STATEMENT OF RICHARD A. SPIRES

FORMER CHIEF INFORMATION OFFICER OF THE U.S. DEPARTMENT OF HOMELAND SECURITY AND INTERNAL REVENUE SERVICE,

CURRENTLY CEO OF RESILIENT NETWORK SYSTEMS, INC.

BEFORE THE

SENATE APPROPRIATIONS SUBCOMMITTEE ON FINANCIAL SERVICES AND GENERAL GOVERNMENT

JUNE 23, 2015

Good morning Chairman Boozman, Ranking Member Coons, and members of the Subcommittee. I am honored to testify today in regards to the recent Office of Personnel Management (OPM) data breaches, while addressing issues and making recommendations regarding approaches on how the federal government can more effectively safeguard data and improve its cybersecurity posture.

Serving as the CIO of a major department (DHS) as well as the CIO for a large bureau (IRS) in the Department of Treasury, I had ample opportunity to understand the dynamics inherent in federal government information technology (IT), including how government agencies generally dealt with their IT security vulnerabilities. While at the IRS and DHS, I worked closely with the Chief Information Security Officers (CISOs) at both organizations to implement approaches that would address these security vulnerabilities. I also worked across the federal government on these issues, serving for a period as the Vice Chair of the Federal CIO Council and also as the Co-Chair of the Committee for National Security Systems. Given the gravity of this issue, I hope that my testimony is of value to Congress and the Administration in helping to address systemic weaknesses in how the federal government protects data and its IT systems from compromise.

Please note that I never worked at OPM and while I will allude to some of the alleged details of the recent OPM data breaches, my testimony describes broader systemic issues that must be addressed if we are to better protect our government's data and IT systems. In fact, I would urge Congress and the Administration to avoid a tactical approach that addresses narrow technical fixes based on these latest breaches – the weaknesses that led to these types of breaches are deeply rooted and require sweeping changes in our approach to IT and cybersecurity management and practices. Further, the weaknesses in the federal government's IT security posture are almost always based on IT practices that have been in place over many years. I served in the Bush and Obama Administrations and saw the same systemic problems in both. This should not be viewed as a political issue, but a call to action to fix a set of issues that can not only have a beneficial impact on securing data and systems, but improve IT management and delivery of systems as well.

My testimony will first focus on identifying the root causes that have led to a situation allowing massive data breaches of sensitive data and personally identifiable information (PII) to occur in government. I will then provide a set of recommendations to address these root causes that can, based on my experience, be implemented over a two-to-three year timeframe. As I describe below however, there is a window of opportunity to drive these changes that Congress and the Administration cannot afford to miss.

Root Causes of IT Security and Data Protection Vulnerabilities

The situation in which most federal government agencies find themselves susceptible to data breaches and compromises of core mission IT systems, are the result of three primary root causes, which include:

1. ***Lack of IT management best practices*** – The very best cybersecurity defense is the result of managing your IT infrastructure and software applications well. During the decades of the 1970s and 1980s, agencies could build and deploy IT systems with little regard to security issues. This was not necessarily a management failure since there were very few security issues to be concerned with prior to the broad use of the Internet and the rise of the ubiquitous data networks. However, beginning in the 1990s and up to the present, the federal government has not properly managed its IT. The government has failed to effectively adapt with the changes in IT and the evolving cybersecurity threat.

   As example of these failures, when I served at IRS and then at DHS, we would all-too-routinely discover IT systems outside of the IT organizations purview that had been developed and deployed without the proper IT security testing and accreditation. This highly distributed approach to IT management has led to the deployment of thousands of data centers across the federal government. Federal agencies today struggle with managing and maintaining this dispersed infrastructure and disparate systems. In far too many instances, hardware and software assets are not systematically tracked, software is not routinely updated and patched, and critical hardware and software has reached end-of-life and, in some cases, is no longer even supported by the vendors. And while I am big proponent of cloud technology, I am concerned that many agencies are not necessarily using cloud capabilities to streamline and simplify their infrastructure, but rather creating new IT "stovepipe" infrastructures. This complexity of maintaining a sea of vastly different systems in an ocean of differing underlying IT infrastructures makes it increasingly impossible to properly secure such a complex IT environment.

   Worse, when the government did realize it had these issues and attempted to fix them, entrenched interests made it exceptionally difficult to effect the necessary changes. For instance, a number of laws have been passed that attempted to address IT management practices, most notably the Clinger-Cohen Act of 1996, which mandated a strong agency CIO that could begin to rationalize IT within an agency. Yet Clinger-

Cohen is viewed as failed legislation in the federal IT community since in reality, none of the agency CIOs have the authority granted by Clinger-Cohen. Components, Bureaus, and program offices have generally resisted efforts to bring more oversight and discipline to IT management and operations under the theory that it impedes mission and business progress for agencies. Unfortunately, we are paying a huge economic cost for those decisions resulting in inefficiency, duplication and unsecure IT systems and infrastructure. And what is now worse; we will likely pay a greater cost in the exposure of PII of millions of current and former government employees, and potentially a cost to our national security.

2. ***Lack of IT security best practices*** – While well intentioned and appropriate for its time, the Federal Information Security Management Act (FISMA) skewed the approach for government IT information security. Originally passed in 2002, it set a course for how IT security effectiveness has been measured in government. While there are some good components of the law, the unintended consequence is that it forced CISOs to look at the controls for individual systems when in reality, IT systems across the government were already becoming more interconnected and viewing systems in isolation hid the impact on the larger enterprise security posture. Further, based on OMB guidance, FISMA was implemented during a period when the cyber-threat was still emerging and the evolution of technology hadn't yet recognized the necessity of a security development lifecycle. In fact, until very recently, systems would be certified and accredited based on a three-year cycle, which, while perhaps manageable, is comical when looking at the rapid evolution of technology and the cyber-threat environment. And furthermore, the law required the generation of paper-based reports, which diverted time, resources and personnel from effective security efforts. At both IRS and then DHS, I was consistently reluctant to put my confidence in the yearly FISMA report since it did not reflect the reality of the true security posture of our overall IT environment. That can only be done by proper use of tools that continuously monitor the IT environment and are able to react and mitigate threats in near-real time.

3. ***Slow and cumbersome acquisition process*** – The problem is exacerbated for government when funds are available to invest in IT security, yet it is ponderously slow and difficult to buy commercial solutions to help address vulnerabilities. When I was at DHS, I was a proponent of the continuous diagnostics and mitigation (CDM) program, but it was dismaying to see how long it took (two plus years) just to implement Phase 1, and then for agencies to go through an additional competitive process within the CDM program itself to obtain capabilities. I am all for fair competition, but with sophisticated adversaries that will exploit any and all vulnerabilities, the government is even more vulnerable when it takes many months (if not years) to be able to deploy new IT security capabilities.

Recommendations for Addressing IT Security and Data Protection Vulnerabilities

Clearly the federal government's overall IT security posture is poor, yet there is some momentum building that can result in fundamental changes that greatly improve that posture over a couple of years. While it is disappointing to have such large and damaging data breaches occur at OPM, I hope that the Congress and the Administration use this opportunity as a call to action for needed IT and IT procurement reform. Below are four recommendations to address the root causes for the IT security and data protection vulnerabilities outlined above.

1. ***Effectively implement the Federal IT Acquisition Reform Act (FITARA)*** - In December 2014 Congress passed and the President signed FITARA, which was included in the 2015 National Defense Authority Act (NDAA). FITARA is meant to address the systemic problems in managing IT effectively in an agency and while there are a number of provisions, the main intent of the bill is to empower the agency CIO to address these problems. Foremost of these problems include duplication of IT infrastructure and systems, lack of the use of best practices in IT acquisition, and the implementation of proper procedures to ensure IT security is properly addressed throughout an agency's IT organization and infrastructure.

   To ensure that FITARA does not suffer the same fate as Clinger-Cohen, a successful roll-out within agencies is critical. I am very pleased to see the approach OMB and the new Federal CIO, Tony Scott, are taking to support this roll-out. OMB just issued its final guidance to agencies for implementation of FITARA. In developing this guidance, OMB sought significant outside input, including guidance from former government CIOs, CFO, CAOs, CHCOs, and COOs and importantly, OMB asked for public comment on this draft guidance, which will improve content, understanding, and buy-in over the longer term.

   I recently testified at a hearing on FITARA and its role in improving IT acquisitions to the Subcommittees for Information Technology and Government Operations of the House Committee on Oversight and Government Reform.[1] I am not going to repeat much of that testimony, but I want to highlight the following:

   > "In terms of accountability, it has to start with the Administration and rests with OMB and the agencies. In particular, OMB must help ensure that the agency CIOs have the capability to perform their job and have the support from agency leadership to give them the chance to drive the required change to effectively implement FITARA. Further, the agency leadership must be supportive of the agency CIO, having the individual's back, particularly in agencies that are operating in a federated environment (this is particularly an issue in the cabinet-level departments). Congress … can support these efforts by demanding aggressive implementation of FITARA by agencies, development of measures for assessing FITARA's impact, and transparency in

[1] Richard Spires written testimony for that hearing is available at https://oversight.house.gov/wp-content/uploads/2015/06/Spires-Statement-6-10-FITARA.pdf

reporting of ongoing progress, while also highlighting obstacles in agencies to be overcome."

There is much confusion regarding IT security and the best way to protect data and systems. There is no single product or service that offers complete protection, and in my experience, without IT management best practices implemented across an agency, many of the security tools are simply ineffective. IT management best practices are foundational to success, and effective implementation of FITARA is the government's best hope to address decades of mismanagement.

2. Drive adoption of IT security best practices - To the government's credit, there has been a fairly aggressive shift in thinking from the traditional FISMA reporting approach to continuous monitoring of IT systems and the overall IT environment. I was also pleased to see that Congress passed much needed reform in the FISMA Modernization Act of 2014 last December, and I hope Congress will closely work with the Executive Branch to ensure that implementation delivers enhanced security.

That being said, when I look at the current Cross-Agency Priority (CAP) cyber-security goals[2], I feel the government is still behind current IT security best practices. For example, if you look at the overall objectives, the CAP goals will typically consider objectives of less than 100% as success, such as 95% for automated asset management or 75% for strong authentication. Higher numbers are certainly better than lower ones in these metrics, but we are dealing with adversaries that are advanced and persistent, that will almost certainly find the holes and exploit them – it is simply a matter of time. Likewise the Einstein system can aid agencies in detecting threats, and the promise of Einstein 3A is the proactive blocking of malicious traffic. However, Einstein is only helpful if the traffic is actually going through the system - in many agencies today, there are Internet connections that are not monitored by Einstein and I posit that this is another example of poor IT management. The government has invested hundreds of millions of dollars in the Einstein program yet agencies continue to posture and delay implementation. In effect, these approaches have led the federal government to establish a virtual "Maginot Line" as its key IT security strategy.

Based on the current situation and what I see evolving in the cybersecurity industry, I recommend a rethinking of how we are measuring success, with focus along three lines:

a) There is without a doubt a continuing need to pursue cybersecurity tools to prevent intrusions, but perhaps even more importantly, detect them quickly when intrusions do occur. The Einstein program identifies and protects against known "signatures" or characteristics of malicious activities, thereby preventing those intrusions. However, more advanced protective capabilities are required to prevent intrusions that the government is not yet aware of, thereby further

[2] A description of the CAP cybersecurity goals and the status can be found at http://www.performance.gov/node/3401/view?view=public#overview

reducing the government's attack surface. With enhanced automated protection, network defenders can then focus on detecting and remediating only the most sophisticated and potentially dangerous attacks – rather than trying to decide which of the seemingly endless alerts to pursue today. The cybersecurity industry has made great strides in these areas in the last few years, and government should be using the most advanced tools for prevention and detection that leverage threat intelligence from users all over the world.

b) Even with the most advanced prevention tools, the government needs to assume that sophisticated adversaries will still gain access. So alternative approaches are needed, and in particular, ones that relies on creating more trust in online interactions. The root of all trust is verified identity. I must know that it is who I believe it to be, and in the online world, multi-factor authentication methods are key to doing that. There are a plethora of newly available technologies to enable multi-factor authentication for both internal (government) as well as external users. And some of these solutions can integrate with antiquated systems. The government needs to step back and rethink how it very rapidly implements ubiquitous use of multi-factor identity authentication. Even though the root of trust is identity, there is more to the trust equation. In the "physical" world, I trust another because I have high confidence they will act in a manner that I expect. Some of the most damaging data breaches have come from individuals that where properly authenticated and authorized to use systems and access data. Their behavior, however, was not in keeping with what was expected. This is commonly called the insider-threat problem. There are new technologies and capabilities today that can bring in other context, such as an audit log or behavioral analysis systems to assess someone's trustworthiness on a regular basis. These additional factors, beyond those used to assess authenticity, are key to fully establishing and monitoring trust.

c) Finally, the government needs to target additional protection of an agency's most sensitive information, whether it be data sets or documents. Tools and products exist that enable agencies to protect information, independent of the likely insecure environment in which they operate. Agencies should focus on their most valuable information. I do recognize that there are limitations given some of the antiquated systems in which such information resides, but by focusing efforts on the most sensitive information, the government could ensure, within two to three years, that only trusted parties have access to an agency's most sensitive information. This would go a long way toward thwarting additional major and damaging data breaches.

3. ***Attract, train, and retain talented cybersecurity professionals*** – Even the best cybersecurity tools in the world require talented people who know how to use them. The shortage of cybersecurity professionals across the country continues to be significant problem. This is particularly an acute problem for the federal government. While the mission is very attractive to many cyber professionals, the hiring process and compensation models are not competitive with what individuals can make in the

private sector. Even with direct hiring authority, the government is not getting the talent it needs. The government needs more investment in training for current staff and the flexibility to hire that is competitive with the private sector. I do commend Congress for incorporating new flexibility for DHS to hire and pay cyber professionals into S.1691 also passed last December. Congress should monitor how DHS uses this authority, and consider expanding the authorities to other departments and agencies to help address the government's cybersecurity personnel shortage.

4. ***Develop a streamlined IT cybersecurity acquisition process*** - It is difficult to implement state-of-the-art IT cyber security solutions if you have no way to rapidly evaluate them before purchasing. The CDM and Einstein programs could potentially serve as government-wide vehicles for this process, but it has taken significant time to put them in place and I recommend an approach that enables individual agencies to rapidly bring in solutions and try them in a test-bed environment. After thorough testing and based on what works best, agencies should be able to roll security solutions into production. This approach would ideally encompass traditional cybersecurity vendors, but also new vendors that have little to no government experience – they are an incredible source of technical innovation. The government is simply not getting the best solutions through the existing acquisition process. I recommend that Office of Federal Procurement Policy (OFPP) work with the General Services Administration (GSA) and DHS to put a more streamlined CDM in place - one that would enable rapid addition of new capabilities as they become available in the commercial market.

Conclusion

Certainly the data breaches at OPM are terrible for the government and for those millions of us that may be negatively impacted in the future. Viewed through the right lens however, this episode can be the impetus for much needed and sustained change. And given the need to implement FITARA, the current Administration has a golden opportunity to set the correct foundation for success moving forward. This should not be viewed as a political issue but rather requires sustained leadership focus and commitment, and I am pleased to see such leadership currently coming from both Congress and the Administration. It is critical to make enough progress during the next 18 months to ensure that leadership commitment to FITARA, FISMA Modernization and to other needed changes in IT security are sustained into the next Congress and Administration.

Thank you for the opportunity to testify today.