STATEMENT FOR THE RECORD OF
STEVEN GROBMAN, SENIOR VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, MCAFEE, LLC
BEFORE THE WAYS AND MEANS SUBCOMMITTEE ON SOCIAL SECURITY
May 17, 2018, 10:00 AM

Good morning, Chairman Johnson, Ranking Member Larson and members of the subcommittee. Thank you for the opportunity to testify today. McAfee has over 1,000 employees based in Plano Texas, in Chairman Johnson's congressional district. We have found the district, with its strong base of IT professionals, to be a very friendly business environment. We also appreciate Chairman Johnson's long dedication to the district and our country, and I know he will be missed when he retires from Congress at the end of the year.

I am pleased to address the subcommittee on modernizing the identity and authentication system for citizens of the United States. This will have a profound impact on our citizens, our security and our economy. The Committee's focus on holding a "big think" hearing makes a great deal of sense. Before developing policy and operational solutions to solving our nation's identity management challenge, we need to make sure we're asking the right questions so the right identity management system requirements can be defined and the right roles and responsibilities for both the public and private sectors can be delineated.

First, I would like to provide some background on my experience and McAfee's commitment to cybersecurity. As McAfee's Senior Vice President and Chief Technology Officer (CTO), I set our technical strategy, ensuring that we create technologies that protect smart, connected computing devices and infrastructure worldwide. A large part of my role as CTO is driving innovation at McAfee, and my team includes: McAfee Labs, R&D, threat research and McAfee's internal CISO organization.

Prior to joining McAfee, I spent over two decades in senior technical leadership positions at Intel Corporation related to the field of cybersecurity, resulting in being named an Intel Fellow and worldwide McAfee CTO in 2014. I have 24 U.S. and international patents in the fields of security, software and computer architecture. I earned my bachelor's degree in computer science from North Carolina State University.

MCAFEE'S COMMITMENT TO CYBERSECURITY AND IDENTITY MANAGEMENT

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions from device to cloud that make the world a safer place. By building solutions that work with other industry products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices and in the cloud, we secure their digital lifestyle at home and while on the go. By working with other security players, we are leading the effort to unite against state-sponsored actors, cybercriminals, hacktivists and other disruptors for the benefit of all. McAfee is focused on accelerating ubiquitous protection against security risks for people, businesses and governments worldwide.

McAfee has also made a commitment to helping our customers address their identity management challenges. McAfee's Identity Theft Protection allows users to take a proactive approach to protecting their identities with personal monitoring, financial monitoring and recovery tools needed to keep identities personal and secured. Key features include:

- Cyber Monitoring – Scans the online black market and the Dark Web and alerts users when their personal information is at risk.
- Social Security Number Trace – Delivers reports of known aliases and addresses tied to a users' Social Security Number so they can review for potentially fake identities.
- Credit Monitoring – Sends reports based on lending and credit history, and alerts users to changes to their creditworthiness.
- 24/7 Dedicated Agent Support – Allows users access to agents who can answer questions and provide guidance on topics from using credit responsibly to handling identity theft.
- Identify – Provides complete visibility into data, context and user behavior across all cloud services, users and devices.

In addition, we've done a lot of thinking about identity management and what problems we as a nation need to solve. Here are some of our thoughts.

THE SOCIAL SECURITY NUMBER CAN NO LONGER BE USED AS AN EFFECTIVE AUTHENTICATOR

The once venerable nine-digit Social Security number first appeared as an identifier in 1936. It has become the de facto national identifier and a federal credential that people use for a range of both governmental and commercial purposes – uses for which it was never designed. Simply knowing an SSN has become accepted as a mechanism in many cases to impersonate an individual; it's also become a premier target for cybercriminals. SSNs are sold in bulk on the cybercrime black market for as little as one dollar. Once stolen, the SSN cannot easily be reissued or replaced, making it a weak foundation upon which to build identity.

The steady stream of major breaches where consumers' SSNs have been stolen creates a compelling opportunity for change. Last year's Equifax breach resulted in 145 million US-based users having their personal information compromised. Attackers reportedly exploited a vulnerability on the company's website to steal names, Social Security numbers, birthdates, addresses and, in some cases, driver's license numbers and passport numbers. Breaches like this remind us that the United States needs to modernize the national identification standard for its citizens. It is unrealistic for a Social

Security number (SSN) to be shared and distributed to many parties and stay confidential for the better part of a century.

Policymakers need to modernize the systems and methods that identify citizens as well as enable citizens to prove their identity with minimal risk of impersonation and without overtly compromising privacy. A good start is to determine what digital technologies offer strong security to create renewed confidence in the modernized credential system that must replace our current paradigm of using the current SSN across public and private ecosystems.

The growing cyber threat makes finding a solution even more urgent. McAfee Labs logged 63.4 million new samples of malware – an all-time high – in the fourth quarter of 2017. We found that cyber criminals are increasingly targeting the healthcare sector, where information, including personal identifiers, is non-perishable. The sale of personal information, including Social Security numbers, has become a lucrative business in underground markets.

NOT A NEW PROBLEM

While we're hearing more about it now because of recent breaches, the matter of using the SSN as a personal identifier is not a new problem. Twenty-five years ago, computer scientists voiced concerns about sharing a single piece of permanent information as a means of proving a person's identity. Simply having this piece of information was sufficient for an individual to prove his or her identity. Part of the problem is that there hasn't been an incentive, or forcing function, to change the way identity transactions work.

Ironically, we have not taken steps to develop better standards for protecting personal identity, yet we've taken these steps in other areas, such as credit card security. For many years, individuals' credit card numbers, the card expiration date and CID (card identification) number were all that was necessary to prove individuals could charge against an account. The massive retail breaches forced a reconsideration of this practice. The financial services industry recognized that this model needed to be changed and transitioned to chip-based technology or smart card–based credit card capabilities.

In Europe and much of the rest of the world, the transition was to a system known as chip and PIN, where the card not only has a computer chip, but the individual also must enter a unique PIN that is stored on the card. In the United States, the transition has been first to a partial improvement where a chip in a credit card can be used to prove physical possession of the card by having the smart card respond to a cryptographic challenge that it uniquely can respond to. This system can be enhanced in the future with the full adoption of "chip and PIN," which will have the chip only respond if the correct PIN is entered as well.

With chip and PIN, there is never any disclosure of the secret information to parties with whom individuals are transacting. It is simply a matter of using math -- cryptography algorithms – to prove that individuals are who they say they are, as opposed to giving the parties something that would let them impersonate the individual. The simplest technical requirement truly boils down to that. The question we need to ask as U.S. citizens is, why would we move forward to a more secure system for financial instruments such as credit cards but lag in our progress toward a more secure system for proving our identities as individuals?

DEFINING REQUIREMENTS

We must recognize that there are three elements that need to be discussed: identity, authentication and authorization. In our current SSN system, the simple number plays a role in all three, while in the field of computer science, we recognize the criticality of looking at these independently. Identity is the identifier that should be public and not pose a risk to the individual if many parties know it. The President of the United States' @POTUS Twitter handle is an identity. It identifies the President; however, knowing the Twitter handle does not let you impersonate the president.

Authentication is the process of proving you really are a specific identity. Authentication typically relies on something you know (a password), something you have (for example, a smart card) or something you are (such as a biometric). The strongest form of authentication requires multiple forms of authentication, such as a PIN (something you know) combined with a smart chip card (something you have). Authorization is granting a capability to a specific identity – for example, allowing a user to receive benefits or have access to specific information such as private medical data. All three – identity, authentication and authorization – must be part of a new personal identification system.

We have all the technology pieces to begin the journey to a high-quality, high-security and well-thought-out identity solution for U.S. citizens. We understand the cryptography, biometrics, how to build hardware devices and how to deploy them to scale to millions of people. We can apply the lessons we have learned, using proven technologies, from mechanisms such as our financial instruments, as well as looking at what has and has not worked in countries that have moved to more modern identity systems.

There are several ways to do this, from simply implementing proven credit card technologies such as "chip and PIN" for personal IDs, to employing technologies that are directly based on who someone is, such as biometrics (which makes it more difficult for a thief to use a stolen card or token). Chip and PIN technologies could allow individuals to electronically authenticate with a higher level of security than if they simply asserted a number (such as our existing SSNs).

What's going to be more challenging, however, is coming up with a solution that strikes the right balance between security and privacy, and deciding what the scope of this should be. Is this a solution for individuals to prove their identity for government-related services and transactions, Social Security and other government benefits? Or is this the solution for individuals to prove who they claim they are for other types of transactions? States currently provide identity solutions such as driver's licenses or ID cards. Does the new standard complement that? Does it replace elements of that?

These are some of the difficult questions that need to be debated: What is the intent? How do we want to protect privacy? What is a reasonable requirement to ensure that all citizens of the United States can prove their identity regardless of wealth or access to advanced technologies? Is it a reasonable requirement to have the federal government maintain a biometrics database for citizens such as fingerprints, iris scans or facial features? How will citizens who are disabled or require someone to legally act on their behalf utilize a next-generation authentication system? How will recovery mechanisms work when technology assets are lost, stolen or socially engineered? As a technologist in the field of cybersecurity, I have many building blocks at my disposal that can be used to define a next generation system; however, answering these questions is critical to choosing an appropriate solution.

We also must understand the pragmatic requirements of a next generation system. What are the cost constraints and funding options? How quickly must we move to this new system, and what does that migration plan look like? How many years does the underlying cryptography need to be secure?

This last question is interesting in that we are on the verge of quantum computing becoming a viable reality, likely within the next two decades. Quantum computing relies on the principles of quantum physics to solve specialized classes of mathematical problems that are not practical to solve on traditional computers. Quantum computers use quantum bits (qubits), unlike digital computers, which are based on transistors and require data to be encoded into binary digits (bits). These qubits can exist in multiple states simultaneously, offering the potential to compute a large number of calculations in parallel, speeding time to resolution. One of the key workloads that quantum computing is well suited for is to break the underlying cryptography that protects the world's data – specifically, the RSA public key algorithm, which is at the heart of most protection and identity solutions. RSA public key is at a high risk of compromise when quantum computing becomes a reality.

While we applauded the work by NIST to start the process to look for quantum-safe algorithms, we must understand that adversaries can place data on the shelf now (especially if it has long- term value such as national secrets) and attack it later when quantum computing becomes viable. Similarly, a next generation identification system should last 100 years or more, such that the next generations can prosper from the systems we invest in today. Careful consideration needs to be made about whether this new capability needs to be quantum safe – or at a minimum, have an architecture that allows the replacement of algorithms as quantum safe capabilities become available, even if we start with well-understood and tested components of today.

MOVING TOWARD A SOLUTION

I've been asked if blockchain technology could help put us on a path toward a secure identifier. I do not recommend this approach. Blockchains are a powerful technology that solves some very specific problems. They enable a trust model for an immutable ledger when a trusted party does not exist. In the case of cryptocurrency, this is exactly the problem you are trying to solve: you want to ensure that you can create transactions without reliance on any trusted agency or government. Part of what drives the viability of cryptocurrency is incentives for individuals to run the distributed infrastructure that powers the blockchain. We find, however, that blockchain has performance, scalability and privacy challenges that are not easily overcome.

During the cryptographers' panel at this year's RSA conference, Ron Rivest, a well-known cryptographic expert whose name accounts for the "R" in "RSA," discussed some of the failings of blockchains for certain security applications. He noted that they "fail miserably in terms of scalability, throughput and latency…[and] in certain applications [such as] voting they are a very poor fit.…[I]n many applications they are a bad database choice…. [T]hey have limited security properties that may or may not fit your need."

In the case of our next generation ID system, we have a trusted central authority (the US Government) and require significant scale for the infrastructure that would not be served well by a blockchain distributed system and architecture. Instead, we should focus on well understood tools and principles that our knowledge of cryptography, authentication and identity technologies provide, as opposed to falling victim to the "blockchain" hype.

We need to focus on what problems we are trying to solve. If a key requirement is that an individual's identity is not transferable, or that an individual can't have multiple IDs, then biometrics may be worth considering. India has moved to a national biometric identity program, allowing 1.3 billion citizens to prove their identities through fingerprints, facial recognition and eye iris scans. The country faced an even more difficult problem than compromised SSNs because there was no single starting database of citizens. Because benefits came with being a citizen, there were concerns that an individual might attempt to register in one town under one name and then register in another town under another name. The Indian government addressed this issue by creating a biometrics database to register its population. If your biometrics were already in the database, the government would know that you were a duplicate person. It also provided a mechanism that let you walk into any government office and reprove that you were you.

In the U.S., we need to move to a system in which an individual can prove their identity to someone, but not make it such that when proving their identity, they're giving the other party the ability to impersonate them. If we continue to rely on private pieces of information to prove our identity, we will continue to have those pieces of information stolen and misused—which will impact millions of individuals in the United States.

Yet there will certainly be an interim period during the transition that will require SSNs to play a role. There is a difference between using a number as an identifier and having that identifier be considered sensitive information. Given that lots of data already exists in all sorts of databases, and SSNs are used as a part of those datasets, it would be unrealistic to ban their use overnight. But they should be used strictly as an identifier, so they cannot be used to prove that imposters are the genuine individuals.

It is reasonable that the IRS uses an SSN as a part of its tax accounting solution, at least for the near term. But if somebody calls the IRS and simply gives their SSN and date of birth, that in and of itself should no longer be sufficient for the IRS to believe that the individual is definitively who they claim to be. It is the difference between using something as a reference to an individual as opposed to being an authenticator – an instrument that proves an individual identity.

We need to debate if keeping the SSN as an identifier is acceptable as long as it is not used for authentication or direct authorization. As mentioned earlier, a piece of data that is only an identifier does not pose a security risk even if it is widely known. The most critical focus should be on eliminating the SSN for authentication. We do need to recognize that we are running out of SSNs. The number of permutations in a 9-digit number is 1 billion. There are now about 325 million citizens in the United States, which could exhaust the pool of SSNs within a few generations. Is this acceptable? If we determine it is OK to re-use SSNs, we have some headway, but if we are re-architecting the system, it may be a good time to consider a larger namespace that eliminates the need for re-use in the long run.

Change will require a good partnership between the private sector and federal, state and local governments, given that identity is something that is used where citizens interact with many forms of government. Even within the private sector, we will need partnerships to determine what is appropriate for different types of private transactions.

We need to move quickly, however. Every day that we do not solve this problem sets up the opportunity for criminals to use compromised consumer data for the impersonation of individuals whose data has been breached. Granted, the world needs to operate during the transition, and we need to have a high level of pragmatism to work through this. At the same time, we should not indefinitely kick the can down the road and ignore the problem, forcing ourselves to default to systems that are inherently insecure.

The mega retail breaches of a few years ago changed financial institutions' perspectives and pushed U.S. merchants to move to chip-based credit cards. That series of events was the catalyst that made major industries take a step forward in using available technology. The Equifax event is very similar; it is a catalyst that should make us say, "Let's talk about this."

Now I'd like to make some policy recommendations.

POLICY RECOMMENDATIONS

Issue an Identity Management Executive Order – The Administration's executive orders on IT modernization and cybersecurity focused attention on modernizing our federal IT and cybersecurity capabilities. While these orders touched on identity management, the state-of-affairs in identity management is at such a critical stage that the President should issue an up-to-date executive order on this topic. An executive order on identity management would be a powerful call to action to all federal departments to leverage existing authorities to drive real change. Such an order would reinforce the Office of Management and Budget's (OMB) recent identity management guidance, "Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management".

Examples of initiatives should include:

- Developing model legislation to ban the simple knowledge of a Social Security number as an accepted form of authentication throughout our economy.
- Doubling down on privacy – what works in some countries will not work in the United States, given our long-held aversion to the type of system India has developed.
- Reinvigorating the National Strategy for Trusted Identities in Cyberspace, NSTIC, by funding and staffing it properly to continue progress between the public and private sectors on identity management standards.
- Encouraging and enabling federal agencies to act as validators of identity, given the many credentials over which the federal government has authority, including passports.
- Mandating all federal e-government services provided directly to citizens require the use of strong authentication to enhance trust in government services.

The latter action would improve citizen trust and satisfaction in government services and set an example the private sector is likely to replicate, given the power of the government to influence adjacent markets. But achieving success will require federal agencies, particularly the Social Security Administration, to double down on their IT and cybersecurity modernization efforts. Agencies should leverage IT modernization innovation funds to ensure their authentication systems are both modern and secure. Care needs to be taken to ensure cloud services that help enable citizen authentication are secure end-to-end, given the risk of assuming that just because personal identifying information (PII) is in the cloud, it is secure.

Let Innovation in the Private Sector Flourish – The private sector has not stood still. The FIDO (Fast IDentity Online) Alliance has made progress toward addressing the lack of interoperability among strong authentication devices and solving the problems users face creating and remembering multiple usernames and passwords. The Organization for the Advancement of Structured Information Standards (OASIS) has developed the Security Assertion Markup Language, an open standard for exchanging authentication and authorization data between identity providers and service providers. A standard called OAuth has also been developed – an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.

Yet more needs to be done. To date, the private sector has not solved the authentication challenges needed to build a truly modern identity management system. More private sector collaboration is needed to construct all the technical components – all the truly open and interoperable standards needed to give American citizens the high-quality identity management environment they deserve. If more progress is made in creating interoperable standards based on collaboration, a single, more proprietary, de-facto identity management system could develop.

While there are examples of de-facto standards, in the PC industry for instance, the risk of de-facto standards, particularly in an area as vital to the national interest as identity management, is that vendor lock-in could slow down innovation and progress. The government, led by NIST, should collaborate with FIDO and the other private sector identity management alliances and working groups, to share best practices and encourage the development and deployment of truly open standards and technologies. An identity management ecosystem based on open architecture solutions will promote innovation and increase the freedom of citizens to choose the identity management approach that meets their own needs.

Invest in Research and Development – The government has a fine track record of supporting basic research and development managed by universities and other centers of learning such as think tanks. These investments have enabled the United States to lead the world in semiconductors, software and bio-medicine. Investments in identity management research and development can produce similar results, particularly in a world where such stair-step innovations as quantum computing have the potential to disrupt our current and future identity management models.

Move Faster in Driving Quantum-Safe Algorithms and Integrating into Identity and Crypto Solutions – The government needs to incentivize and fund aggressive research into quantum computing. The private sector has already put a good deal of effort behind developing a quantum computer, with companies like Intel and Microsoft making good progress. Other nations realize that the country that develops the first quantum computer will have a significant advantage over others. The U.S. should take note of this and – at a minimum – make sure quantum-safe algorithms are integrated into network protocols and data protection algorithms as well as identity solutions. It is a matter of when, not if, quantum computing will be available to break current quantum-unsafe algorithms. A new identity architecture should at least allow the replacement of algorithms as quantum-safe capabilities become available.

CONCLUSION

It is an honor to testify before this subcommittee. We face identity management and cybersecurity challenges that merit immediate and sustained attention and investment. The fact that this committee, with its Social Security oversight and policy authority, is focused on solving the identity management challenge is truly encouraging. I appreciate your interest in considering my recommendations and look forward to answering your questions.