accenture

DEFINING A CYBER MOON SHOT

A ROADMAP FOR FEDERAL CYBER LEADERS

TABLE OF CONTENTS

The world is experiencing a digital revolution. One that is fundamentally changing how we experience our lives— in ways we have yet to truly understand. As our personal and professional communications and interactions have moved online, so has a broad range of threats. Hackers, criminals, terrorists, and adversary nation states have outpaced our nation's cybersecurity defenses. The Government's inability to keep pace with cyber threats is now a national state of cyber emergency and without immediate action, the United States risks jeopardizing its freedom and prosperity.

IT'S TIME. FOR A CYBER MOONSHOT

On May 25, 1961, President John F. Kennedy delivered his historic Moonshot speech to Congress that set the U.S. on a course to send a man to the moon. "Now it is time to take longer strides," Kennedy told Congress that day, "time for a great new American enterprise—time for this nation to take a clearly leading role in space achievement, which in many ways may hold the key to our future on earth." He then challenged NASA and the nation to a seemingly unimaginable task: to put a man on the moon [and safely return him to Earth] by the end of the decade.

At that time, the United States possessed the technological know-how to achieve a moon landing. What it lacked was a vision for harnessing its technological prowess to achieve a dramatic and tangible outcome. Three factors were essential to Moonshot's success: 1) **concerted leadership** to drive unprecedented innovation, 2) a **specific call to action** igniting unparalleled collaboration across the public and private sectors 3) and a **sustained investment** ensuring continued success.

Nearly fifty years after the first moon landing, the U.S. has a compelling opportunity to apply the lessons of that Moonshot to the opportunities and challenges of today. The Digital Age has revolutionized business in both the private and public sectors, and in this environment, data and digital operations are our currency. Today we possess the technological know-how to accomplish a cyber moonshot. To achieve success we need bold new approaches to address the vulnerabilities we face today and to overcome the challenges we will face tomorrow, such as protecting the Internet of Things (IoT).

It's time to be more intentional about cyber products and services and to act in a focused and integrated way across government agencies. The economic and national security costs of failing to act decisively are simply too high.

Today is the day we must launch a moonshot for the Digital Era: a clear plan for securing the digital landscape over the next five years. This paper discusses how our government can launch and successfully execute our Cyber Moonshot.

THREE WAYS CONGRESS CAN ADVANCE A CYBER MOONSHOT

ALLOW AGENCIES TO RETAIN AND REINVEST SAVINGS TO DRIVE IT MODERNIZATION

INCENTIVIZE OPERATIONAL EFFICIENCIES BY OFFERING A SAVINGS MATCHING FUND

ENCOURAGE ADOPTION OF AUTOMATED CYBER DEFENSES THAT LEVERAGE ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) TO DRIVE SCALABILITY

BECOMING CYBER RESILIENT

The call for a Cyber Moonshot is a call for true Cyber Resilience. We must assume that our systems, information and processes are under continual threat of compromise and we must engineer them to be fault tolerant.

By doing that we can create a baseline level of confidence that does not waver when an unexpected event hits and being ready with a systematic plan and cyber defenses in place when an attack occurs.

When we achieve this:

- Government, business and citizens will operate without excessive fear of loss, compromise, or damage.
- Continued innovation in enhanced citizen services will continue to be delivered on a secure and resilient foundation.
- Information needed to secure our nation will be accessible to only the right users.

Tell us what you think true Cyber Resilience will mean to the federal government. #CyberMoonshot

THE PATH FORWARD: LEADERSHIP & TECHNOLOGY

IT STARTS WITH LEADERSHIP

Across the government, our nation's cybersecurity efforts remain fractured. "When compared against 17 major private industries, our federal, state and local government agencies rank third lowest in cybersecurity."[1]

For a Cyber Moonshot to work we must establish unity of action–all agencies must have the advantage of benefitting from cyber intelligence and lessons learned.

With cyber emerging as the next battlefield more strategic and productive approaches are needed.

Four ideas to consider:

Create a new secretary-level cybersecurity role with a direct line of reporting to the White House and with the authority to direct and oversee the cyber strategy across the entire federal government. This position could be supported by a new Cyber Board that has oversight across key government agencies to ensure changes are being tackled aggressively.

Create a single agency that has authoritative responsibility for the nation's cybersecurity.

Act decisively to close the gap between the public and private sectors. We must recognize that our critical infrastructure extends to and through the private sector and execute on real commitments, ensure constant engagement, respond at the speed of the private sector, and leverage government authorities and resources. Perhaps even establish a quasi-public corporation to combine private sector speed with the government's authority and resources.

Tackle cybersecurity from the ground up by ensuring strong access to STEM education and cyber career paths for our nation's youth and re-think what it means to deploy a cyber workforce in ways beyond a four year degree.

What cyber leadership changes do you think would most impact the success of a Cyber Moonshot? #CyberMoonshot

At the end of the day, a safe system provides the right data access to the right users at the right time—only.

Tom Greiner,
Accenture Federal Services

BUILDING THE CYBER RESILIENT ENTERPRISE

It is no longer possible to distinguish between our federal agencies and their mission delivery and the technologies that empower these operations. As such, we need to rebuild our enterprise infrastructure to reflect this reality. Assuming we get the basics right to bring all federal agencies up to par with current standards in a systematic and cohesive way – we must establish a strong cyber resilient foundation, one that shifts the balance of power away from our adversaries and tips the scale in our favor. We believe there are five essential steps in this part of the Cyber Moonshot journey:

1 **Embrace the Cloud for Security:** leverage the unique, enabling features of cloud technology to eliminate vulnerabilities, create a more defensible barrier and enable more dynamic cybersecurity. Using the cloud to enhance security will allow us to significantly limit our exposure to cyber risks.

2 **Engage in Proactive Defense:** Shift from a reactive to a proactive approach to cybersecurity. Don't guess, know! Continuously hunt, probe, and root out dangers such as Advanced Persistent Threats (APTs), before the adversary can exploit them. Apply machine learning and artificial intelligence to automate detection and response.

3 **Demand a Data-centric Approach:** Harden systems from the inside out by encrypting and anonymizing data to minimize the potential for loss if an adversary gets in. This starts with prioritizing the most important data assets—"the crown jewels"—across the government and devoting the necessary resources to secure them.

Tell us what you think the most critical technology step is for helping us shift the balance of power. #CyberMoonshot

4 **Require Security by Design:** Security must no longer be viewed as an after the fact compliance exercise that results in added cost. Rather it should be engineered into the core of every system from the get-go. Agencies must adopt a more agile approach to security during the development process that brings all practitioners to a high level of proficiency in security in a short period of time, ensuring security needs and recognize that this isn't a one-time exercise as today's dynamic systems requite continuous cyber hygiene.

5 **Build-in Cyber Resilience:** Leverage the advanced capabilities of software-defined computing and storage to build cyber resilient systems. A moving target is hard to hit – and if they cannot find you, they cannot attack you.

Each of these five critical technology advances will be covered more deeply in subsequent Cyber Moonshot papers.

SECURING THE INTERNET OF THINGS: THE GREATEST CYBER CHALLENGE OF ALL.

Beyond strong leadership and establishing an advanced cyber technology posture, the Cyber Moonshot must address the immense challenge of securing the growing IoT landscape.

What we are doing today simply won't work in the near future. The sheer number of IoT devices will make human control and oversight impossible which means we must proactively pursue security solutions that detect and respond to threats at machine speed. Artificial intelligence and machine learning will fulfil this critical role in enabling confident, assured use of IoT capabilities.

By 2020 more than 34 billion devices[2] will be connected to a platform or another device and with more than 90 percent of Americans currently using three or more devices[3], the accompanying flow of data–often highly sensitive–will continue to grow.

IOT WILL INFLUENCE EVERY ASPECT OF MODERN LIFE.

FROM DRIVERLESS CARS, TO BETTER MEDICAL TECHNOLOGY, TO MORE EFFICIENT DELIVERY OF CITIZEN SERVICES, IOT WILL BE PART OF NEARLY EVERY FACET OF OUR DAILY LIVES. IT WILL BE THE FOUNDATION THAT KEEPS OUR NATION RUNNING, FROM ELECTRICITY SYSTEMS TO FINANCIAL SERVICES AND TRANSPORTATION.

ARTIFICIAL INTELLIGENCE IS ESSENTIAL TO A CYBER MOONSHOT

Today's cybersecurity tools are focused on detection and remediation. This approach is too slow to combat the volume and relentlessness of today's threats.

AI and machine learning offer new possibilities. When combined with the Cloud, AI can help us scale our cyber efforts through smart automation and continuous learning the drives self-healing systems.

Artificial Intelligence can create a cyber immune system. It can limit attackers by shutting the open doors and windows we have right now.

Nicole Dean, CISO,
Accenture Federal Services

The learning process also helps to spot vulnerabilities. Over time, security professionals can be taught the finer points of machine learning, so they can augment the machine learning and algorithm process with human checks and verifications that reduce the risk of false positives.

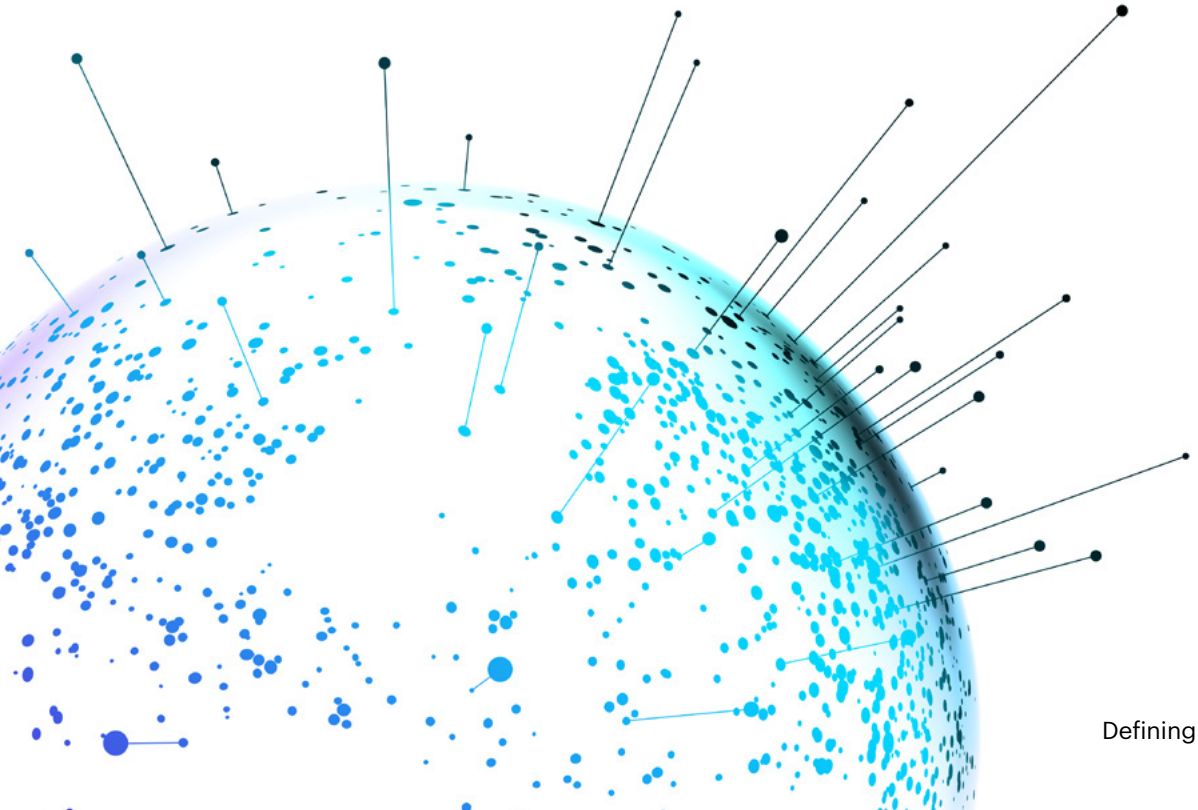
Additional benefits of using machine learning to secure the IoT include:

- Drawing insightful patterns and trends from vast amounts of data
- Developing more predictive security models
- Continuously learning from data without re-programming machines
- Instantly detecting abnormal behavior and proactively respond

We live in a world where the weakest player is the source of a cyber attack, and all kinds of everyday items are now being connected to the internet. They all become potential threat vectors. This ever-expanding digital network must be secure if it is going to continue to be the backbone of the global economy.

Gus Hunt,
Cyber Practice Lead,
Accenture Federal Services

Tell us if you are on the path to deploying AI solutions in your cyber environment. **#CyberMoonshot**



CONCLUSION: FROM **MOONSHOT** TO **REALITY**

The U.S. has the resources and the ingenuity to make its digital networks safer and stronger. With focused leadership, the adoption of the right technology practices, and the power of AI and machine learning combined, a Cyber Moonshot will be successful and we will achieve a true state of cyber resilience.

As Kennedy said in his Moonshot call,

> **"We choose to do...not because they are easy, but because they are hard; because that goal will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone, and one we intend to win."**
>
> **JFK**
>
> **September 12, 1962**

We can land this Cyber Moonshot, shift the cyber balance of power, and make the Federal Government and the nation safer and stronger. It is a journey that requires concerted leadership, relentless vision and focus and a sustained investment.

We are ready now to put ourselves on the right path to being safer in five years.

Tell us how you can commit to helping achieve a national Cyber Moonshot. **#CyberMoonshot**

WHAT CAN YOU DO NOW?

The path forward may be slightly different depending on where federal agencies are in their cyber journey. There are a few key things that each agency can do **right now** to start to shift the balance of power in your favor:

1. Immediately improve basic cyber hygiene to ensure systems are patched and up to date
2. Accelerate cloud migration for security purposes
3. Identify your "crown jewels" and focus on securing those systems by adopting a data-centric security approach to minimize the potential for loss
4. Adopt DevSecOps processes, bringing together IT modernization and cybersecurity investment, to ensure business, IT, and cyber needs are cohesively addressed
5. Adopt effective and proven proactive defense measures—hunting, red-teaming, penetration testing—to root out APTs, close the holes, and build a more capable and hardened defense posture
6. Promote a Security First mindset where cybersecurity is viewed as everyone's responsibility

REFERENCES

[1] http://info.securityscorecard.com/2017-us-government-cybersecurity-report

[2] http://www.gartner.com/newsroom/id/3598917

[3] http://www.businessinsider.com/bi-intelligence-34-billion-connected-devices-2020-2015-11

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE FEDERAL SERVICES

Accenture Federal Services is a wholly owned subsidiary of Accenture LLP, a U.S. company, with offices in Arlington, Virginia. Accenture's federal business has served every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations.