September 20, 2017

Via E-mail to: itmodernization@cio.gov

Chris Liddell
Director of the American Technology Council
1650 Pennsylvania Ave NW
Washington, DC 20502

Re: McAfee's comments in response to Request for Comments on the IT Modernization Report

McAfee LLC appreciates the opportunity to respond to the American Technology Council's Request for Comments on the *Report to the President on Federal IT Modernization*, posted August 30, 2017. McAfee has been an active participant with our federal partners in advancing cybersecurity, and we welcome the focus and ultimate goals of the draft report.

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions 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, we secure their digital lifestyle at home and away. 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.

Before beginning our comments, we want to express how extremely pleased we are to see the Administration's focus on improving and modernizing the way the U.S. government operates and provides services to American citizens. While the effort cannot and will not happen overnight, you have a real opportunity to fundamentally change for the better how the USG operates in the digital realm. The effort to unify and simplify capabilities, infrastructure and services allows all agencies, regardless of size, the ability to take advantage of the economies of scale. This consolidated approach should result in a more cost-effective way to assure federal facilities are

able to use the innovations of today instead of the antiques of yesterday. The modernization effort's goals of providing more transparency, more consistent management and better overall security is a real positive for the American people.

We hope you find our comments on this plan helpful.

Cyber Hygiene

The report states that it is not simply enough to patch HVA systems and tack on additional tools in order to protect them. We absolutely agree. Furthermore, we believe one of the biggest problems still plaguing IT today is the lack of follow-through on simple cyber hygiene processes such as assuring the latest and most secure software is running on all systems. Malicious actors need only find a single foothold to be able to lay the groundwork for an impactful attack on the enterprise. Rarely do they need to go after the HVA systems initially when they can easily get on the network through an unpatched or misconfigured system and then spend the time needed to discover the HVA systems' vulnerable software or trust relationships.

In past breaches, a lack of patching or execution of proper authentication and configuration processes has provided the attacker the ability to exploit globally well-known vulnerabilities. Modernized IT efforts need to incorporate the best current security practices, which includes assuring that a service or capability can be updated when patches or security updates are available. It is no longer acceptable for IT shops to push updates out a quarter to fit it into an organizational schedule. Updating or patching a service's capabilities must be designed and built into the service's management processes before the service is even deployed. Proper cyber hygiene is as critical to an organization's security as brushing your teeth is to dental health. It simply must be done. Any planning to modernize federal IT must include a serious focus on operational maintenance for all operational components of the deployed architecture from the beginning.

Piloting Needs

The plan identifies pilot projects for the TIC, SOC and the acquisition pilot. It is clear from reading the plan that other areas are ripe for piloting as well. We agree there is a need to test ideas out and to "fail fast" in order to really learn what works and what doesn't. A pilot that fails can be extremely beneficial if the root cause and lessons learned are understood and properly communicated to those who can benefit from them.

One of the common problems with pilots is that they are often open-ended with no real measurements for success. Some are outsourced to non-USG organizations with little or no oversight or real final deliverables. Often these types of pilots end up taking much more time and resources than needed to demonstrate feasibility. We applaud the fact that in Appendix D, there are real metrics for success. We encourage those responsible for implementing pilots to approach each pilot in a manner requiring success metrics and report-outs that inform appropriate decision makers as to what was learned. In order to get the results required to make longer term decisions on next steps, the pilot process used needs to be agile, able to deliver proof of concept in 90 days or less and proof of value in 120 days or less. Properly implementing a consistent pilot process assures that decision makers will be able to determine the right path to take with minimal impact to the anticipated timelines and costs.

Quantum Computing's Impact on This Plan

Today, data protection relies on a set of algorithms that secures everything from web connections to critical data stored or transferred in organizations or governments around the world. Today, cryptography is at the center of our data protection mechanisms for data both at rest and data in transit.

Some of these cryptographic algorithms are called "quantum safe," meaning the mathematics of the algorithm are not subject to attack by a quantum architecture. An example of a quantum safe algorithm is the symmetric AES algorithm used for bulk data encryption. Algorithms that are "quantum unsafe" have properties that would significantly increase the risk that a future quantum architecture could break the encryption. An example of a quantum unsafe algorithm is RSA's public key algorithm. RSA public key cryptography (PKI) is currently used to protect and secure communications across the internet. People look at their browser's lock icon to see if their connection to a web site is "secure," meaning it is using RSA PKI. If you have sent an email or a text, connected to a VPN, had your systems patched remotely, or use a "single sign on" capability in your organization, you are most likely using the RSA encryption algorithm.

While the ability to have a practical quantum computer is still years off – some estimate five years, some 20 – research is advancing rapidly. Both Google and IBM expect to have a functional quantum computer within the lower end of the estimate. The Chinese Academy of Science and Alibaba are also actively researching quantum computing.

There are reasons this is important to consider now. As we transition the federal government to more cloud-based services, we must be cognizant of the impact that the ability to break critical algorithms and capabilities, such as RSA PKI, will have on our ability to maintain the secrets and security of the data at rest and our fundamental means of securely communicating on the internet.

For example, data protected by quantum-unsafe algorithms today allow enemy nations and bad actors to "put on the shelf" encrypted data captured today and wait for the technology to mature. We must start to ask how long specific data should remain secure or secret. If the answer is one or two years, we should be fine using current algorithms. For data that must be kept secret for decades or longer, however, now is the time to start the transition to quantum safe algorithms.

As the public key infrastructure in use today is critically dependent on the RSA algorithm, we could wake up one morning and find that all communications on the internet are the equivalent of plain-text from some nation, actor or company's perspective. Even more concerning is the fact we may not even know that is the case and continue with business as usual as if nothing has changed. Fortunately, there are organizations experimenting with post-quantum cryptography key exchange to assure we have a means to secure communications and data once large quantum computers are available.

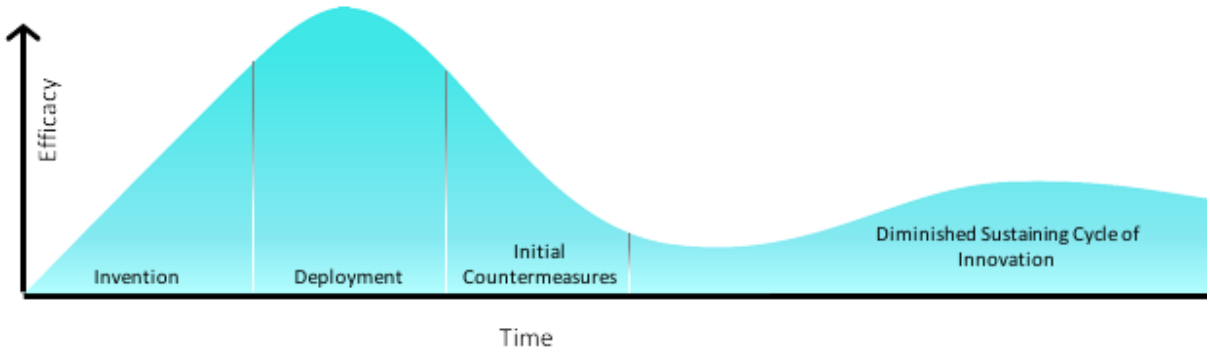
The above comments are not meant to be alarmist but simply to anticipate the environment that will exist once this plan is successful and fully implemented. It is important these considerations are properly addressed as a part of implementing this plan so as not to create inadvertent national exposure and a crisis in the not-too-distant future.

The Case for Separate Cybersecurity Procurement Processes

For too long, government and business have viewed purchasing IT products and cybersecurity products in the same way. It has become extremely apparent this is a mistake, and we must look at new ways to view and procure each.

A common assumption is that software improves over time. This is indeed true for general IT-related software, as time allows the vendor of the product or service to shake the bugs out. Each updated version becomes just a bit better as input from users is incorporated.

The cybersecurity product effectiveness lifecycle, however, is very different from traditional IT software. In cybersecurity, we see a trend where every new defensive technology loses effectiveness once market deployment is large enough to drive adversaries to build countermeasures and evasion tactics. The effectiveness of these new security offerings follows the path of the Grobman Curve. The cycle looks like this:



Because of this cycle, it is especially important that procurement of cybersecurity products and services not be lumped in with regular IT products, which increase in usefulness and effectiveness over time as the software matures. Cybersecurity products are initially extremely effective, but as time goes on the adversaries learn ways to bypass or circumvent the capabilities of the products and the cybersecurity products become less effective. Because of these differences, the Administration and policymakers need to view procurement of cybersecurity products very differently than traditional IT products and services.

We urge procurement reform to speed up the acquisition of up-to-date cybersecurity solutions to enable the government to compete with fast-moving hacker techniques and tactics. We urge adoption of flexible procurement rules that enable the use of software-as-a-service capabilities to allow rapid deployment of state-of-the-art cyber capabilities. This will help free agencies from having to manage separate procurements simply to upgrade the security capabilities of existing cybersecurity programs.

USG Risk Management

Over the last few years, the NIST Cybersecurity Framework has helped change the security dialog from "compliance" to "risk management" within a large portion of U.S. organizations. This is an extremely positive trend. It is important the Framework continue along this path and focus on cyber risk management. We are

extremely pleased to see it being mandated within the U.S. government and as part of this plan. The Framework commendably represents an effort to solve the complex problem of protecting ourselves from cybersecurity threats in a way that harnesses private sector innovation while addressing the cybersecurity needs of governments, businesses and citizens. The focus on reviewing, understanding and improving organizational cybersecurity protection programs is a positive change from where organizational focus has been in the past. The transparent and collaborative process NIST led in developing the Framework has served as a model not only for other U.S. government agencies but also for governments worldwide seeking to address cybersecurity-related issues. McAfee has been an active participant in the Framework's development and update process, and we look forward to continuing to partner with NIST and other government agencies as future versions of the Cybersecurity Framework are enhanced.

The Importance of Security and Privacy by Design

As new services are developed, adopted or piloted as a part of this plan, it is critical that both security and privacy are at their core and that privacy and security complement each effort. Proper protection of individual privacy in services does not just happen. It needs to be designed and engineered in from the beginning of the service development process. Likewise, security by design means designing security in right from the start. Adding or "bolting on" security features to a system, network or device after it's already up and running has inherent weaknesses and inefficiencies. Cybersecurity and privacy must be built in at the very start of the design and development process. Both privacy and security must be intrinsic to a development organization's thought processes, and both must be embedded in a service or network element so they become integral parts of the service's or element's functioning. This approach is not only more effective; it is less cumbersome and less expensive than trying to lock down systems that are leaking personally identifiable information (PII) or are inherently insecure.

Protecting Citizen and Government Employee Information

Given the sizeable number of breaches of PII data, most recently Social Security Numbers (SSN) in the Equifax breach, it is apparent that the standard means for identifying US citizens is failing. As the federal government moves to modernize its digital operations, it should address the fundamental way governments at all levels provide proof of identity for its citizens and a means to validate citizens receiving services.

This is not a new problem. As early as 25 years ago, computer science advocates voiced concerns around sharing an SSN – a single piece of permanent information – with others as a means of proving your identity. Part of the problem is there hasn't been a forcing function or an incentive to change the way these identity transactions work. Simply having these pieces of information constituted the ability of an individual to prove his or her identity. The irony is that we have not taken steps to come up with a better standard despite recognizing that a single piece of information is not adequate in many other places, such as credit cards.

For many years, your credit card number, expiration date, and CID number were the things proving you could charge against an account. A few years ago, millions of credit card numbers were compromised during several major data breaches in the retail sector. From the credit card perspective, it was recognized that the existing model needed to be changed, and the transition began to "chip and PIN" or smart card–based credit card capabilities. The underlying technologies for credit cards using a chip never need to disclose the secret information to parties with whom you are transacting. You are simply using math, cryptography algorithms to prove that you are you, as opposed to giving others something that allows them to impersonate you. From a U.S. perspective, why would we move forward to a more secure system for financial instruments such as credit cards, but lag in our progress towards a more secure system for proving our identities as individuals and citizens?

We have all the technology pieces to begin the journey to a high-quality, high-security, 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 learned using proven technologies from mechanisms such as our financial instruments, and we can look at what has and has not worked in countries that have moved to more modern identity systems.

The retail mega-breaches of a few years ago changed financial institutions' perspectives and pushed U.S. merchants to move to chip and PIN 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 makes us say, "Let's talk about this" and get to work on solving this now. If almost half of U.S. citizens have their SSNs and other personal information compromised, we cannot assume that the information can be used any longer as the sole criteria for someone proving their identity. 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.

The government has a duty to ensure that citizen data is accurate and protected. As a part of the IT modernization efforts, McAfee encourages the federal government to begin the necessary conversations with industry, the privacy community, and state and local governments to start moving to a system in which individuals can prove their identity to someone, but not automatically give the other party the ability to impersonate them in a completely different transaction.

Fostering Interoperability

In cybersecurity overall, we need a different approach where technology – enabled by strong collaboration – can be deployed rapidly to security platforms so they can communicate with each other over open communication protocols. Organizations in both the public and private sector need security tools that are interoperable and interchangeable to protect against existing and prospective threats. As cybersecurity solutions become interoperable, they become more efficient and cost-effective. They also become easier to maintain than an IT environment of disparate systems. Over time, more interoperable cybersecurity systems also will contribute to closing the skills gap as these systems become more widely deployed and require less manual intervention.

McAfee calls on the cybersecurity industry to design technology to an open standard, on an open platform so customers are not locked into proprietary technologies that don't work with each other or allow for change. Customers deserve the ability to deploy best-of-breed security solutions, but if they need to install a complete infrastructure just to do so, then customers lose. By having interoperable standards for interface and exchange formats, the industry could move to a more plug-and-play capability for security products. This has been successful in the past with efforts such as the Security Content Automation Protocol (SCAP), currently in use in the HBSS and CDM programs. SCAP provides a wide variety of vendors the ability to exchange compliance and patch validation content.

McAfee has long believed in breaking down the walls that separate vendors' security products, and we have taken a major step toward doing just that by opening our Data Exchange Layer (DXL) – a communications fabric that enables unprecedented collaboration in an open-source, real-time system – to other developers and vendors to use at no expense. OpenDXL™ is at the core of our mission to enable security devices to share intelligence and orchestrate security operations at rapid speed. As

of today, a growing set of security companies are actively connecting or planning connections to the DXL ecosystem. Open DXL is a big part of what we mean by Together Is Power. No single industry partner can cover the vast spectrum of security and privacy problems, just as no single industry partner will catch every issue every time. Only by working collaboratively in the private and public sectors can we build the tools and infrastructure needed to defeat cyber attackers.

We encourage the government to work with the private sector to make the vision of a truly open and interoperable cybersecurity ecosystem become a reality. Such an ecosystem promotes a great deal of competition and innovation. At the same time, it also promotes collaboration – making sure that systems work together. The real benefit is an environment that promotes enough competition to deliver innovative solutions, but enough collaboration to ensure that these new and innovative solutions can work together. Much like the railroad industry that agreed on basic rules of the road – e.g., size and gauge of the tracks and right of ways – the security industry needs rules of the road to allow cooperation, so that firms can compete on implementations to allow for as much innovation as possible.

Moving Forward

Thank you again for the opportunity to provide comments on the draft Report to the President on Federal IT Modernization. McAfee applauds the continued close collaboration between industry and the U.S. government. We support the Cybersecurity Executive Order and commend the Administration for prioritizing federal government IT modernization and cybersecurity, recognizing the merits of NISTs Cybersecurity Framework, and valuing a flexible, multi-stakeholder approach to promote stability in the global IT infrastructure. We are ready to support implementation of the EO, as appropriate, through the work of the American Technology Council and other appropriate avenues and look forward to continuing to partner as you drive the IT modernization and cybersecurity initiatives forward.