stage, we start with a candid Q&A with General Keith Alexander, Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service. Next, we feature perspectives from other leaders in cybersecurity and mobility, including alphabetically:

- **Dr. Edward Amoroso**, Chief Security Officer, AT&T
- **Gregory Garcia**, former Bank of America Partnership Executive for Cybersecurity and Identity Management, and the first Assistant Secretary for the Office of Cybersecurity and Communications, U.S. Department of Homeland Security
- **Lieutenant General Susan Lawrence**, U.S. Army Chief Information Officer/G6
- **Dr. Peter Levin**, Chief Technology Officer, U.S. Department of Veterans Affairs
- **Christopher Painter**, Coordinator for Cyber Issues, U.S. Department of State
- **Greg Schaffer**, Assistant Secretary, Office of Cyber Security and Communications, U.S. Department of Homeland Security
- **Teri Takai**, Chief Information Officer, U.S. Department of Defense

I want to thank these leaders for taking time out of their difficult schedules to share with us their ideas on leveraging and securing the use of mobile computing. Thank you to each of you for the time, insight and dedication to mission that you shared with us.

This issue also includes analysis on our theme from CGI Initiative Fellow Barbara Fast, who previously served more than 32 years in U.S. Army where she retired at the rank of Major General and led intelligence, operations and security systems. In her article, Barb examines issues in securing the mobile supply chain, network, apps and data, and highlights opportunities

for public-private partnerships to play a critical role in tackling those challenges. Thank you, Barb, for your leadership on this journal. We truly couldn't have done it without you.

Finally, a special thank you to CGI Initiative for Collaborative Government Fellows Dr. Jim Peake and Molly O'Neill, whose vision and insights were invaluable in creating this journal. And thank you to Sarah Lindenau for managing this "Securing the Mobile Frontier" project with excellence and a smile!

Now, onward to *Leadership!*

Andrew McLauchlin

Executive Director

CGI Initiative for Collaborative Government

Securing the Mobile Frontier

By Barbara Fast

Cybersecurity in the mobile age is everyone's responsibility, requiring strong partnership among businesses, governments and citizens



We are living in an information age that has changed the way we conduct business and share information.

For government and industry, technology has allowed a level of interconnectedness that we have never experienced before.

The ability to connect with anyone at any time and quickly access the data we need is a great convenience that has made it easier for us to conduct business and military operations, improve services and stay in touch with our customers.

Barbara Fast

But living in a digital world is like living in a bad neighborhood. It doesn't mean you shouldn't leave your house, but you have to take some precautions. Just as you wouldn't open your door to just anyone, you don't want to invite an unfamiliar application or attachment into your network, and you want to make sure you have the security necessary to protect your data.

A couple of decades ago, there were very few people involved in cybersecurity, but now it's everybody's responsibility — from the person who wants to bank online to any organization or nation conducting business online.

As we learn from our experts in this journal, the mobile environment has added a whole new dimension to what it means to secure our enterprise. It's not quite the Wild West, but we are still on the frontier when it comes to securing mobile devices and determining how they connect reliably to an overall network. There is a cyber ecosystem that must be managed, and mobile devices are just a part of the bigger picture.

A Way of Life

From veterans who download their health records via the Veterans Affairs Department's website to soldiers who use smart phones on the battlefield, more individuals, businesses and government organizations are using mobile devices as part of their daily routines and creating a global interconnectedness. Just as doing business on the Internet became the norm, operating in a mobile environment is not a choice any more but a way of life.

Why has this happened? Today's technology is more robust, bandwidth has increased, software advances have made it easy to download an application to a mobile device, and there is much better interconnectedness — from a mobile device to the cloud to the enterprise. That combination of technology and human development has allowed us to take advantage of connecting from anywhere and freed us from the desktop.

That's why it's important to treat cybersecurity as an ecosystem and recognize that all the parts are interdependent on one another. Organizations must rely on a multilayered set of solutions to protect the most valuable resource we have: the data that resides on our networks. This includes sound supply chain production and procurement practices. We can't expect to secure anything 100 percent, but we can mitigate the risk of being attacked, and if we are attacked, we can mitigate the risk of being compromised and more quickly react and restore service.

We have to make sure we know where the knowledge points are, where the valuables reside that need protection and how to develop a defensive posture to protect them. When it comes to securing mobile devices, the connections must have integrity.

How Much Security is Enough?

The million-dollar question is: How much security is enough? If we had the answer to that, we would buy only what we need. But there are a lot of unknowns, and the situation is not static. Furthermore, the tolerance for risk differs from organization to organization and even from department to department. The key is risk management and deciding what you should spend your money protecting. I come from a military background, so I start with the commander's information requirements and look for high-value capabilities that would cause an organization to fail if they weren't available. It's the same basic principle for commercial and private risk management considerations.

Prioritizing security is a challenge because it is difficult to measure how well your investment is doing. How do you know what you've been able to prevent? The sign that no intrusions have occurred is obviously a good thing, but how do you measure that? More and more organizations are incorporating a new technology into their game plans. For example, cloud computing makes accessing mobile applications easier, but it has to be secured just like the rest of the environment. Whether it's a public, private or hybrid cloud, it is part of the cybersecurity ecosystem.

For AT&T Chief Security Officer Edward Amoroso, the future of security lies in virtualization, which means moving identity management and threat detection to the cloud. In that scenario, Amoroso said, "I just tell the ISP, 'Here's my policy: I want you to filter the viruses from my e-mail, I want you to filter spam, and I'd like these services to be allowed and these services to not be allowed. I don't want my employees on Facebook, for example.' The Internet Service Provider can very easily do that for wired and wireless service."

"Organizations must rely on a multilayered set of solutions to protect the most valuable resource we have: the data that resides on our networks."

There are other security considerations as well. Increasingly, cybersecurity has become an international concern as digital communications and business transactions transit the globe. Many countries have leapfrogged from having little to no infrastructure to modern digital and wireless technologies.

Just ask Chris Painter, who is responsible for implementing the U.S. International Strategy for Cyberspace as cyber coordinator at the State Department. When the strategy was released in May, Painter sent a cable to State Department posts worldwide asking them to talk to their host governments and identify the officials who were tracking cyber issues in those countries so they could “be our eyes on the ground” and find opportunities to work together. That won’t be easy, however. Although data can be sent around the globe in nanoseconds, our ability to act and react is still functioning in the 20th century. The mobile environment doesn’t recognize sovereign boundaries, and today we still lack international laws to enable us to act against bad actors.

A Challenge We Must Accept

Although more work needs to be done, it’s reassuring to know that there is more government-to-government and government-to-industry collaboration today than there has been in the past, and we have made progress on advancing cybersecurity issues with our allies. Having appropriate laws in place, as well as national and global standards, will help. And there are bonafide privacy concerns that must be factored into solutions.

There is also a huge education component to securing networks. Better awareness, from Congress to institutions and individuals, will help create the conditions and framework for a comprehensive approach. People need to understand that they have to play a role in security. And that they are the first line of defenders. There will be some tough lessons along the way, but it’s a challenge we must accept.

When it comes to enforcement, it’s better to use more carrot than stick because people respond better to incentives. Consider the Defense Department.

Teri Takai, DOD’s CIO, said that by adopting a pragmatic leadership stance and offering a carrot instead of brandishing a stick she hopes to convince the military branches that moving to a common identity management infrastructure is in their best interest.

“One of the tricky things about information technology implementation, unlike some weapons systems, is that it’s as much about customer experience and the way people feel about their

technologies as it is about the technology,” Takai said. “Otherwise, these migrations would be pretty easy.”

“You Now Have Your Data. Be Careful.”

With cybersecurity, it’s important to strike the right balance and make it easier for end users to operate securely without expecting them to do too much, especially with mobile computing. Some organizations, particularly in the military, are struggling with whether to allow people to download applications to mobile devices or access Facebook on their operational network. Those are the kinds of struggles that mobile technology brings to bear. Some security solutions will simplify things for users, but personal responsibility is essential.

That is evident at the VA, where CTO Peter Levin said one of the biggest concerns about a Web-based function that allows patients to download their health information was more human than technical. Once downloaded, the information was much more susceptible to being lost, stolen or otherwise compromised. Levin said he posted a warning to veterans “with big bold letters on the website: ‘You now have your data. Be careful.’”

Ultimately, cybersecurity is everyone’s responsibility. Whether you are a government agency, military service or global business, we share more similarities than differences when it comes to cybersecurity. We are all operating on the same network, so the problems are bound to be similar and some of the solutions are similar, too. It’s how they are applied that will be different. As the articles in this journal illustrate, you can’t underestimate the power of strong partnerships and leadership when it comes to cybersecurity.

BARBARA FAST is vice president and senior advisor on cybersecurity at CGI and a CGI Initiative for Collaborative Government Fellow.

Leadership - Resilience - Flexibility - Communication

Gen. Keith B. Alexander, Commander, U.S. Cyber Command and Director, National Security Agency/Chief Central Security Service shares insights on leading for success in the mobile frontier and amid the rapid evolution of technologies and threats.

Organizational Leadership

Q: October 31, 2011, marks the one-year anniversary of US CYBERCOM active operations. You had to stand up a new organization quickly with multiple major changes happening



Gen. Keith B. Alexander

Image Courtesy of National Security Agency

simultaneously across very senior stakeholders. What do you feel were the biggest challenges you faced in standing up CYBERCOM? And how did you overcome them?

A: Fundamentally, CYBERCOM represents a new approach. The scale and rapid evolution of technology requires a resilient, flexible approach, changing our conduct and culture to one that features a dynamic, active cyber defense – using our understanding of

adversary capabilities to dynamically and rapidly defend military networks. Our military relies on its networked systems for every facet of force projection and, when establishing CYBERCOM, we were keenly aware of the gap between the sophisticated capabilities available to exploit and degrade those networks and the defenses in place to protect them.

There were several significant challenges on the ground to achieving that vision. First, we had to merge the two legacy organizations (Joint Functional Component Command for Network Warfare [JFCC-NW] and Joint Task Force for Global Network Operations [JTF-GNO]), representing the military’s cyber “offense” and “defense” to operate effectively as one unified force – CYBERCOM.

Then, we focused on merging their actual operations. We established a Joint Operations Center, transferred operational control of the JTF-GNO mission set to Ft. Meade, Maryland, and stood down JTFGNO’s 24/7 watch center in Arlington, Virginia.

That task involved careful planning to ensure that the daily functions of the Department of Defense’s networks were unimpaired, given that they are constant targets. We also established effective operational command and control processes for the consolidated mission sets.

Once we had begun to operate as one synchronized force, we focused on serving our customer requirements and building relationships with key partners. We trained and embedded liaison officers at the Combatant Commands and began working closely with the Commands to help understand and define their requirements for operating effectively in cyberspace. We also worked to ensure that these liaison officers were setting the foundation to grow into larger Cyber Support Elements over time.

We were able to accomplish these critical milestones because we have great people. Thanks to their exceptional efforts, we were able to stand up and lay the foundations for our vision of a rapidly evolving and effective active defense.

Q: What advice would you have for other executives who are faced with similar complex and rapid changes in their organizations?

A: In one sentence, I will share the best advice I've learned from one of my mentors: communicate, communicate, communicate. CYBERCOM represents a new way of operating in a rapidly adapting domain. We needed to communicate the core principles of our strategic vision and then work closely with the leaders and staff of the Command to get the Command to full strength and capacity as rapidly as possible.

Q: What are some core management principles and approaches that you have relied on in standing up CYBERCOM?

A: First, teamwork. We knew that this command would have to operate as part of a cohesive and comprehensive team— Team Cyber. I firmly believe in teamwork – within the Command, and with our interagency and international partners. We must marshal all of our respective talents to develop innovative solutions for mutual concerns.

Second and perhaps most important: people. Amazing people are capable of amazing achievements. Let your people know how amazing they are, support them and step back. The military and civilian personnel of CYBERCOM have challenging jobs. Their creativity and ability to rapidly innovate and execute are what have underpinned the Command's achievements in its first 18 months.

Q: What experiences in your life were major influences for you in shaping your management style? Why?

A: Over the past three decades, I have served in a wide variety of Joint and Army positions, including 15 years in command. I have served as the Deputy Chief of Staff of Intelligence, Headquarters, Department of the Army; Commanding General of the U.S. Army Intelligence and Security Command; Director of Intelligence, United States Central Command; and Deputy Director for Requirements, Capabilities, Assessments and Doctrine, J-2, for the Joint Chiefs of Staff. These roles of increasing responsibility provided the set of experiences and relationships I draw upon each day.

“Extending our information reach through new technology gives us great capability, but it also extends our vulnerability.”

Perhaps most importantly, I have had exceptional mentors throughout my career. While I learned a great deal, technically, from them, the most important lessons they taught me were those of leadership. People are our greatest assets, and I believe they perform the best in a positive leadership environment.

Focusing more exclusively on cyber, the knowledge gained serving as Director, National Security Agency, Chief, Central Security Service and Commander, Joint Functional Component Command—Network Warfare (JFCC-NW) were instrumental in shaping my vision of how the military needs to operate effectively in cyberspace. NSA’s cryptologic work in SIGINT/Computer Network Exploitation, Information Assurance and Network Threat Operations is superb and foundational to the nation’s future success in the cyber domain.

That knowledge has led me to champion NSA’s work and greatly value the outstanding professionals and expertise at NSA/CSS.

Leading for Success in the Mobile Frontier

Q: What do you see as the most critical challenges in achieving the right balance between taking advantage of mobile technologies to gain a communications advantage over the enemy and making sure communications are secure from enemy interception or interference?

A: I am an advocate for using mobile technologies. As I said, the key to managing complexity, from the battlefield to the office, is to communicate — which means access to, and movement of, information.

Extending our information reach through new technology gives us great capability, but it also extends our vulnerability. We’ve all seen the significant increase in malware focused on mobile devices as the new frontier. Today’s mobile devices are targeted as access points to enterprise networks and the valuable information stored either in e-mail, on the device or on the home network.

The Department of Defense, and government, writ broadly, have all learned that technology built only for government use is not a cost-effective or rapid way to deploy information technology. Rather, leveraging commercial technology while implementing careful configuration and best practices to maximize security is the best approach.

And as the technology across government and industry converges, we are also seeing a similar convergence of mission interest in security. Corporations are worried about threats to their intellectual property and the integrity of their networks via mobile devices, and so we are

seeing a move to incorporate security into commercial devices. We are actively supporting that via our information assurance partnerships with industry and across the USG.

Q: What is CYBERCOM doing today to create a team approach with the military services to secure the use of mobile devices?

A: The addition of mobile devices to DOD's inventory does create some unique challenges, but they're ones we face regularly. CYBERCOM is leveraging work that NSA is doing to secure mobile devices and championing these efforts for the services. The key is to leverage this new technology, ensure it is secure and work with the services so that we can acquire and deploy these technologies for best operational and defensive effect.

We also have to remember that security (or insecurity) is fundamentally a systemlevel problem. The adversary attacks the system where it is weak. So we have to secure not only the mobile device, but also the transport of information, the infrastructure at the backend that supports it, every partner in the system, and everything in between. So the notion of team is much broader than ever before.

Q: How do you view the future for network defense with the influx of mobile devices, particularly in regard to mobile security and network situational awareness?

A: We believe that both the private sector and the USG value secure mobile devices – devices that protect the corporate and personal data resident on the devices and on the enterprise networks they access. As greater and greater capability moves to mobile devices (e.g., banking), security becomes more and more valued. We are working closely with the private sector to ensure that the lessons learned from the last two decades of PC security are applied to mobile devices.

We believe that the future of network defense is a much more dynamic problem than in the past. New technologies and devices will continue to appear in our environment. So we can never secure the defense one device at a time. We need to improve the whole ecosystem through standards, best practices and improvement to the supporting infrastructure.

Q: How will Cyber Command work with the department to grow the cyber workforce of the future to defend and secure mobile networks?

A: The Department must grow the cyber workforce to operate and defend both mobile and fixed networks. Working with our Service Component Commanders, we have identified the base set of personnel resources needed to meet a subset of Operational Plans in support of the Geographic Combatant Commands. The Chairman, Vice Chairman and Service Chiefs are working together to generate the forces we need.

"We believe that the future of network defense is a much more dynamic problem than in the past."

More broadly, we are leveraging the work of government partners like DHS to increase the nation's overall cyber workforce capacity through programs like the Centers of Academic Excellence in Information Assurance (CAE-IA) and the National Initiative for Cybersecurity Education (NICE). We also fully support efforts to interest American teens in science and technology. Various states and not-for-profits have launched contests and scholarships to interest American high school students in S&T. Attracting the nation's best and brightest to science will ensure our finest minds drive the nation's economic growth and national security.

Q: What key challenges have you seen that you expected? That you didn't expect?

A: The key challenge is, of course, the threat. The cyber threat continues to mature, posing risks to the nation. Our leaders— from President Obama on down— have emphasized this point, and for good reason. Our nation now depends on access to cyberspace and the data and capabilities residing there; we are collectively vulnerable to an array of threats ranging from network instability to criminal and terrorist activities to state-sponsored capabilities and actions that are continually evolving. While I emphasize that we have not suffered disastrous or irreparable harm in cyberspace from any of these risk categories, we must be prepared to counter this evolving threat. Building a common understanding of the threat is key to achieving a whole-of-government and whole-of-nation effort.

On a more tactical level, what we have found as we improve our common operating picture, our intelligence and our operations to create effects is that DOD does not have the capacity to do everything we need to do to defend our military networks. To put it bluntly, we are very thin, and a crisis would quickly stress the military's cyber forces.

The problem has two facets—there are too few trained service personnel out there in the first place, and the services need to hold on to as many of them as they can. Thus, the biggest issue I see is the need for collaborative force development— including joint standards, recruitment, training, deployment, sustainment, and retention across the services.

Q: How have you overcome those challenges? And what lessons have you learned that will reshape your approach in the future?

A: First and foremost, we are communicating the threat to educate key decisionmakers on our nation's vulnerabilities to cyber threats and the steps that we need to take to protect our critical networks. It will take a team — across the government and private sector — to measurably improve the nation's security in cyberspace. At CYBERCOM, we are focused on working with NSA, DISA and the services — our core partners — to measurably improve the security of military networks.

Q: What recommendations do you have for other senior leaders as they work to take advantage of mobile technology while securing its use?

A: I recommend we challenge our people to push the envelope in using commercial technologies while working to configure and use them in the most secure ways possible.

I also urge senior leaders who are considering mobile technology (or any technology) to stand back and realize that their mission needs are not likely unique. We need to think of these as enterprise-level problems – shared problems requiring shared solutions. We cannot afford to have every organization independently chasing the latest technology. By working together, we can bring together our best minds in technology and security, bring critical mass to the marketplace, put in place enterprise-level security infrastructure and help improve security at national scale.

Q: How is managing cybersecurity programs different from other programs you have led?

A: The information technology environment is the fastest-changing environment in the DOD and the nation. Conventional approaches will not work. To adapt, we work our efforts in 90-day spins, leveraging what we have done, constantly trading technical advances and adjusting our plans. We have had tremendous success with this approach, which we are now applying in our IT efficiencies and effectiveness programs.

Hardware Security and Supply Chain Risk Management:

Q: With the proliferation of mobile devices, what is your perspective on how U.S. organizations can best secure their mobility supply chain to prevent bad actors from inserting hardware components containing malicious software code and the like (mobile devices, servers that operate mobile applications, etc.)?

A: Supply chain risk mitigation is a national effort under the Comprehensive National Cybersecurity Initiative. The global technology supply chain affects mission-critical aspects of the DOD enterprise, as well as core U.S. government and private-sector functions, and its risks must be mitigated through strategic public/private-sector cooperation. DOD is supporting interagency efforts to increase assurance in our information and communication technology supply chain. (Public Affairs Guidance DOD Strategy for Operating in Cyberspace July 2011)

Q: Mobile computing poses different hardware security challenges than desktop environments, with two leading platforms (iOS and Android), and more platforms continuing to mature (e.g., Windows and BlackBerry). How can we best secure mobile device hardware in an extremely heterogeneous environment?

A: First, there is great value in leveraging the lessons learned from the work done to improve the security of PCs over the last decade. The private sector began incorporating roots of trust in

devices (e.g., Trusted Platform Modules [TPMs]) over the last decade, providing a “root” for further security to build upon in the device.

The second is to evolve our thinking from securing devices and systems to securing data — ensuring that the most valuable IP, whether source code or R&D designs, is protected and kept on networks where access controls are carefully managed. I think roots of trust and smart data will help reduce these risks.

We must recognize that there has been a fundamental change in our information environment. New devices and technologies will appear rapidly, so we must plan for that. Everything from our gathering of requirements, acquisition and security decision-making must be more rapid and nimble. We must also reshape the entire ecosystem through standards, better security infrastructure and improvements “upstream” in the life cycle with key vendors. We cannot get what we need by waiting for it to appear, then trying to secure it.

Q: How are you shaping DOD partnerships to incent innovation and arrive at solutions that are platform neutral and trusted, while building in supply chain security?

A: The evolution of commercial technologies like cloud technology and smart data offer tremendous opportunity in ensuring the security of our infrastructure. They give us the opportunity to implement and manage security at enterprise-level scale, in addition to the IT benefits. DOD is aggressively pursuing these technologies in our IT effectiveness program. We also strongly support the evolution and use of open standards to enable us to choose “best of breed” security solutions and integrate them more effectively.

In today’s fiscally constrained environment where cyber operations and threats are global and exponential in growth, we cannot afford to rely solely on Department of Defense resources. We must leverage partnerships with other governmental agencies, countries, industry and academia to form a comprehensive defense against cyber adversaries.

Securing the Airwaves

AT&T Chief Security Officer Edward Amoroso patrols the 21st century battlefield of the mobile network

By Stephanie Kanowitz

Photography by Noah Rabinowitz



AT&T's Dr. Edward Amoroso

In the 1980s, Edward Amoroso was a member of the security design team for then-President Ronald Reagan's Strategic Defense Initiative, the program that sought to build a space-based shield to protect Americans from a nuclear ballistic missile attack.

Now, as chief security officer at AT&T, Amoroso oversees a strategic defense initiative of a different nature — securing billions of bytes of information as they travel over the airwaves and wires.

On an average business day, nearly 24 petabytes of data travel over AT&T's global backbone. Although that backbone includes 46.6 million access lines and 19.3 million wired broadband connections, a huge share of that information moves via wireless networks. In 2010, wireless connections on the company's network increased by 8.9 million, the largest jump in AT&T's history. The company also operates the country's largest Wi-Fi network with 29,000 hot spots nationwide.

"If I look back over the decades, it becomes crystal clear that security in the mobile ecosystem has to become virtual."

Almost 18 million broadband customers in more than 150 countries use home Internet services, smart phones and other mobile devices to share information ranging from innocuous tweets and Facebook status posts to purchases containing highly sensitive personal banking information, tax returns with Social Security numbers, confidential medical records, and even commercial and state secrets.

In many ways, Amoroso's challenge hasn't changed: Allow people to conduct their daily lives blissfully under a transparent, trusted security umbrella they never see or want to see. But the cyber threats he now seeks to block, root out and destroy are much more subtle than an incoming ballistic missile.

Shifting the Front Line

The cybersecurity world has become much more complex in the intervening years. Today the term “hacker” connotes malicious intent, but 25 years ago, Amoroso used Unix operating system commands to access others’ machines and understood they were doing the same to his computer. The environment was collegial, but that changed when commercial and public entities began adding important information and transaction capabilities, he said.

“As soon as mobile became part of the infrastructure of a company, the military, power companies and so on, it’s not enough to say, ‘Oh, well, I’ll just promise to not [use what I find],’ which is what we did in the early days of the Internet,” Amoroso said.

"When you go from convenience to necessity, then suddenly the underlying infrastructure becomes important, and that's where the security comes in."

As the Internet has evolved, it went from being a tool for technologists to being a required part of personal and professional communication. We now expect to be able to communicate on the go anytime, anywhere with confidence and security.

“Remember when your BlackBerry or your smart phone was a convenience?” Amoroso said. “Today, it’s a necessity. When you go from convenience to necessity, then suddenly the underlying infrastructure becomes important, and that’s where security comes in.”

Hackers’ intent is of little consequence to Amoroso; his response is the same regardless of whether the suspicious activity comes from a curious kid or a malevolent nation state.

“The problem for us as [Internet service providers] is that a kid in a garage hacking and a nation state hacking look the same,” he said. “It doesn’t do you much good to get yourself wrapped up in the intrigue because we’ve seen teenagers who are really, really good, and we’ve seen nation states that are really, really bad.”

Amoroso said it’s unfair to expect consumers who are largely untrained in technology to be systems administrators fighting toe-to-toe with expert hackers. In the early days, the contracts between ISPs and their customers stated that all the providers had to do was move traffic the way a phone company connects callers.

Today, customers don’t want every piece of data coming to them out of fear of hackers and viruses, Amoroso said. They want a virtual Do Not Call list. He believes the future of security lies in virtualization, which means moving identity management and threat detection to the cloud.

In that scenario, Amoroso said, “I just tell the ISP, ‘Here’s my policy: I want you to filter the viruses from my e-mail, I want you to filter spam, and I’d like these services to be allowed and

these services to not be allowed. I don't want my employees on Facebook, for example.' The Internet Service Provider can very easily do that for wired and wireless service."

Virtual makes sense to the next generation of mobile users. They accept that systems are maintained virtually, he said, and they easily relinquish control.

"If I look back over decades, it becomes crystal clear that security in the mobile ecosystem has to become virtual," Amoroso said. "If the computer was basically a virtual terminal or virtual desktop and there wasn't as much software there and more of it was in the cloud, then you wouldn't have so much to break, right? The way Facebook doesn't break because it's out there somewhere."

Amoroso puts the alternative in perspective by asking, "Do you really want to have to worry about doing security administration on your BlackBerry? No, not in a million years. Let somebody else do it."

"As soon as anybody under 25 is in a position of leadership, you know it's going to be mobile, you know it's going to be virtual, you know it's going to be cloud," he added. "All those words are things that are connected to youngsters."

One way to secure what's "out there somewhere" is to create decoys, Amoroso said. Deception is a highly understudied and underused, although well-proven, form of defense. Setting up decoys that mimic actual infrastructure can trick adversaries into thinking they're attacking something real, he said. "You can imagine the uncertainty [for attackers] that comes out of that type of arrangement and the value to anybody protecting critical infrastructure," he said in a video about protecting the national infrastructure from cyberattacks on AT&T's Tech Channel.

Securing the Insecure

The root of the problem with cybersecurity lies in the fact that the Internet was not built with security in mind, Amoroso said, and retrofitting it for protection is an ongoing, inherently faulty process.

"The infrastructure was built to support cooperation and communication and the collaboration between different groups," Amoroso said. "Protocols were designed that way, systems were designed that way, software was designed that way. The computer you have at home was designed that way. There's no inherent or intrinsic security, you just plug into an Internet service provider."

When the Internet went from being a tool of the Department of Defense to one of the people, every sector of the U.S. economy wanted to be part of it. "We had a big time-out and retrofit security onto the whole thing, and it was never retrofit properly and it's still not retrofit properly," Amoroso said.

To address the problem, he said, two main problems with the Internet have to be solved: domain names and routing.

“The Domain Name System to this day is a pretty easy thing for someone to go in and muck around with and cause problems simply because it was designed as a very collegial thing,” he said, adding that “it’s tremendously easy for someone at the ISP level to redirect you around.” For example, in April 2010, the networking hardware that routes Internet traffic sent requests from 15 percent of IP addresses through China, knocking many websites, including U.S. government ones, off-line, according to a Nov. 23, 2010, article by the Massachusetts Institute of Technology’s “Technology Review.”

"We haven't gotten to the point yet where we're all comfortable that there are appropriate protections for things that we would connect to the Internet."

One of the steps Amoroso recommends for improving security is diversification, as opposed to the current practice of interoperability. He acknowledges that interoperability has its advantages, including reduced training costs, ease of use and ease of procurement. But the pros don’t outweigh the cons. Interoperability “is a situation where an attack, a worm, a botnet — some sort of malware — once it finds its way into the enterprise has an almost trivial path to the rest of your infrastructure,” Amoroso said in the AT&T video.

The rise of mobile applications and the ease of simply clicking and downloading an app have further complicated the security puzzle. Gone are the days when no one would insert a disk into a hard drive unless it came in tamper-free shrink wrap from a reputable store. “All of that is broken down now with the concept of an app store,” he said. “Some of us still think about buying a shrink-wrapped copy of Microsoft Office and here it is, I can put my arms around it. It’s mine. It’s not off in Neverland. Kids don’t think that way. I buy shrink-wrapped Office for my kids and they say, ‘Dad, that’s stupid.’”

Fixing the Information Superhighway

In “Cyber Attacks: Protecting National Infrastructure,” published in November 2010, Amoroso suggests actions government and commercial leaders can take to improve their security posture, such as separating internal assets, using multiple layers of protection and being aware of indicators that suggest problems before harmful effects are seen. He also offers larger policy recommendations to tackle the difficult work of overlaying security on top of something that was built to be open.

“We haven’t gotten to the point yet where we’re all comfortable that there are appropriate protections for things that we would connect to the Internet,” he said. “One of our goals as an ISP is to get to that point of ubiquitous trust in network infrastructure.”

Security takes time, Amoroso acknowledges, and he cites examples of technological advances whose safety concerns were gradually eliminated. “Lighting fixtures were dangerous things in the early days, and people were very nervous about using AC power,” he said. “Even cars in the early days were relatively dangerous.”

Computer science is still new and therefore open to vulnerabilities, he said, adding that people write software, the building blocks of the cyber world, and human error is inevitable.

“It’s almost as if we were building bridges out of blocks that we knew would fail,” he said. “When you drive up to a bridge, there’s a big sign that says, ‘Wait a minute, before you go over this bridge, you have to click on this I accept button.’ If you read the ‘I accept’ screens for software it says, ‘This really doesn’t work and if there’s a problem, it’s your fault.’”

“Security generally is something that comes in after a particular device, system or infrastructure becomes important,” he said. “As an engineer, I wish security were incorporated in advance because we all know that’s the time to do it, but unfortunately — maybe it’s an American thing, maybe it’s a human thing — we often don’t want security to get in the way of adoption, and that’s happening over and over again.”

Vulnerabilities can run from trivial to potentially catastrophic, as in the case of nuclear power plants, Amoroso said. Ten years ago, engineers with minimal computing knowledge linked dial-up modems to electromechanical controllers to enable remote maintenance and administration.

On the surface, that capability saves workers time and organizations money, but Amoroso pointed out that if workers can access critical infrastructure from home, so can hackers.

“These are extremely intelligent people who run these systems, but they’re not computer scientists and they certainly haven’t been trained in computer security,” he said.

Amoroso is on a mission to adapt security to the existing information superhighway so everyday people can use mobile solutions with confidence. It won’t be easy, but drawing on the 10 principles outlined in his latest book, he believes achieving that kind of assurance is possible. For example, he recommends being discreet about the details regarding your technology, software, systems and configurations to help avoid or at least slow some attacks. He also emphasizes raising awareness among IT managers so that they can understand and recognize the difference between normal activity and potentially dangerous anomalies.

Geek-Ridden Start

As a kid in Fort Monmouth, N.J., Amoroso knew two things: He liked computing and he wanted to work at Bell Laboratories. In fact, he said computing is in his DNA. His father was a computer scientist at the Army’s Communications-Electronics Command, and both his brother and sister are computer scientists.

“The whole family is pretty seriously geek-ridden,” Amoroso said. “I grew up in and around the Internet. When I was a young teenager, I was sitting in front of a computer terminal logging into the ARPANet in the mid-’70s, poking around and looking at things, so I always had an interest in computing.” ARPANet — the Advanced Research Projects Agency Network — was the precursor to today’s Internet.

Amoroso fulfilled his dream of working at Bell Labs in 1985 and became one of a small group of people who were paying attention to cybersecurity in that decade. He notes that only about 300 to 400 people attended the annual National Computer Security Conference (now the National Information Systems Security Conference) as recently as the mid-1990s.

“At the time, this security discipline was a sleepy sort of thing where you had some hackers and weirdos doing it and people doing cryptography,” said Amoroso. “I loved it because for the first 10 years of my career I was in the lab. I was in bliss.”

Between studying the ills of cybersecurity and the potential cures, Amoroso continues to revel in technology, particularly how it helps him stay in touch with his daughter, who’s away in college.

“I know my daughter’s schedule. I know what kind of day she’s having,” he said. “Now I have instantaneous, ongoing communication with everybody, which is both good and bad, but the point is that the technology bends to fit our lives.”

Amoroso recognizes that just as his focus has shifted over the years from ballistic missiles to even more nuanced warfare, his children’s generation will continue the fight. But his job today is twofold: filling the security gaps created by a technology that has experienced unprecedented and exponential growth while anticipating and warding off new threats in the increasingly mobile world.

Racing for the Advantage

Greg Garcia relies on partnerships in the race to stay ahead of the cyber ‘bad guys’

By Stephanie Kanowitz

Photography by Rich Frasier



Greg Garcia

Greg Garcia is not one to sit and spin his wheels. He thrives on speed, a little danger and the overall chase. So it's little surprise that the bicycling enthusiast gravitates toward the intersection of information technology security and government policy.

“It’s speed, it’s endurance, it’s tactics, it’s strategy, and then there’s the adrenaline,”

Garcia said of IT security. He was referring to the race to stay ahead of what he called the

“bad guys” by anticipating their next move, a race that’s ultimately about safety and protection.

Those elements mimic the thrill he gets from cycling: “To be in a peloton of 50 cyclists, wheel to wheel, shoulder to shoulder, going 30 miles an hour,...the idea of sprinting to the finish and leaving the others behind and jockeying for the advantage, it’s a high-speed chess game. It’s tactical, it’s strategic, and it’s fast.”

Despite his love of competition, Garcia is a man who believes in partnerships. For example, from 2009 to December 2011, Garcia served as partnership executive for cybersecurity and identity management at Bank of America.

The bank has 29 million active online banking customers and handles trillions of dollars a day in financial transactions, many of which are done via mobile devices. Garcia’s background gave him an automatic edge in tackling the public/private challenges of the job: His extensive private-sector experience is complemented by stints on Capitol Hill and at the Department of Homeland Security.

From 2006 to 2009, he served as the first assistant secretary of cybersecurity and communications at DHS. Earlier in the decade, he served on the professional staff of the House Science Committee, where he helped write the Cyber Security Research and Development Act of 2002. The law gave cybersecurity efforts a much-needed boost by providing nearly \$1 billion in federal research funding to colleges and universities.

Along the way, Garcia has held leadership roles at prominent technology associations and his own consulting firm, where he advised companies that want to contribute to the national cybersecurity mission.

Securing ‘Mobile Everything’

Garcia has maintained his cadence in a race without a finish line. He has learned to be proactive and reactive to technology’s constant and lightning-quick evolution. Mobile technology is just the latest frontier. Mobile devices are becoming the preferred mode of communication for many people. As evidence, a recent Pew Internet and American Life Project study found that 87 percent of smart phone owners access the Internet or e-mail via their handheld devices, with two-thirds of them doing so on a typical day. Furthermore, 25 percent of smart phone owners say they mostly go online using their phone rather than a computer.

With the demand for mobile capabilities comes the need for fast-adapting security. Indeed, keeping up with a proliferation of applications and features that have no central owner is one of Garcia’s main challenges.

“What’s developing is mobile everything — mobile computing, mobile identities, mobile banking,” he said. “Many customers are rightfully cautious when it comes to financial services on a mobile platform. But I think the demand will continue to grow. We’ve got to meet that challenge and bring the bank to the customers in ways that are convenient and secure.”

To do it, he uses an old standby — partnerships. At the fundamental level, he said device and software developers need to include security in their frameworks. “We need to continually impress upon vendors that as customers, we demand high security so customers aren’t given devices or apps that are fundamentally insecure,” Garcia said.

"I think we need to be concerned mostly about the kinds of attacks that have the rippling effects that can cause loss of confidence in the Internet as a mode of doing business."

Next, the commercial sectors must work together on cybersecurity. Beginning in 2003, the government called on various industries to work together to protect critical infrastructure and collectively find and eliminate vulnerabilities.

“The financial sector works very well together for one particularly compelling reason, and that is that we don’t look at cybersecurity in competitive terms,” Garcia said. “You might think that’s counterintuitive. Wouldn’t one bank want to say, ‘Hey, we’re more secure. We keep your money more secure than the next bank’? In cybersecurity, it’s not as easy to say that, and it’s because we are all interconnected. Banks realize they are all targets.”

Lastly, industry and the government must join forces. Threats range from hackers who are simply curious to those who are politically motivated, as well as cyber criminals and cyber spies. It's impossible for one entity to monitor them all.

“What everyone should know is that the policy and business as they relate to cybersecurity go hand in hand,” Garcia said. “Because we are in the world of technology and the Internet and security, we're all interconnected, and if we're all interconnected, we're all interdependent. And if we're all interdependent, it means we'd better be working together and collaborating and sharing the kinds of cybersecurity information and best practices that we can deploy to protect ourselves collectively. Information that isn't shared is useless.”

“There is a fundamental understanding that major financial institutions that manage financial transactions over a technology network have a responsibility to partner with, coordinate with, collaborate with the government, with other financial institutions, with other industry sectors to be sure that collectively we're not missing anything, that we're able to join forces and share with each other so we have a common operational picture about what's happening — not just in day-to-day cyberattacks, incidents or probes but what's happening over time,” he said.

The Cost of Safety

Cybersecurity is important to any industry, but the financial sector banks on it; people need to know that their money is safe. With that in mind, Bank of America and other leading banks have instituted \$0 liability protection for any fraudulent activity originating from online banking.

“I'm not concerned that we have something called a cyber Pearl Harbor that's going to break down the Internet,” he said. “I think we need to be concerned mostly about the kinds of attacks that have rippling effects that can cause loss of confidence in the Internet as a mode of doing business.”

“I am concerned about what we cannot see,” he added. “This is where connecting the dots, as it were, in cyberspace is so critically important, where we have the ability of government and industry to share the kind of information that's going to protect us.”

The challenge lies in making that sharing routine and the relationship natural. Garcia said we need to move beyond the past need-to-know mindset and embrace the need to share. “That's a cultural shift more than anything else. It's something that takes time and commitment.”

Of course, cybersecurity requires resources, too, which Garcia says is an ongoing challenge even when budgets aren't tight. “It is often difficult to prove the negative,” he said. To illustrate, he describes a typical conversation: “‘Boss, we invested a million dollars in a security strategy, and we haven't had any cyberattacks.’ And the boss says, ‘Is that because we invested a million dollars or is that just because we were lucky? Prove it to me.’”

To demonstrate the value of cybersecurity, Garcia turns again to joining forces by presenting a plan to managers that compels them to get onboard. “One way to look at it is to go through risk-based scenarios, do the what-ifs,” Garcia said. Once you do that, it’s easy to show that cyberattacks can affect every aspect of a company and its customers.

“I think any reasonable company can look across the threat environment in this country today and say the likelihood of a cyberattack happening against us is pretty good now because it’s proliferating, because it’s big business, because people can buy hacking tools online now. They’re freeware and open source.”

Connecting Government and Industry

Garcia began his career with a focus on business. He earned a bachelor’s degree in international business from San Jose State University in 1985. Interestingly, the school’s motto is “Powering Silicon Valley,” America’s technology heartland.

Ultimately, innovation attracted Garcia to technology, and government service attracted him to security. He joined the House Science Committee a week after the terrorist attacks of Sept. 11, 2001.

“I came into the technology field seeing how government policy, whether it’s legislative or regulatory, can affect the success of business generally and technology innovations specifically,” he said. “I knew early on that I wanted to be at that connect point where I could influence how government thinks about technology and make sure the technology industry was prepared for changes in government policy and that it can contribute to economic growth.”

"What gives me energy are the people who understand that collaboration isn't just a word, it's a path to success."

He spent almost two years working with the Science Committee to promote political outreach to the IT community, but his proudest accomplishment at that time was helping to author and enact the Cyber Security R&D Act.

“I had come from the technology community to the Science Committee to do my part, and the first piece of legislation I ever wrote became law,” Garcia said. “Probably not a lot of congressional staffers can claim that notch in their belt.”

When he left the Science Committee in April 2003, he affirmed that commitment by becoming vice president of information security programs and policy at the IT Association of America. He resigned from that position when President George W. Bush asked him to join DHS.

Cybersecurity Czar

When Garcia was appointed assistant secretary of cybersecurity and communications at DHS in October 2006, then-DHS Secretary Michael Chertoff said, “Greg brings the right mix of experience in government and the private sector to continue to strengthen our robust partnerships that are essential to this field.”

Again, the word “partnership” appears. At first, Garcia felt inundated, but he pedaled through and found his rhythm.

“Shortly after I was appointed, somebody had sent me a link that went around the Internet and somebody had created a video that said, ‘If you were Greg Garcia, what would you do?’” Garcia said. “I actually listened to it and took some advice from these people. There was a big spotlight on me. It was a spotlight I certainly didn’t shrink from, but I rapidly realized that cybersecurity was becoming a very hot topic, and so there certainly was no shortage of federal government agencies that rightly had something to say about it.”

When Garcia took the job at DHS, he became the highest ranking cybersecurity official in the government and was referred to as the cybersecurity czar until Howard Schmidt was appointed cybersecurity coordinator at the White House.

As the first person to hold the position at DHS, Garcia had the opportunity to shape it. Top of his to-do list was — what else? — to partner with government agencies that had a variety of responsibilities, such as defense, diplomacy and law. Chief among his partnership initiatives was the co-called “Einstein” intrusion-detection program that enabled Garcia’s Computer Emergency Readiness Team, or US-CERT, to help government agencies protect their networks from cyberattacks that were increasingly targeting sensitive government data. Garcia also collaborated with the Defense Department’s Joint Task Force for Global Network Operations on threat data sharing and with the Federal Trade Commission on consumer awareness about cyber crime and security tips.

“I think those relationships are evolving within the government,” he said. “We’ve come a long way since the time I kicked it off with DHS, so I have only optimism for the future.”

During his two-plus-year tenure at DHS, Garcia oversaw the National Cyber Security Division, the National Communications System and the Office of Emergency Communications, where he helped establish a National Emergency Communications Plan and 56 plans for federal, state and local first responders.

When he left DHS in December 2008, he e-mailed colleagues at the department: “We have affirmed the urgency of cybersecurity across the nation and embarked on a comprehensive cyber initiative that will measurably strengthen the security of our nation’s networks against domestic and international threats.”

Three years later, he said DHS is still on the right track. “DHS is recognized as the principal interface between the government and industry as it relates to cybersecurity, and they need to strengthen that role and make sure they take leadership in that area,” he added.

After shifting gears between industry and government work, Garcia is happy to be back in the private sector. “I see dedicated people in both worlds,” he said. “What gives me energy are the people ...who understand that collaboration isn’t just a word, it’s a path to success. And I saw it in government, at Homeland Security. There are people who are still there who were on my team at DHS and are still dedicated because they believe in it.”

“We often find ourselves in professions that we fall into, but I love what I’m doing,” he added. “I’m part of something bigger than myself.”

Connected for Battle

Lt. Gen. Susan Lawrence leads the Army's charge to go mobile, secure its networks and protect its information

By Colleen O'Hara

Photography by Zaid Hamid



U.S. Army's Lt. Gen. Susan Lawrence

When Susan Lawrence quit her waitressing job in her hometown of Ida Grove, Iowa, to enlist in the Army, smart phones and network-centric warfare were not part of the common vernacular.

Lawrence enlisted in what was then the Women's Army Corps one week after her 18th birthday, specializing in home economics, typing and shorthand. Today, Lawrence is a lieutenant general and chief

information officer of the Army overseeing a \$10 billion information technology budget.

Throughout her Army career, where she has commanded at every level from platoon to signal command, Lawrence said she has relished challenging assignments. And her current job is no exception.

A Sea Change

The Army is in the throes of a modernization effort that will transform the way it develops, buys and fields new technology. The plan centers on creating a capable, reliable and trusted network that allows the Army to collaborate with anyone anywhere in the world and provide every soldier access wherever they are.

This will be a sea change for the Army, which has been spending time and money on multiple networks that don't talk to one another, data that is hard to access and technology that takes too long to acquire and field, Lawrence said.

"You cannot share information across 30-plus networks," she said. "They are all built differently with different standards with different configurations. We will have to direct the standards, direct the configurations and direct the common operating environment."

The Army, like other government organizations, is being forced to do more with less, which means that it can only afford one networking environment, and that is the LandWarNet. “We’ve talked about it for a long time, but we have never enforced it,” Lawrence said.

Cybersecurity underpins everything in the Army’s modernization plans. It is a challenging opportunity, Lawrence said, because the Army has to balance the need for sharing information with the need for protecting the information.

In Congressional testimony in April, Teri Takai, Defense Department CIO, said that DOD networks are under constant attacks from cybersecurity threats launched from the Internet and malicious software embedded in e-mail attachments or removable media. DOD spends more than \$2 billion a year on information assurance and cybersecurity.

Some of the plans the Army has on tap to counter those threats include enabling constant monitoring of machine-to-machine activity, reducing the number of access points into the network by creating regional hubs, giving each person a single identity on the network so they can access data from anywhere even via a handheld device from the field, and moving data to the cloud.

Constant monitoring automatically flags anomalies on the network, similar to when a credit card company calls to check on suspicious charges on an account. It is easier to monitor five regional hubs, Lawrence said, than it is to monitor numerous access points.

“It takes very little money to attack us in the cyber environment,” she said. “You just need a computer and to be hosted somewhere. So that’s why those kinds of monitoring and architecture reviews are important.”

Data Access from Anywhere

The Army has just finished setting up its fifth regional hub node at Camp Roberts, Calif. Using a suitcase-size satellite terminal, soldiers can connect to one of those regional hub nodes from anywhere in the world and have access to their network and data. Soldiers in Afghanistan are testing droid-like devices that connect to LandWarNet via a secure tactical radio. The devices, which they wear on their sleeves, give them real-time reports and data so they know, for instance, where enemy or friendly forces are.

“Whether it is a squad going out on a humanitarian effort or an entire division in major combat operations, you will connect to the network and your data will be there,” Lawrence said.

Having an end-to-end network also helps the Army maintain continuity in wartime situations. For instance, before the 82nd Airborne Division deployed to Afghanistan, the Army installed the Afghan mission network in Gen. James Huggins’ headquarters, Lawrence said.

“He wasn’t on the tactical network, he was on THE network,” she said. “Every day he had the operational update and the intelligence update, and he knew exactly what his mission was going to be when he landed in Afghanistan because he was part of it every single day.”

Having a single identity on the network makes it easy and safer to access data from anywhere. DOD’s Common Access Card provides that single identity to Army employees and gives them access to their e-mail and other data on the network, no matter where they are located.

The Army is testing a plan to allow users to connect their personal mobile device to the network using the CAC as a means of identification and authentication. Because the Army has embraced virtualized computing, the data is kept in the cloud, not on an individual device or a server under a desk, which improves security.

“You connect to the network, we authenticate it’s you, we scan your device so we can be sure there is no virus or malware on it, and then you have access to your authorized portion of the cloud,” Lawrence said. “At the end of the day, when you unplug, that data stays in the cloud. If you lose your Droid, we don’t care because our data is not there. It remains in the cloud. That will go a long way to securing our information.”

“Disciplining Ourselves into Compliance”

Taking personal responsibility for network security is also essential, Lawrence said. “When you read about our security infractions, it’s almost always because someone did not follow policy or procedures,” Lawrence said. “Disciplining ourselves into compliance is a big part of what we must do in security operations. I am glad we are recognizing it for what it is. It is a warfighting domain; it is a threat.”

Another important effort is under way to introduce new technology such as mobile devices and wireless technology into the Army much faster through Network Integration Evaluations, which take place at Fort Bliss twice a year. During the evaluations, the Army tests products to see if they can fill a capability or technology gap. For instance, at the last test, the Army found a commercial product that solved a radio interoperability problem.

"If we build this environment and it doesn't meet the needs of what our soldiers and leaders need, then we won't get it right."

“We have to acquire IT much faster than we do today,” Lawrence said. “Today we are held under the same standards and regulations for how we acquire a tank or a helicopter, and as we all know, IT turns over every 12 to 24 months.”

How security is incorporated into the network is part of the exercises. “If you think about security as an afterthought, it will never be secure,” Lawrence said. “Security has to be in the design of a product from the very beginning or we won’t achieve what we want to achieve.”

However, all those efforts will be futile without enforcement of a common operating environment. As a result, the Army is directing the LandWarNet architecture and standards “so everybody can’t bring their own products and build their own environment,” Lawrence said.

At one point, the Army had 13 types of handheld devices and 28 network management tools on the network. “When you are trying to put together a network with 28 different network management tools, it’s almost impossible,” she said. The Army also plans to reduce its network applications — mainly old applications — by 30 percent to 50 percent.

Those are lofty goals, and Lawrence knows it won’t be easy. “Sometimes it’s hard for someone to understand, but it will make their lives easier,” she said. “It will make industry’s lives easier if we publish these standards.”

Out of The Comfort Zone

Change comes with the territory. Lawrence has a sign hanging in her office that reads: “Change is good. You go first.” But the Army’s shrinking budget will act as a great motivator. The secretary of the Army has tasked Lawrence to return \$1.5 billion to the Army by fiscal 2015. Where will the savings come from? Enterprise e-mail will give back about \$100 million annually, data center consolidation will return another \$100 million, and enterprise licensing will save millions. This is just a start.

But despite all the efforts to become more efficient, Lawrence points out that in the Army, overall mission accomplishments and effectiveness outweigh efficiencies. “Everything I am doing is not necessarily about efficiencies. It’s about building an interoperable network that can collaborate with our partners and being able to secure our networks and protect our information. The great second order of effect is that we are gaining efficiencies as we’re doing it.”

It’s also important to understand and try to meet users’ needs, Lawrence said. “If we build this environment and it doesn’t meet the needs of what our soldiers and leaders need, then we won’t get it right. They want mobile devices on the network. I hear them. I got it. Now how are we going to do it while securing our networks and protecting our information?”

Being a good listener is important to Lawrence, and she is in constant contact with the senior civilians and colonels “who really run the organization” to get them to think strategically. One of the ways she has learned from her bosses: “They never let me get into my comfort zone. They always pushed me into something bigger and better than just doing my job. Now I say to my team, ‘I will never let you stay in your comfort zone.’”

Every week she asks her young leaders to tell her three things they did to make the Army a better Army. Although it was hard at first, they are catching on, Lawrence said. “I think most of them realized how important they are to our success. If we’re going to be successful in the CIO’s office and do all the things we’ve been asked to do, it will be because of them.”

It's important to share ideas as the Army goes through its changes. "The thing that has been the best for me is my collaboration with my partners in industry, in academia and in the other services. I don't need to learn the lessons again if they already have," Lawrence said. "In fact, I redesigned one of my directorates based on the Air Force and how they look at their enforcement of policies. So the time I spend with those individuals is very important."

Lawrence knows that her job requires perseverance, something she understands intimately.

She has served in operational assignments in Europe, Korea, Southwest Asia and the United States and has held positions in three different divisions, two corps, and now as CIO/G6. During this time, she earned her bachelor of science degree from Campbell University in North Carolina and a master's degree in information systems management from the University of Georgia. She is also a cancer survivor.

When Lawrence was going through her cancer treatments, her team commissioned a mosaic that sits framed in her office. It depicts her life story from when she enlisted in the Army up until she made general.

Still, Lawrence hesitates to take all the credit for her success. "How did I get here? I worked with some fabulous people and I had bosses who had a lot of faith and confidence in me and continued to challenge me," Lawrence said. "As an 18-year-old private at Fort Leavenworth, Kansas, to even dream of being the CIO at the U.S. Army was impossible."

Open Warfare

The VA's Peter Levin believes openness, not secrecy, is the key to mobile security

By Jacob Comenetz

Photography by David Wiegold



VA's Dr. Peter Levin

As chief technology officer at the Department of Veterans Affairs, Peter Levin is responsible for the cybersecurity of the largest medical system in the United States and the second largest federal agency. His job involves helping to facilitate and secure the flow of personal health information among the VA employees at hundreds of hospitals, clinics and offices nationwide, and making that information available electronically to the 21.9 million veterans

and their families who depend on the VA for their medical care. Medical professionals and veterans are increasingly seeking to access that information via mobile devices, which raises new concerns about privacy.

"What the success of Blue Button really is indicative of is not the overall quality or insight of the program, it's the absolute, acute need of people to get access to their data."

Appropriately, Levin has come to think about cybersecurity and mobility in a biological sense, with a focus on minimizing the threat of an intruding antibody.

"You want to surround the threat that you know is going to get in, just like your body knows it will be infected someday, it just doesn't know when and it doesn't know how," he said. "But it has, over millennia, developed an extraordinarily effective response to disease. It's a biological example, but it's a metaphor that translates well to electronic threats in the context of network security."

He has a less-than-conventional vision for creating a mobile, agile VA while ensuring the security of millions of personal records in the cloud and in telemedicine. "My vision is not that we're going to be perfectly secure," he said with characteristic honesty. Instead, he is working to defend against scalable breaches using a "configurable, nuanced, rapid response that's triggered by the detection of intrusion."

That realistic viewpoint is behind the VA's groundbreaking effort to securely add smart phones and tablet PCs to its network. In October 2011, the department issued a request for information for vendors to help build a national mobile device management (MDM) system that would allow at least 10,000 and as many as 100,000 mobile devices running iOS, Android and Windows operating systems to securely connect to the VA's network — the largest such deployment in the federal government.

MDMs manage and protect information from a central location, which VA officials said will be in the cloud for their system. The devices will be managed remotely and provide encryption and reporting capabilities so VA officials can keep track of the devices while enforcing the department's security, management and other policies. The MDM system will also allow iOS devices to connect to a VA app store where users can download applications.

Security Through Openness

As the VA and the veterans it serves expand their use of mobile devices, Levin applies an unexpected twist to secure the software and data they access: He is a vocal advocate of open-source technology development and the open sharing of health data. That perspective is grounded in the knowledge that security breaches happen in large numbers on a daily basis. The VA is particularly vigilant about the issue, given the 2006 breach in which 26.5 million personal records were compromised when a laptop computer was stolen from a contractor's home. The incident led to a re-examination of cybersecurity policies governmentwide and to the VA sending Congress monthly updates on its security efforts.

"Proprietary system are the ones that are inherently more vulnerable because if you think that there aren't people who are trying to break into those systems just as much, you're wrong."

As a result, VA officials including Secretary Eric Shinseki and Deputy Secretary W. Scott Gould have undertaken a big push to shore up the agency's information technology system in recent years. Part of that effort involved naming Levin CTO and senior adviser to Shinseki in May 2009 and increasing his influence, as well as that of Chief Information Officer Roger Baker, who is responsible for the agency's operational IT requirements.

Those moves have borne results. In September, Levin was justifiably proud that President Barack Obama had publicly referred to three breakthroughs in which Levin had played a key leadership role: the Blue Button program, which gives veterans access to their health information and allows them to share it with doctors outside the VA; the progress being made on processing a backlog of claims, some dating to the Vietnam War, via an innovation competition; and definitive steps toward the long-standing goal of creating a single electronic health record (EHR) for military service members to be shared between the Department of Defense and the VA.

Still, Levin knows that plenty of work remains. For example, the VA is enabling the 134,000 medical professionals who work at 152 VA hospitals to securely access patient records using mobile devices and cloud-based applications through a groundbreaking initiative Levin led: a platform for improving veterans' EHRs called the Open Source Electronic Health Record Agent. The system's underlying principle is in keeping with what Levin said is a key tenet of his approach to cybersecurity: Open-source development offers the fastest, safest and most transparent way to accelerate progress.

"The reason you do open source is because you level the playing field," he said. "You make it completely transparent, and you make it so anyone can participate. Those three factors, combined with a standards-based, openly architected, modular system, will keep you on the cutting edge."

Public Servant, Private-Sector Mentality

Levin relishes the challenge of balancing openness and security. After all, he has built a career on doing the unexpected. The Washington, D.C., native didn't have much interest in school until he realized he was better at math than he thought. He went on to study electrical and computer engineering at Carnegie Mellon University, conduct post-doctoral research at the Technical University of Munich, and eventually become associate dean for research at Boston University's College of Engineering. Today, he is a consulting professor of aeronautical and astronautical engineering at Stanford University.

Along the way, he spent many years as a successful tech entrepreneur in the private sector, including the semiconductor industry, which lies at the heart of all computerized technology.

Levin has never taken the easy road. At Carnegie Mellon, he wrote a simulation program for electromagnetic field theory, which, for most people, is the least enjoyable part of an engineering curriculum, he said.

"So, of course, that's what I wanted to do," Levin said. "The thing that nobody wanted to do is what I absolutely had to do."

That drive paid off. Working in collaboration with Professor Jim Hoburg, Levin wrote a program that attracted the attention of Hans Steinbigler, a pioneer in the field of simulation programming. Steinbigler invited Levin to do his post-doctoral research in Germany.

After completing his studies, he went into private industry, where he was founding chief executive officer of the cybersecurity software company DAFCA Inc. and executive director of Astaro, an Internet security company based in Karlsruhe, Germany. Shortly before joining the VA, he co-founded and led an award-winning semiconductor software design company and was a partner in a venture capital firm based in Dusseldorf, Germany.

It was serendipity that brought Levin to the VA. In 2008, he escorted a close friend who was receiving an award at the White House and met James Peake, then VA secretary, in the Green Room.

“I asked a question about the lack of telemedical services offered,” Levin said. “It happened to be on my mind.”

Shortly after Obama won the presidential election, Levin got a call from Peake asking to meet with him. After learning everything he could about telemedicine and distilling it into a few PowerPoint slides, Levin went to the VA headquarters in downtown Washington, D.C., for the first time.

“I had to look it up on a map,” Levin said. “I had no clue where it was. I had never served in uniform. What do I know about health care delivery? I’m a semiconductor guy.”

The opportunity Peake offered was one Levin couldn’t pass up.

“You can imagine my grandmother’s small apartment in Forest Hills, with the gold-framed iconic picture of Franklin Roosevelt,” Levin said. “Math and science were an expedient way to education, to make money. But I still believe that the best thing you can do is care for the public interest.”

That lifelong affinity for politics and government has found expression in the CTO position, where Levin guides improvements in veterans’ health and benefit services “by promoting a deeply collaborative culture, renovating business processes and leading the development of new technology platforms,” he said.

Going for the Layups

Levin arrived at the VA in June 2009 with a strategy for establishing leadership early on. In close cooperation with the secretary, deputy secretary, chief of staff and CIO, Levin decided to go after the “layups.” Inspired by the strategy Peter Sims outlines in his book “Little Bets: How Breakthrough Ideas Emerge from Small Discoveries,” Levin wanted to build momentum for transformational change by systematically taking small, exploratory steps and being open to new ideas along the way.

“He wrote down my playbook,” Levin said of Sims. “It’s exactly what I did and still do — not try to boil the ocean or solve every problem in the first two weeks.”

Levin said his first layup was not in an area his bosses expected. “For personal reasons, I was keenly focused on suicide prevention,” Levin said, referring to the fact that he lost many family members to the Holocaust and knows that survivors and their descendants have high rates of suicide, divorce and mental illness. “For me, that was a place where a morally transcendent

problem met personal interest, met the opportunity to actually do something meaningful and worthwhile quickly.”

He proposed augmenting the Veterans Crisis Line with an anonymous online chat service for veterans who didn’t feel comfortable talking on the telephone. One month later, the service was a reality.

“With Roger Baker’s help, we got that stood up quickly, and today we have had more than 3,000 interventions,” Levin said. “It’s hard to say how many would have led to tragedy, but I bet it’s more than one. In my faith tradition, if you save one, you save the world.”

Acute Need for Data

After that, Levin turned to what he describes as an “almost trivial project called Blue Button” — a Web-based feature that allows patients to download and share their health information with health care providers, caregivers and others they trust. Blue Button is a collaborative effort with the Department of Health and Human Services’ Centers for Medicare and Medicaid Services, DOD and the Markle Foundation, a private, not-for-profit philanthropic organization.

Many colleagues advised Levin against confronting layers of bureaucracy and red tape to unify data from different platforms in a single, accessible, user-friendly format. But Levin feels strongly that veterans should be able to access their data, and he said he won approval from the secretary to “just try to drill a hole through the fortress.”

Levin told Shinseki he’d have 20,000 to 25,000 users within a year. “He looked at me kind of sternly and said, ‘That’s a big number. Just make sure you hit it,’” Levin recalled. Blue Button had 25,000 users within six weeks.

Since launching in October 2010, the system has attracted more than 500,000 users and has been adopted by major health insurance companies such as Aetna and UnitedHealth Group. Still, Levin insists that Blue Button is merely a good platform that “a freshman at any junior college could have come up with.”

Others view it less modestly. At a recent Consumer Health IT Summit sponsored by the Department of Health and Human Services, Dr. Donald Berwick, administrator of the Centers for Medicare and Medicaid Services, called Blue Button “iconic and magical.”

“What the success of Blue Button really is indicative of is not the overall quality or insight of the program,” Levin said. “It’s the absolute, acute need of people to get access to their data, and that’s why you’re seeing it run like this.”

The program is revolutionizing the approach that has been in place since 2004 when HHS’ Office of the National Coordinator for Health IT proposed a national infrastructure that would let health providers share information.

The office's model is "institution to institution or provider to provider, and Blue Button shows up frankly as an idea that nobody thought of," Levin said. "What about the voice of the patient? What about the patient's access to data? What we're discovering to our delight is that patients want to be involved."

Blue Button downloads health information in a simple text file or enhanced PDF that can be read, printed or saved on any computer. Implementing it raised several security concerns, however. Because thousands of veterans would be downloading their personal health data via mobile devices, Levin used encryption technology to protect the data as it moves between VA's secure MyHealthVet system and other data assets. That way, any breach that might occur would at least be containable.

Levin acknowledges that favoring transparency comes with risks. "There were folks who were nervous about it, and there are still plenty of them," he said. "They're jittery for a reason, but that was the choice we made."

It came down to a fundamental policy choice. "Are you going to give them the information that they asked for, even if there's a cybersecurity risk, which you can train them to remediate or at least to lessen?" he asked. "Or are you not going to give them the info and tell someone who carried a gun in your name, who shot bullets to defend your liberty, that you are not going to have access to your information because we don't think you're smart enough to keep it private?"

The argument proved compelling, Levin said.

"More Eyes, More Brains, More Secure"

As recently as three years ago, the VA did not have a Facebook page or a Twitter account for keeping in touch with its constituency. Today, the department's Facebook page is one of the most popular in the federal government, with more than 143,000 friends. Levin often reads the comments to keep tabs on how people perceive his work.

In one case, intuition told him that a veteran was in trouble, and he decided to reach out to the man from his private e-mail account. The man replied, and the two have become close correspondents.

"To make a long story short, we write to each other very often, and I rely on him for a lot of things, not the least of which is to tell me what's really going on," Levin said. "How does a Vietnam-era veteran see the things that I think are so transformational, so earth-shaking and important that I interrupted my career, moved my family, and maniacally, obsessively devoted myself to the care of veterans?"

Looking forward, he plans to forge ahead with his open-source plans, a term he says is misleading. "It implies that because the code is exposed, you're inherently more vulnerable to

hackers exploiting something that you haven't discovered yourself. And what is scientifically known, well-studied, quantified and stress-tested is that exactly the opposite is true. Proprietary systems are the ones that are inherently more vulnerable because if you think that there aren't people who are trying to break into those systems just as much, you're wrong."

Levin sees open-source development as an important way to anticipate and defend against the unexpected in the ever evolving mobile frontier. "Open source has the added advantage that you've got a lot of people looking at it at the same time," he said. "It really is a blunt-instrument argument: more eyes, more brains, more secure."

Global Cyber Sleuth

The State Department's Chris Painter relishes his role as a cyber diplomat

By Colleen O'Hara

Photography by Zaid Hamid



State Dept.'s Chris Painter

From tinkering with an old Amiga computer in college to prosecuting one of the first computer hacking cases in the country, Chris Painter's life has always revolved around computers and technology.

Painter has even adorned his office walls with posters from science fiction movies that

involve hackers on the run, espionage and computers taking over the world. He said the

posters "highlight for visiting diplomats and industry leaders the popular misperceptions of computers."

In real life, he plays the leading role in implementing the United States' International Strategy for Cyberspace, a task that most people would find formidable but one that Painter finds exciting.

"This is not a subject for governments alone, but will require close collaboration with the private sector."

As the first coordinator for cyber issues at the State Department, Painter is on the global stage partnering with other countries to create a more secure, reliable and open Internet. His focus encompasses the security of mobile devices, which are being used more and more around the world and are just as susceptible to attack as more traditional computers, Painter said.

"It's an international problem that will require international collaboration among governments and other stakeholders," he said.

Painter's current role is a natural progression in a professional journey that started 20 years ago as a federal prosecutor tackling some of the earliest cybersecurity cases.

Back then, cybersecurity "really didn't get any kind of higher policy attention," Painter said. "Cyber crime did to some extent. Law enforcement, in many ways, was a bit ahead of the curve because they were facing actual intrusions, but even they hadn't organized around it."

Times have changed. Now, cybersecurity is a priority for people at the highest levels of government, particularly as new mobile technology makes it easier to connect with the world. Painter's boss, Secretary of State Hillary Rodham Clinton, has said it is a foreign policy imperative to ensure a free and open Internet and the international community needs to have a serious conversation about the principles that will guide us in maintaining an Internet that benefits the world.

Painter is uniquely qualified to facilitate that conversation because his career has mirrored the rise in prominence of the Internet and the now global implications of cybersecurity. From his work prosecuting famous computer hacker Kevin Mitnick and other cyber criminals to his role at the White House as senior director for cybersecurity policy, Painter has been one of the United States' lead actors in a real-life cybersecurity thriller.

Before he left the White House to join the State Department, he helped develop the International Strategy for Cyberspace. Although it started as the "creative cacophony" of 18 agencies in a room, all voicing their perspectives on cyberspace issues, over the course of a year and half, it coalesced into a unified framework for all cyber issues, including cybersecurity, Painter said. "Everyone had great ideas, but they weren't meshed up. Putting this under one strategic framework was important and a huge accomplishment and something no other country had done."

The experience broadened his view of the issues. "One of the things I recognized as we were writing this international strategy is you can't look at cybersecurity in these narrow silos," Painter said.

"Cybersecurity is critically important, but if you don't look at it in the broader context, it will always be seen as a niche issue and a technical issue. It will always be seen as a cost, and people won't understand the benefit."

Eye on Mobile Security

Many countries have already reacted favorably to the International Strategy for Cyberspace, a 25- page document that "outlines not only a vision for the future of cyberspace but an agenda for realizing it," as President Barack Obama said.

Although it is a U.S. strategy, it's meant for the world. Painter said the United States wants to expand the dialogue beyond its traditional allies to those in the developing world, where many people, especially those in poor and rural areas, missed the personal computer stage and went straight to mobile phones. From 2005 to 2010, cell phone use tripled in the developing world to nearly 4 billion mobile subscriptions, according to the International Telecommunication Union. And many of those people are using the phones to access the Internet.

So naturally the International Strategy for Cyberspace will accommodate the growing use of mobile technology. "It took us a long time even in this country to care about these issues, and

there is still a lot of work to be done,” Painter said. “Developing countries can learn from what we did right and also from our mistakes.”

It has only been in the past few years that the United States “has realized at a senior level that security is important to enable all the positive economic and social benefits that new technologies afford,” Painter said. “As other governments, particularly in the developing world, are facing some of these issues for the first time, they have an opportunity to approach this problem from a holistic standpoint and make sure that innovation and social growth are empowered by more secure systems.”

With that in mind, in July the State Department partnered with the Justice and Homeland Security departments and the government of Kenya to host a seminar in Kenya for five east African countries on issues related to cyber crime, cybersecurity and Internet freedom.

As part of that effort, Painter has traveled to Kenya twice in the past few months and has seen firsthand how mobile use is evolving in that part of Africa. For instance, Kenya has an innovative payment system that allows people to pay bills and make purchases by transferring money electronically via their cell phones. It’s akin to swiping a credit card, but it’s revolutionary for people who might never have had a bank account before.

“It’s not just large countries that get innovative and profit from this,” Painter said. “This is the wave of the future.”

Given the growth and penetration of mobile devices and mobile broadband, security is as important as it is in the desktop PC world, Painter said. “Those platforms are just as susceptible to compromise and attack. This is not a subject for governments alone but will require close collaboration with the private sector so, to the maximum extent possible, security can be baked in instead of added later.”

On the Case

Painter has always had an interest in computers and is a self-professed early adopter of technology. As an undergraduate at Cornell University, he studied literature, political science and biology. He balanced reading James Joyce, programming Fortran, and studying differential equations and chemistry.

After he earned a law degree from Stanford University, he went to work at the Ninth U.S. Circuit Court in Seattle as a law clerk for Judge Betty Fletcher, who he said has been at the forefront of many cyber issues. He later worked at law firm Arnold and Porter in Washington, D.C., where he handled technology, cable television and satellite issues.

In 1991, he moved to Los Angeles to work as a federal prosecutor. As an assistant U.S. attorney, “you get fascinating cases like people robbing banks with their name tags on — not the smartest criminals,” he said with a laugh. “But at the same, there were some high-tech cases

going on, which I gravitated to. Frankly, there weren't a whole lot of people who understood or cared or wanted to get involved in that."

"We could find opportunities to work together with other nations to realize a positive vision of cyberspace."

In one of the first hacking cases to gain widespread media attention, Painter helped track down and prosecute Kevin Mitnick, who had hacked into the networks of major technology companies and Pacific Bell's voice mail computers, among other crimes. Mitnick eluded capture for two-and-a-half years until he was finally arrested in North Carolina in 1995 and eventually confessed to wire fraud and computer fraud as part of a plea deal.

Painter said what he learned from the Mitnick case is that "there is no shortage of individuals and groups who would seek to exploit vulnerabilities in our broadband and mobile systems. That requires unprecedented coordination and international cooperation to address those threats."

He also helped prosecute the first Internet stock manipulation case in which an individual created a fake Bloomberg page with false tips that a company was about to be sold, causing the stock to rise by 30 percent. In 2000, when distributed denial-of-service attacks took down Yahoo, eBay, Buy.com and other sites, the case, which Painter also worked on, captured public attention because people were becoming more dependent on computers.

"You still had this dichotomy of people thinking, 'This is kind of cool,'" Painter said. "They didn't really see how it harms them, so it's not like it is today."

The attacks were traced to a teenager in Canada, which meant working with authorities on the other side of the border to apprehend the culprit.

The international aspects of the case sent Painter down a new path professionally. From Los Angeles, he was working closely with the chief of the Computer Crime and Intellectual Property Section and others at the Justice Department, Painter said. "Then I decided to come back to the 'mother ship' at Justice and help run that section for a number of years and get more involved in the international activities there."

As part of those activities, since 2002, Painter has chaired the G8 High-Tech Crime Subgroup, where he has worked with dozens of foreign governments.

After a stint as deputy assistant director of the FBI's Cyber Division, Painter served in the White House as senior director for cybersecurity policy on the National Security Staff. During his two years at the White House, he was also acting cybersecurity coordinator before Howard Schmidt was named to the post and was a senior member of the team that conducted the Cyberspace Policy Review that Obama commissioned shortly after he took office.

At a Cyber Crossroads

In February 2011, Clinton hired Painter to create and lead the new Office of the Coordinator for Cyber Issues at the State Department, where a key part of his job is changing the perception of cybersecurity and other cyber issues from purely technological to mainstream policy issues.

“The key to convincing senior leaders to invest in cybersecurity is weaving it into the broader context of a business or the government,” Painter said. “This isn’t something that should be discussed in the dark techno-corners, it’s something that should be discussed across the board. My office is deliberately supposed to look at the whole suite of cyberspace issues so we can realize a positive vision of cyberspace — for which cybersecurity is one supporting part.”

Painter added that we are at a crossroads where we must choose how to deal with the darker side of cyberspace. “The question is: Are we going to have an Internet that is open, secure and reliable that will enable growth or will we have something different?” Painter said.

“The things you are trying to enable are social growth, Internet freedom, open communication, and economic innovation and growth,” he added. But for those efforts to succeed, people must feel secure when communicating or conducting business in cyberspace. In other words, they must feel safe from crime and intrusions into their privacy.

“We have to balance usability with security of systems,” he said. “If you have security that is so overwhelming you can’t use the systems, they’re worthless to you. If usability is king and you never think about security, then in the long run, that usability is going to be undermined.”

He emphasizes that technology can have a transformative effect and a natural evolution that countries shouldn’t stymie. “It could lead not only to democratization and social growth, but also to economic growth and innovation.” Nevertheless, “we have to be cautious as we go forward. There are some states that find that openness threatening.” Working with those countries will require patient, persistent diplomacy, he said.

Widening the Aperture

To achieve the international strategy’s vision, collaboration among government, industry and non-governmental organizations is vital, Painter said.

“Governments have to develop a culture of working with industry,” he said. “It’s second nature in the U.S., but it’s not the case in the rest of the world. You really need that. It’s not just one group of actors that will control this.”

The U.S. has worked collaboratively in multiple areas to enhance cooperation on international law enforcement and to combat cyber crime. One example is in the Organisation for Economic Co-operation and Development’s principles for Internet policy-making, which “reflected the

input of governments, the private sector and civil society, and as a result was a far more inclusive and stronger document,” Painter said.

It is also important to bring the technical and policy communities together — two groups that are not necessarily used to dealing with each other.

Painter said that when DHS drafted its National Cyber Incident Response Plan in 2009 to establish a comprehensive approach to natural and man-made disasters, it was built from the beginning with private-sector involvement. “It was a much more inclusive process,” Painter said. “That changed the dynamic where people felt like they had a stake in it.”

Fortunately, the increased focus on cybersecurity has prompted agencies to get together more often, Painter said. “The fact that there are frequent discussions at a high level with various interagency aspects to them means that people are more comfortable with each other,” he said. “Communication between agencies and coordination between agencies is far better than they have ever been.”

At the State Department, Painter’s office formed a cyber coordination group whose members come from all over the department and have experience working with countries all over the world. That shared expertise is invaluable in broadening awareness of the sweep of issues that cybersecurity affects. When the International Strategy for Cyberspace was released in May, Painter sent a cable to State Department posts worldwide asking that posts talk to their host governments and identify the officials who were tracking cyber issues in those countries so that cyber points of contact could be designated.

“Through this engagement, we could find opportunities to work together with other nations to realize a positive vision of cyberspace — an open, interoperable, secure, and reliable information and communications global infrastructure,” he said.

“We’re trying to work with other governments to see what we can do together,” Painter said. “We need to be smarter about the way we organize. Many stakeholder groups are doing good work but not coordinating it. By working together, we can amplify each other’s message.”

That’s especially important in these times of economic uncertainty. Everyone is facing limited resources, which means we need to prioritize, find creative solutions, partner with other government agencies and share information better, Painter said. In short, financial constraints are forcing agencies and countries to collaborate more. “That’s ultimately the right solution anyway, so it’s good people are being driven that way,” Painter said.

His experience working with people from all over the State Department, the government and the world has been “a widening of the aperture in my career,” Painter said. “I feel very lucky to be here at the State Department and to have that expanding view, and there is some benefit to having done this as long as I have because I can look back and say, ‘Here is how things have changed.’”

“Not that we’re close to being finished,” he added. “We still have work to do.”

Now it’s up to Painter and his team to help achieve the long-term goal of what the Internet and cyberspace will look like, and playing a leading role in the challenge suits him just fine. “I am far happier to be in a position where I can engage in this now than to be on the outside looking in,” he said.

Running the Rapids

DHS' Greg Schaffer steers organizations through the cyber whitewater to secure federal systems and national infrastructure

By Colleen O'Hara

Photography by Stan Barouh



DHS's Greg Schaffer

It used to be relatively easy for Greg Schaffer to carve out some time in his week to kayak or row and enjoy some time on the water. These days, however, most of his time is spent helping organizations navigate the choppy waters of cybersecurity.

As assistant secretary for cyber-security and communications at the Department of Homeland Security, Schaffer helps organizations safeguard and secure cyberspace at a time when cyberattacks are increasing and the use of new technology such as mobile devices is on the rise.

A lawyer by trade with an abiding interest in technology and a bad case of “early adopter’s disease,” Schaffer got involved early in his career with computer-related cases. Back in the 1990s, when almost half of his time was spent on cyber-related legal issues at the law firm of Manatt, Phelps and Phillips, Schaffer said it was clear that things were going to change.

“We predicted that as the economics started to be driven by this new thing called the Internet, so would go crime, so would go espionage, and so would go so many other things,” he said. “And that’s exactly how it has played out over the years. The more society leverages this technology to do good things the more those who would do us harm leverage this to do what they do.”

When Schaffer became a computer crime prosecutor in the Computer Crime and Intellectual Property Section at the Department of Justice in 1997, he became immersed in cyber crime full-time. Every day he witnessed the constant and persistent threats and intrusions — some known and some unattributed — aimed at federal and private-sector systems.

At DHS, Schaffer works to counter those threats by helping federal civilian agencies secure their computer systems and helping the private sector safeguard the nation’s critical infrastructure, such as utilities and financial and telecommunications systems.

DHS' programs include consolidating the number of external connections federal agencies have to the Internet and deploying intrusion-detection capabilities at those points. Also, through the National Cybersecurity and Communications and Integration Center (NCCIC) and U.S. Computer Emergency Readiness Team (US-CERT), it works to identify threats with the public and private sectors and develop effective security responses. The world of cybersecurity can be murky, and threats are coming from many different places, Schaffer said. "We find ourselves now with a threat picture that looks like society writ large." There are petty criminals who aren't very sophisticated but can get access to the tools that allow them to commit various intrusions and crimes, Schaffer said. There are so-called hacktivists who use technology to push a political agenda. There are more sophisticated criminals who are focused on following the money, whether it's through stolen identities or cash stolen through credit card numbers or bank accounts. Sophisticated nation-state actors could also potentially conduct espionage, attack intellectual property or do harm to the national infrastructure, he added.

Facing multiple domestic and international threats, DHS and the Department of Defense established a memorandum of agreement, cleared for open publication on October 13, 2010, "to collaborate to improve the synchronization and mutual support of their respective efforts in support of U.S. cybersecurity."

The threats "really run the gamut," Schaffer said. "You can't talk about this space as having a threat actor or a set of threat actors. You have the whole range of misbehavior that you see mirrored from the physical world happening in the cyber world."

And while newer technology helps us do our jobs better, there can be a downside from a cybersecurity perspective. As the use of mobile devices, networks, cloud computing and other technologies rise, not surprisingly, so too do the number of cyberattacks launched against government and private networks.

"I think for IT and security professionals everywhere the pressure to stay ahead is enormous."

In fiscal 2011, US-CERT responded to more than 100,000 incident reports and released more than 5,000 actionable cybersecurity alerts and information products, said DHS Secretary Janet Napolitano at a conference sponsored by the Washington Post in October 2011. Attacks are increasing in complexity, frequency and consequence, she said, adding that we've come close to having a part of the critical infrastructure shut down.

Assessing Risk

Schaffer is not averse to risk. Before joining DHS, he was senior vice president and chief risk officer at Alltel Communications, where he was responsible for logical security, physical security, internal and external investigations, fraud, law enforcement relations, privacy, and regulatory compliance.

For four years before joining Alltel, Schaffer was a director at PricewaterhouseCoopers in the Cybercrime Prevention and Response Practice, where he developed and implemented computer forensic examinations in connection with major internal investigations at Fortune 500 companies.

Assessing risk is one of the most difficult challenges in cybersecurity, Schaffer said. “It’s fairly easy for organizations to get a handle on their physical security. It’s much harder to do that on a network. People don’t necessarily know the value of their intellectual property or their digital assets. And networks change and evolve so quickly that it is extremely hard to know which part of this behemoth to focus on.”

Staying Ahead of the Mobility Curve

There is no denying that mobile devices are here to stay as part of the threat equation, said Schaffer, who is the proud owner of a BlackBerry, an iPhone and an iPad. But “people are just starting to realize what the impact of mobile really is on their networks.”

Mobile devices allow users to operate in spaces that they never could before — on a bus, in a coffee shop or at a park — but those environments are not typically as secure as the office enterprise network. “You’re connecting to networks over which you have less control. We roam about with these devices, and they have Wi-Fi capability and cellular capability and Bluetooth capability and location identification. There are a range of things these devices can do, and the applications are doing all kinds of things with your data potentially in the background.”

With the growth of mobile applications, most people are starting to see their work and private lives comingle. “I have a 9-year-old and a 12-year-old, and they are pretty convinced that that iPads and iPhones are gaming platforms,” Schaffer said. “People are no longer keeping separate those things that they do for business and those things they do for pleasure, and again that creates certain risks. I am pretty careful not to do that, but I don’t think everyone goes down that same road.”

"You have the whole range of misbehavior that you see mirrored from the physical world happening in the cyber world."

Once users start putting both business and personal data on a single device, there are a range of security issues to consider. For instance, what if the device is left on the backseat of a taxi? What if there is a lawsuit and the device is part of a personal legal matter? “Now you have suddenly exposed the other side whether it’s the personal side or business side to some kind of legal process simply by having it all comingled on the same device,” Schaffer said.

The technological challenges of those devices, he added, are that “they are evolving so fast and the application space is evolving so fast that it is hard to keep up and secure things in the

demand curve that has been created. So I think for IT and security professionals everywhere the pressure to stay ahead of that is enormous.”

So how do organizations keep their data safe as the use of mobile devices increases? The guidance in many cases is awareness, Schaffer said. “It’s making sure that people really understand what they are buying into when they connect certain things to this ecosystem,” he said. “Having people who really understand what these challenges are and how careful they need to be is one of the things we spend a lot of time doing. We do that through training, awareness programs and education programs.”

Getting Cloud Security Right

The same goes for cloud computing, which allows agencies to make their data accessible from anywhere, even via a mobile device. That poses new risks that need to be mitigated, Schaffer said, but if those risks are appropriately addressed, cloud computing can be done in a secure way.

“Indeed, by aggregating and having a single place where you can deploy strong security measures for many entities, you may be able to do security more efficiently and effectively in a well-managed secure cloud than, say, 100,000 small businesses might be able to do on their own. The same is true for small departments and agencies within government.”

It’s very important that users ask the right questions before moving to the cloud, he said. A poorly secured cloud makes an organization extremely vulnerable because many assets are aggregated in a single place. They must be sure their cloud provider has the appropriate controls, defines different levels of security to be deployed, and provides important data such as log and audit files if a breach occurs.

DHS supports the governmentwide Federal Risk and Authorization Management Program, which is designed to help agencies to move to the cloud by providing a standardized approach to assessing and authorizing cloud providers.

It is another way DHS helps federal agencies “get their security right,” Schaffer said. “We will also put boots on the ground to assist someone during an intrusion or as preventive work to help them make sure they are ready for any problems that may occur in the future. We are able to do some red-teaming with government entities to give them a sense of how things are working or not within the security regimes that they have put in place.”

Cyber Hygiene

Schaffer drives home the message that cybersecurity is a shared responsibility that we are all going to have to deal with. The more people who engage in and deploy solutions for cybersecurity, the better off we will be because this will help lower the cost, Schaffer said.

“This is like a public health issue,” he said. “If we are not all washing our hands, a significant portion of us will get sick and it will cost us more. The goal here is really to get to a baseline level where we are all more secure than we are today. Caring is a self-fulfilling prophecy in certain cases. What we really need is for the baselines to come up.”

Legislation introduced by the White House in 2011 and currently before Congress would help DHS further its cybersecurity agenda. The legislation would give DHS tools it needs to secure the nation’s most critical infrastructures, close potential gaps in DHS’ patchwork of cyber authorities, strengthen criminal penalties, make it easier to share cyber information, and enhance the agency’s work with the private sector, among other things.

In addition, DHS has been given temporary direct-hiring authority from the Office of Personnel Management and seeks permanent, additional hiring authorities in its legislative proposal to continue to build its cybersecurity workforce. It also now leverages some of the National Security Agency’s resources to help develop intrusion-detection technologies that will prepare alerts for the private sector to create patches and workarounds when needed, Napolitano said in October.

Much of what DHS does requires cooperation and collaboration with other agencies and companies. Fortunately, Schaffer said that in the past 15 years, it has gotten easier to do. “It’s not perfect, but it’s better,” he said. “I think there is a recognition of how important this is. I think departments and agencies have worked together on some serious intrusions over the years that have really educated them.”

Also, there is now a National Cyber Incident Response Plan that delineates what the roles and responsibilities are for many of the players and “gives the DHS a responsibility to play that central hub and aggregation and distribution point for incident response.” The 24/7 NCCIC provides a common operational picture for government agencies as well as the private sector. “It puts people in a position to feel a higher level of confidence that they have the data they need in order to execute well when things are happening.”

As agencies and business owners become more engaged in the risk management process, there will be a much greater emphasis on cybersecurity than there has been in the past. “There will be a recognition that these are enormously valuable assets and the only way I can protect them is to make sure we’ve got the right solutions in place,” Schaffer said. “And that will be good for everybody.”

Chain of Security

Teri Takai is shaping policies to strike the balance between taking advantage of mobile devices and securing the supply chains that deliver them

By Jacob Comenetz

Photography by David Wiegold



DOD's Teri Takai

For Teri Takai, the key to overseeing cybersecurity for the world's largest defense organization is striking a delicate balance between enabling mobility and safeguarding information that is often crucial to national security. In her role as the Department of Defense's chief information officer, she must also convince a widely diverse group of constituents that a shared approach is best.

DOD has always had a highly mobile workforce, but the proliferation of mobile devices is radically altering the department's already challenging security environment. On the one hand, mobile technology offers immense potential for gaining a tactical edge in military operations. For instance, the Army is deploying troops to battle zones armed with smart phones and is developing specialized mobile applications for a wide range of functions. On the other hand, the security risks have never been greater, with public, commercial and military digital assets under constant attack.

"What we're looking at right now is: How do we set policy that allows for uses where mobile technology actually makes sense, and which is also restrictive enough so that people don't go out and buy just anything?"

Because there is no single method for using commercial mobile devices in military situations, Takai is considering multiple approaches. In the past, the Pentagon typically developed proprietary technology with built-in security and other requirements. But now mobile devices are blurring the line between personal and professional activities, and something as innocent as an employee wanting to check work e-mail from a smart phone can have unexpected security consequences. As a result, DOD increasingly has to work with partners outside the defense industry to ensure security.

“Now we’re faced with a very different dynamic, which is commercially available devices that were not built for defense being introduced into our network,” Takai said. “That’s been a real challenge for us.”

Balancing Flexibility and Security

Takai’s team has formed a working group to create policies for using mobile devices “not because people are going to do something intentionally wrong,” she said, “but because they won’t appreciate the threat and the risk of these devices.”

The Commercial Mobile Device Working Group, which includes representatives from the Army, Navy, Air Force, and other agencies, is developing policies to cover the full range of security requirements, which must be especially rigid with regard to classified information.

“What we’re looking at right now is: How do we set policy that allows for uses where mobile technology actually makes sense, and which is also restrictive enough so that people don’t go out and buy just anything?” she said.

“We put out one policy that actually started down the path of saying, ‘Here are the things to think about,’ or ‘Here are the things that you have to consider as you’re deploying.’ We have a second policy that’s in the works that’s the next level of being restrictive, to be prescriptive about what devices you can use that are not connected to the network but that have the capability to display information,” she said. “What devices can you use if you’re using unclassified information, and then what devices do we need to have in our classified environments?”

The key is finding equilibrium between users’ need for flexibility and DOD’s need for security. “The challenge is that as we push down the ability to make the decision on whether you can use a device, it’s very difficult to say when somebody will thoroughly think through the ramifications of making a bad decision,” Takai said. “The farther down you push it, folks are going to be more focused on the operational need than the security.”

Forging the Supply Chain

Takai is also working on the processes that DOD uses to certify commercial devices for military use, including how officials might investigate supply chains to understand what is embedded in the software and hardware of weapons systems.

Takai brings deep experience in managing complex supply chains to the DOD’s challenge. As part of her 30-year career at Ford Motor Company, she served as director of supply chain systems responsible for coordinating a massive worldwide network of parts suppliers, e-commerce exchanges, production lines, and dealers. After Ford, she also served as managing director of global supply chain for EDS and worked with Federal-Mogul Corporation, a global supplier of automotive supplies and systems.

Now at DOD, she is exploring the Pentagon's relationships with the producers of mobile devices and the software that runs on them. Before the department will allow employees to use mobile devices, providers must modify them to meet DOD's security requirements.

The supply chain "is very big in terms of our thinking," Takai said, because DOD can't "legislate" companies to protect their supply chains.

She has three approaches to supply-chain management. The first is traditional: ensuring that threats don't have an entrée through components in weapons systems. To address that, she's looking to partner with technology companies worldwide.

"We have to partner with those private-sector companies," she said. "We can't, if you will, proceduralize them to protect their supply chain. We've got to work with them. That's No. 1."

Second, DOD is pilot testing processes, particularly in major defense acquisition programs, to see how officials can study the supply chain to understand what's embedded in the software, hardware and weapons systems the department uses. For several years, DOD has partnered with the Department of Homeland Security on the Defense Industrial Base Cyber Pilot. The project allows DOD to share information on threat intelligence with defense contractors and commercial telecommunications providers. By doing so, DOD aims to protect its assets by protecting those of its private-sector partners.

"The third piece that we're beginning to look at is that going forward, there will be a certain amount that we cannot detect," Takai said. "So we're working very hard on what we call resiliency. Understanding that there will be some level of breaches, how do we react to that, how do we ensure that that does not damage our ability to carry out our mission? I think that's going to be a growing area going forward."

Getting to the Right Answer

Takai admits that the transition from her role as California's CIO to her new federal role — where she oversees an IT budget of nearly \$33 billion and must contend with a range of organizational cultures — has involved a steep learning curve.

"Folks in DOD will laugh when they hear me say it, but things really do take a lot longer," Takai said. "Every time I look to make a change, I find some rule or process that I didn't know that I had to go through."

And one difference between being the DOD CIO and a state CIO is that "when you're in state government, you're actually much more citizen-focused because you're just closer to the citizen," she said. "You're very focused on how to help provide technology services that impact the citizen directly."

At DOD, “that’s the least of my job,” Takai said. “It’s not that I don’t worry about being a custodian of the citizens’ money. My job here is much more internal to DOD: How do we make sure that the warfighter is supported? And so that’s a very different kind of role and it’s got a different kind of dynamic.”

She has also been learning how to meet the needs of a wide variety of constituents in a department with more than 650,000 civilian employees and more than 1 million active-duty troops.

“When you’re in the private sector and you’re leading an organization, you have different levers that you can use in order to move an organization through a change process,” Takai said. “You have a different kind of process by which you can actually move leadership around into different kinds of positions. You have different processes around how you can reallocate resources, how you can reallocate dollars. Within government, it’s a much more focused and proscribed process.”

She’s also getting used to changes in budget management. In the private sector, numbers are set within an organization through a single chain of command. In public work, the budget is a collaborative effort among agency officials, various departments and even taxpayers and the media “because media is the conduit to the way that we get our messages out to the citizen around what we are spending their taxpayer dollars on,” Takai said.

“Clearly one of the things that I didn’t get right when I went into government was to really understand the importance of working with the legislature and the legislative body,” she said, “and the importance of getting involved in selling your message about the budget.”

“The other piece of the leadership challenge here at DOD has been in the context of really understanding the culture of our career civil servants and our career members of the Senior Executive Service,” Takai said. “Then there are the political appointees and the relationship there. And then the military. And each of those three has their own culture and their own approaches to looking at things.”

“One of the tricky things about information technology implementation, unlike some weapons systems, is that it’s as much about customer experience and the way people feel about their technologies as it is about the technology,” Takai told reporters at the annual Defense Information Systems Agency (DISA) conference in Baltimore in August. “It’s not about a power struggle for me. It’s about getting to the right answer, which is the ability for everyone to collaborate.”

Fiscal Crisis Management

Her job at DOD is the latest in a series of tough assignments she has tackled at budget-constrained agencies. “I do have this little cloud following me around,” she joked. “The budget deficit always seems to show up where I am next.”

For instance, the financial crisis hit Michigan earlier than other states, and American auto makers such as Ford have been fighting foreign competition for years. California, too, has experienced tough times, as evidenced by the fiscal emergency declared there in 2008 that led to large cuts in aid for public education and social welfare, and reduced benefits for state employees – issues that persist today.

Takai is drawing on her extensive private- and public-sector success in increasing an organization's efficiency by streamlining its IT architecture. Among her initial projects is the consolidation of DOD's IT systems while devising a cloud strategy in accordance with the Obama administration's 25-point plan for reforming federal IT management, released in December 2010.

In addition to the eight data centers she had already closed, Takai had plans to close 44 more by the end of fiscal 2011. "The sheer size of the DOD makes streamlining IT operations or changing IT investment management daunting, yet this size makes the payoff of successes that much greater," she wrote in a blog post on the CIO Council's website.

The next challenge will be cloud computing, which is a key facilitator of mobile technology, enabling warfighter access to data and mobile applications from anywhere using a wide range of devices. "As we begin to consolidate our data centers and as we begin to virtualize and standardize, then we'll be able to look at cloud services," Takai said, adding that the department will likely consider a private cloud at first "because there are certain areas [involving classified work] where we're not yet able to go to commercial cloud services."

DOD is an active participant in the Federal Risk and Authorization Management Program (FedRAMP), which was established to provide a standard approach to assessing and authorizing cloud computing services and products. "We are actually instituting a next-level FedRAMP that takes the FedRAMP requirements and then imposes the additional DOD requirements," she said. "And that will give us the ability, in parallel with the standardization, to look at private cloud services as well as commercial cloud services."

To forge ahead with her plan, however, Takai is collaborating with IT leaders in the various military branches to shape and adopt an enterprise approach that makes the most sense.

"It's not something we've done very well, but the technology is pushing us to go there," Takai said at the DISA conference. "While we've talked about the net-centric environment before this, now we're there."

Never Say Never

Takai admits that working for the federal government wasn't part of her career plan. She had not worked in the federal market or the defense industry before arriving at the Pentagon. Therefore, her path to a top leadership role in federal IT was far from predetermined.

After earning a bachelor's degree in mathematics and a master's in management from the University of Michigan, Takai started her career in the automotive industry. At that time, if you went to work in the Detroit area, "you were going to end up in the automotive industry," she said.

"How do we make sure that the warfighter is supported."

Takai made a name for herself at Ford as an expert developer of large applications, before joining EDS and Federal-Mogul Corporation. Public service didn't enter her mind. "People talk about your career plan, and that was not in my career plan, to work in government," she said.

But in 2003, as Takai tells it, fortune intervened.

"The governor of Michigan at that time had just been newly elected, and a friend of mine knew her and knew that she was looking for a CIO," Takai said. "And I have a golden rule, which is that you always talk to people when they have something that looks interesting. You never turn it down out of hand because it wasn't in your game plan. And it was really one of the most fortunate things I did because former Gov. Jennifer Granholm really is a terrific lady."

Although Takai found the prospect of working for the state intriguing, she said that before she met with Granholm, she didn't know what public service involved. "She actually talked to me about public service, something that I had not thought about in any sense before," Takai said. "It was a real gift to me that she spent that time at a point that I felt I needed something different."

As Michigan's CIO, Takai earned plaudits for streamlining the state's IT — and plenty of awards, including *Governing* magazine's Public Official of the Year in 2005. In addition, the Center for Digital Government ranked the state No. 1 in digital government for four years in a row during Takai's tenure.

In December 2007, Takai was recruited to lead California's 130 CIOs and 10,000 IT employees as the state's CIO. During her tenure, she formed the Project Management and Policy Offices to develop statewide policies for project development and management, released the California IT Strategic Plan, helped secure passage of the governor's billion-dollar-saving IT Reorganization Proposal to consolidate state IT functions under the CIO Office, and made state agencies more accountable by requiring them to submit Five Year IT Capital Plans to her office.

With jobs in two state governments under her belt, Takai said she still hadn't considered joining the federal government. But her high-profile work and former Defense Secretary Robert Gates' cost-cutting drive eventually led to her discussions with DOD.

"It was an interesting 'never say never' because I did say at one time I didn't want to go to federal government — you know, it was too big, I didn't have the experience," Takai said. "And

certainly as it relates to coming to DOD, one of my concerns was that I don't really have a military background at all."

But as she talked to Gates, former Deputy Secretary William Lynn III, Gen. James Cartwright and others, Takai became more intrigued.

"So that's how I got here — not through planning, but obviously I feel very fortunate," Takai said. "I spoke to a group of DOD senior executives recently, and I said to them I feel fortunate that I've been able to join the ranks of what they do because they are the senior professionals who really make the place tick. We, as political appointees, come in to play our role, to try to move things, but they're the individuals who really make a huge difference on a daily basis. We should always be very appreciative of their dedication."

As she seeks to empower DOD's workforce with the latest smart phones and tablets, Takai is dedicated to securing the supply chain for those devices and the information they access. It's a difficult balance, but one she's well prepared to deliver.

About the Initiative

The CGI Initiative for Collaborative Government is a joint public policy project of CGI in partnership with leading academic institutions. Launched in 2008, the initiative's mission is to analyze models of government's collaboration with the private and nonprofit sectors in order to identify best practices in using collaboration to achieve mission results.

Government today partners with the private and nonprofit sectors to accomplish a broad range of mission-related and administrative functions. The question is not whether collaboration will occur, but rather how agencies will collaborate most effectively while retaining strategic alignment, control and accountability.

The CGI Initiative for Collaborative Government is focused on helping government answer this challenge. We focus our analysis in eight special focus areas, seeking to provide practical management approaches that executives can apply to take strategy into action.

Special Focus Areas for 2012

- **Cybersecurity**
- **Environment**
- **Finding Savings**
- **Next-Generation Management**
- **Mobility**
- **Jobs**
- **Health**
- **Open Government**

www.collaborativegov.org