## *Ron Ross*

Chairman Donilon, Vice Chairman Palmisano, and distinguished members of the Commission, I want to thank you for allowing me to discuss some of the nation's challenges and opportunities in protecting the systems and networks that support the United States critical infrastructure as well as the important business functions that drive the national economy. My name is Ron Ross and I am a Fellow at the National Institute of Standards and Technology. I have over thirty years of computer and information security experience that includes a variety of positions in the United States military, Intelligence Community, Federal Civilian government, and the private sector. Currently, I lead the Federal Information Security Modernization Act Implementation Project, the Joint Task Force Cybersecurity Project, and the Systems Security Engineering Initiative.

### The Current Landscape

The United States, along with every other industrialized nation, is experiencing an explosive growth in information technology and living in a world fueled by almost limitless technological innovation—including the development of computing and communications capabilities that are unparalleled in the history of mankind. The technology is powerful, affordable, and compelling, driving massive consumerization from large corporations to small businesses to individuals with their personal devices. The rapid and continuing technological advancements and the dramatic growth in consumer demand is occurring simultaneously with an emerging convergence of cyber and physical systems—sometimes characterized as the *Internet of Things*. This unprecedented technical innovation, mass consumption of new technologies by governments, businesses, and individuals, and ubiquitous deployments of those new capabilities worldwide, have resulted in a highly complex information technology infrastructure of systems and networks that are very difficult to understand and therefore, protect. As a nation, we are spending more on cybersecurity today than at any time in our history, while simultaneously continuing to witness an increasing number of successful cyberattacks and breaches by nation states, terrorists, and hacktivists that are stealing our intellectual property, national secrets, and private information. The situation is not getting demonstrably better over time and will have a debilitating long-term effect on both the economic and national security interests of the United States.

### The Basic Problem Is Simple

Our fundamental cybersecurity problems today can be summed up in three words—*too much complexity*. Put another way, you cannot protect that which you do not understand. Adversaries view the U.S. critical infrastructure and our thriving businesses and industry as a target of opportunity, each adversary with potentially different capabilities and intentions. Increased complexity translates to increased *attack surface*. This provides a limitless opportunity for adversaries to exploit vulnerabilities resulting from inherent weaknesses in the software, firmware, and hardware components of the underlying systems and networks. We have characterized this situation as the *N+1 vulnerabilities problem*. The Defense Science Board pointed out in its 2013 study[1] that vulnerabilities can be categorized by type: those vulnerabilities that are known; those vulnerabilities that are unknown; and those vulnerabilities created by adversaries after they have taken control of your system and network.

[1] Defense Science Board Report, *Resilient Military Systems and the Advanced Cyber Threat*, January 2013.

Simply stated, there are vulnerabilities that you can find and fix, and there are those that you cannot detect and therefore, remain unmitigated. The increasing complexity and attack surface in critical U.S. systems and networks both in the public and private sector, virtually guarantees that the number of serious weaknesses and exploitable vulnerabilities that lie "below the water line" will continue to grow at an alarming rate. While we are making significant improvements in our intrusion detection and response capabilities, those types of tools and associated cybersecurity tactics fail to address the fundamental weaknesses in system architecture and design that can only be addressed with a holistic approach to protection that is based on sound systems security engineering techniques and security design principles. The ultimate objective is to make our systems and networks more penetration-resistant; capable of limiting the damage from cyber-attacks by reducing the adversaries' time on target or lateral movement through the system; and sufficiently resilient to support critical missions and operations.

## Why the Problem Is Difficult to Describe

We operate in two very different worlds—a world of *kinetic space* in which we can engage all of our senses, and a world of *cyberspace* which flies below the radar in a collection of bits, bytes, electrons, and integrated circuits made of silicon. Kinetic attacks such as the September 11th terrorist attacks on the World Trade Center and Pentagon can be observed and internalized and make a lasting impression on all of those individuals who witnessed the devastation. In contrast, cyberattacks operate in cyberspace which is analogous to having cancer in the early stages—the individual feels fine, cannot detect any life threatening condition, and as a result, goes about their business as usual as the cancer spreads to vital organs. While cyberattacks occur on a regular basis, result in serious or catastrophic consequences, and are widely reported in the news media, most organizations feel fortunate that the attacks are happening to others and not them. The cyberspace nature of the problem gives organizations a false sense of security since their systems appear to be operating normally while the adversary steals their intellectual property and highly sensitive information through an exfiltration attack. Strategically-placed malicious code can also hide in the complexity of the information technology infrastructure, giving adversaries the opportunity to bring down an organization's critical capability at a time of their choosing.

## Engineering-Based Cybersecurity Solutions

Today, we have a high degree of confidence that the bridges we cross and the airplanes in which we fly are safe and structurally sound. We trust those entities because they are designed and built by applying the basic laws of physics, principles of mathematics, and concepts of engineering. If bridges were routinely collapsing and airplanes were crashing frequently, the first people called upon would be the scientists and engineers. They would do root cause failure analysis, find out what went wrong, and make the necessary recommendations to fix the problem. Cybersecurity efforts today are largely focused on what is commonly referred to as cyber hygiene-related activities—activities such as asset inventories, patching of systems, configuring firewalls and other commercial products, and scanning for vulnerabilities. While all important and necessary security activities, by definition, they operate "above the water line" and cannot affect the basic architecture and design of the system. Achieving perfection above the water line can still render our critical systems and networks highly vulnerable due to the inability to manage and reduce the inherent complexity of the information technology infrastructure.

The only way to address the ongoing "N+1 vulnerabilities problem" is to build more trustworthy secure components and systems by applying well-defined security design principles in a life cycle-based systems engineering process. Security, much like safety, reliability, and resilience, is an emergent property of a system that does not happen by accident. The disciplined and structured approach that characterizes engineering-based solutions is driven by mission and business objectives and stakeholder protection needs and security requirements. Those highly-assured and trustworthy solutions may not be appropriate in every situation, but they should be available to those entities that are critical to the economic and national security interests of the United States—including, for example, the electric grid, manufacturing facilities, financial institutions, transportation vehicles, water treatment plants, and weapons systems.

To support these objectives, NIST has embarked upon a multiyear systems security engineering initiative to define how security design principles can be applied within a standardized systems engineering process. We are bringing forward specific considerations to government, industry, and academia for a multidisciplinary approach in the engineering of trustworthy secure systems. These considerations are grounded in the fundamentals of computer science, mathematics, and engineering—as well as over forty years of well-defined security design principles that represent the state of the practice.

## A National Strategy Focused on Trustworthy Systems

During the Cold War, the United States invested in a nuclear triad of bombers, missiles, and submarines as a central element in its national strategy to defend the country against a first strike from the Soviet Union. It was the single most expensive investment ever made by the United States, although there was an extremely low probability that we would ever use that capability. The justification for such an expensive investment with low probability of use was directly related to the "asset valuation" that was a key part of the national *risk assessment*. The asset in question was the preservation of the United States of America, our freedom, and our way of life. The consequences of not making the investment in a defensive capability sufficiently strong to defend against or deter a Soviet first strike would have been catastrophic. The cybersecurity threats to our critical infrastructure, businesses, industrial base, and research and development activities today are every bit as important as those kinetic threats that the United States faced during the Cold War—and potentially more important. In fact, the complete dependence on advanced technology, and the interconnected nature of our critical systems and networks, increases the risk exponentially.

Bringing science and engineering-based solutions to cyberspace will require a significant investment of resources and the involvement of the *essential partnership* including government, industry, and the academic community. To meet a similar national challenge and threat in 1960, President Kennedy engaged the best and brightest from government, industry, and academia to do what most thought impossible—putting a man on the moon and returning him safely to Earth before the end of the decade. Eight short years later, we had accomplished the impossible. The clock is ticking and time is short. We have an opportunity to do what is necessary to protect our national treasure and defend the country in the brave new world of cyberspace.

In particular, the following recommendations are provided as part of a national strategy for building, deploying, and sustaining trustworthy secure systems for the United States:

- ***Near Term: Immediate Steps to Stop the Bleeding (1-2 years)***

  The federal government should lead by example by immediately:

  - Conducting an *asset valuation* of all federal data, information, and system assets to categorize and triage by consequence of loss (i.e., low-impact, moderate-impact, high-impact);[2]
  - Reducing the complexity (and attack surface) of deployed systems and networks by moving nonessential or less critical assets (e.g., data, applications, and services) to validated cloud service providers or other validated external service providers (i.e., eliminating the clutter that organizations must deal with in their protection strategies);
  - Prioritizing the remaining essential and critical assets; and
  - Applying system security engineering best practices to reengineer the organization's essential and critical systems and networks to: (i) increase penetration resistance to attacks; (ii) provide a capability to limit the damage to the organization if the attack is successful; and (iii) make the systems and networks survivable.[3]

- ***Mid-to-Long Term: Building a Trustworthy Secure Systems Infrastructure (3-10 years)***

  The federal government should lead a comprehensive public-private partnership to develop trustworthy secure systems for the United States. The partnership should include industry and the academic community and focus on a broad framework and foundation for trustworthy computing and a reasonable execution path for implementation. Activities include:

  - Developing trusted commercial operating systems and applications;
  - Developing trusted firmware and hardware platforms;
  - Building secure supply chain models and approaches;
  - Developing systems security engineering curricula in colleges and universities to ensure that the next generation systems developers possess the requisite knowledge, skills, and abilities to build trustworthy secure systems; and
  - Creating a national-level trustworthy computing framework to establish the basic foundation for building, deploying, and sustaining trustworthy secure component products and systems.[4]

[2] Federal Information Processing Standards (FIPS) Publication199, *Standards for Security Categorization of Federal Information and Information Systems*, provides a comprehensive approach to categorizing federal information and information systems based on a worst-case impact analysis and risk to organizational operations, assets, individuals, other organizations, and the Nation.

[3] NIST Special Publication 800-160, *Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, 2nd Public Draft, May 2016, provides a roadmap for conducting such reengineering activities.

[4] R. Bigman, *Building a Trusted Computing Foundation*, Input to the Commission on Enhancing National Cybersecurity, August 2016.

A national strategy for creating more trustworthy secure systems requires a holistic view of the problem space, the ability to bring to bear the concepts, principles, and best practices of science and engineering to solve the underlying cybersecurity problems, and the leadership and will to do the right thing—even when such actions may not be popular.