



REPORT TO THE PRESIDENT
IMMEDIATE OPPORTUNITIES
FOR STRENGTHENING THE
NATION'S CYBERSECURITY

Executive Office of the President
President's Council of Advisors on
Science and Technology

NOVEMBER 2013





REPORT TO THE PRESIDENT
IMMEDIATE OPPORTUNITIES
FOR STRENGTHENING THE
NATION'S CYBERSECURITY

Executive Office of the President
President's Council of Advisors on
Science and Technology

NOVEMBER 2013

About the President's Council of Advisors on Science and Technology

The President's Council of Advisors on Science and Technology (PCAST) is an advisory group of the Nation's leading scientists and engineers, appointed by the President to augment the science and technology advice available to him from inside the White House and from cabinet departments and other Federal agencies. PCAST is consulted about, and often makes policy recommendations concerning, the full range of issues where understandings from the domains of science, technology, and innovation bear potentially on the policy choices before the President.

For more information about PCAST, see www.whitehouse.gov/ostp/pcast.



The President's Council of Advisors on Science and Technology

Co-Chairs

John P. Holdren

Assistant to the President for
Science and Technology
Director, Office of Science and Technology Policy

Eric S. Lander

President
Broad Institute of Harvard and MIT

Vice Chairs

William Press

Raymer Professor in Computer Science and
Integrative Biology
University of Texas at Austin

Maxine Savitz

Vice President
National Academy of Engineering

Members

Rosina Bierbaum

Dean, School of Natural Resources and
Environment
University of Michigan

Christine Cassel

President and CEO
National Quality Forum

Christopher Chyba

Professor, Astrophysical Sciences and
International Affairs
Director, Program on Science and Global Security
Princeton University

S. James Gates, Jr.

John S. Toll Professor of Physics
Director, Center for String and Particle
Theory
University of Maryland, College Park

Mark Gorenberg

Managing Director
Hummer Winblad Venture Partners

Shirley Ann Jackson

President
Rensselaer Polytechnic Institute

Richard C. Levin

President Emeritus
Frederick William Beinecke Professor of
Economics
Yale University

Chad Mirkin

George B. Rathmann Professor of Chemistry
Director, International Institute for
Nanotechnology
Northwestern University

Mario Molina

Distinguished Professor, Chemistry and
Biochemistry
University of California, San Diego
Professor, Center for Atmospheric Sciences at the
Scripps Institution of Oceanography

REPORT TO THE PRESIDENT IMMEDIATE OPPORTUNITIES
FOR STRENGTHENING THE NATION'S CYBERSECURITY

Craig Mundie

Senior Advisor to the CEO
Microsoft Corporation

Ed Penhoet

Director, Alta Partners
Professor Emeritus, Biochemistry and Public
Health
University of California, Berkeley

Barbara Schaal

Mary-Dell Chilton Distinguished Professor of
Biology
Washington University, St. Louis

Eric Schmidt

Executive Chairman
Google, Inc.

Daniel Schrag

Sturgis Hooper Professor of Geology
Professor, Environmental Science and
Engineering
Director, Harvard University Center for
Environment
Harvard University

Staff

Marjory S. Blumenthal

Executive Director

Ashley Predith

Assistant Executive Director

Knatokie Ford

AAAS Science & Technology Policy Fellow



PCAST Cybersecurity Working Group

William Press

Raymer Professor in Computer Science and
Integrative Biology
University of Texas at Austin

Craig Mundie

Senior Advisor to the CEO
Microsoft Corporation

Working Group Staff**Lauren Van Wazer¹**

Assistant Director, Cybersecurity
Office of Science and Technology Policy

David Pritchard

Senior Director, Chief of Staff
Microsoft Corporation

1. Lauren Van Wazer left OSTP in March 2013.



EXECUTIVE OFFICE OF THE PRESIDENT
PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY
WASHINGTON, D.C. 20502

President Barack Obama
The White House
Washington, DC 20502

Dear Mr. President,

We are pleased to send you this report, *Immediate Opportunities for Strengthening the Nation's Cybersecurity*, prepared for you by the President's Council of Advisors on Science and Technology (PCAST). The document points to areas where executive action can accelerate progress toward protecting the Nation's information systems and assets—a topic of growing concern given that society and the economy have become increasingly dependent on Internet-connected devices and information systems.

Through consultation with its membership and other experts, PCAST's examination of U.S. cybersecurity first produced a classified report on the issue, which was delivered to you in February 2013. This unclassified report is not a comprehensive assessment of the Nation's cybersecurity needs and opportunities, but it makes key insights from that analysis available to a wider audience.

A key conclusion is that, given the increasingly dynamic nature of cybersecurity threats, it is important to adopt protective processes that continuously couple information about evolving threats to defensive reactions and responses; static protective mechanisms are no longer adequate. PCAST recommends that the Federal Government lead by example and improve its own processes to combat cyberthreats. PCAST also recommends a number of approaches to encourage greater adoption of secure practices in the private sector, including leveraging existing regulatory frameworks and focusing on auditable processes of continuous improvement rather than on list-based mandates that encourage a “check-the-box” mentality and provide incentives for minimal compliance.

PCAST also illuminates potential expanded roles for key Federal agencies, such as the National Institute of Standards and Technology, including facilitating the voluntary sharing of information among private-sector entities and enabling approaches for Internet Service Providers to engage their users on issues of cybersecurity. Finally, PCAST recommends that the Federal Government invest in high-risk, high-return basic research with a 10-to-20-year time horizon that, if successful, could fundamentally transform the future cybersecurity landscape.

PCAST is grateful for the opportunity to serve you and the country in this way and hope that you and others who read this report find our analysis useful.

Best regards,

John P. Holdren
Co-chair, PCAS

Eric S. Lander
Co-chair, PCAST



Table of Contents

I. Summary of Findings and Recommendations	1
II. Introduction	5
III. Hardening Efforts Need Attention	7
IV. A National Strategy Can Accelerate the Adoption of Best Practices.	9
4.1 Mandate Processes, Not Checklists	9
4.2 Promote Creation of a Cyber-Safety Culture.	11
V. Dynamic, Real-Time Response Has Become Essential	13
VI. New Engineering Methodologies and New Software Architectures Are Needed	17



I. Summary of Findings and Recommendations

PCAST's report can be summarized by one overarching finding and six additional numbered findings. Recommendations follow from each of those six. The main report text gives background and further elaboration.

Overarching Finding: Cybersecurity will not be achieved by a collection of static precautions that, if taken by Government and industry organizations, will make them secure. Rather, it requires a set of processes that continuously couple information about an evolving threat to defensive reactions and responses.

The additional findings and associated recommendations are as follows.

Finding 1: The Federal Government rarely follows accepted best practices. It needs to lead by example and accelerate its efforts to make routine cyberattacks more difficult by implementing best practices for its own systems.

Recommendations:

- Phase out within two years the use of unsupported and insecure operating systems, such as Windows XP, in favor of modern systems, such as current versions of Windows, Linux, and Mac OS.
- Encourage the universal adoption of the Trusted Platform Module (TPM; an industry-standard microchip designed to provide basic security-related functions, primarily involving encryption keys), including for phones and tablets.
- Encourage the universal adoption of the latest, most secure browsers to facilitate prevention of identity theft.
- Move toward nationwide availability of proofed identities for people, roles, devices, and software. While voluntary in the private sector, these should be mandatory for transactions and data exchanges among Federal users.
- Encourage effective Federal use of automatically updating software, including cloud-hosted software, both for COTS and GOTS² products.

Finding 2: Many private-sector entities come under some form of Federal regulation for reasons not directly related to national security. In many such cases there is opportunity, fully consistent with the intent of the existing enabling legislation, for promoting and achieving best practices in cybersecurity.

2. The acronyms are "commercial off-the-shelf" and "government off-the-shelf," respectively.

Recommendations:

- Within already regulated industries, the regulator should require not a specific list of cybersecurity measures but rather an auditable process by which cybersecurity best practices are adopted and continually improved.
- The President should strongly encourage independent regulatory agencies to adopt regulations that require self-reporting of continuous-improvement practices along these same lines. In particular, the Securities and Exchange Commission (SEC) should mandate, for publicly held companies, the disclosure, as investment risks, of cybersecurity risk factors that go beyond current materiality tests.

Finding 3: Industry-driven, but third-party-audited, continuous-improvement processes are more likely to create an effective cybersecurity culture than are Government-mandated, static lists of security measures.

Recommendation:

- For the private sector, Government's role should be to encourage continuously improving, consensus-based standards and transparent reporting of whether those standards are being met by individual private-sector entities.

Finding 4: To improve the capacity to respond in real time, cyberthreat data need to be shared more extensively among private-sector entities and—in appropriate circumstances and with publicly understood interfaces—between private-sector entities and Government.

Recommendation:

- The Federal Government should act to facilitate the establishment of private-sector partnerships for the real-time exchange of threat data among potentially vulnerable private-sector entities. Data flows among these private-sector entities should not and would not be accessible by the Government. The Government might participate in establishing protocols, or providing technology, for how the data are utilized by the private sector for cyberdefense. The protocols or technology utilized should have sufficient transparency to mitigate legitimate concerns about inappropriate Government access to private data.

Finding 5: Internet Service Providers are well-positioned to contribute to rapid improvements in cybersecurity through real-time action.

Recommendations:

- The Federal Government should establish policies that describe the desired behavior by ISPs as best (or minimum-acceptable) practices.
- The National Institute of Standards and Technology (NIST) should work with ISPs towards establishing standards for voluntary measures by which ISPs can alert users and direct them to appropriate resources when their machines or devices are known to be compromised.

I. SUMMARY OF FINDINGS AND RECOMMENDATIONS

Finding 6: Future architectures will need to start with the premise that each part of a system must be designed to operate in a hostile environment. Research is needed to foster systems with dynamic, real-time defenses to complement hardening approaches.

Recommendations:

- The Nation's research universities and industry laboratories should be more directly partnered in the creation of high-assurance computing systems, including hardware, firmware, and the complete software stack.
- An independent organization should be tasked with the development of certifiable maturity levels with respect to threat-aware design processes for companies that design hardware and software.
- The Nation should invest in high-risk, high-return basic research with a 10-to-20-year time horizon that, if successful, could fundamentally transform the future cybersecurity landscape.



II. Introduction

Cyberthreats span the range from cybercrime (with global economic damage estimated at \$100 billion to \$1 trillion annually³) to potentially devastating cyberattacks against U.S. critical infrastructure, both civilian and military. In peacetime, cyberspace without adequate cybersecurity is a sanctuary from which criminal hackers, spammers, viruses, botnets,⁴ and other cyberthreats prey daily and openly on U.S. individuals and organizations. The Nation's capacity for innovation and commerce, including time-to-market advantages for commercial products and unique U.S. technologies for national defense, is drained by cyber industrial espionage and theft. In wartime, cyberspace can become another platform from which strategic attacks can be launched against the U.S. homeland and U.S. allies and interests abroad; cyber operations against U.S. forces can severely degrade military capabilities. Over the long term, national security depends on sustained economic security. If the Nation does not move aggressively to defend against these cybersecurity-induced disruptions and losses, that economic security will be susceptible to disruption on a timescale and breadth previously not imagined, due to the pervasive dependencies our society now has on information technologies of large scale.

The Internet provides unprecedented scalability of actions by a single individual,⁵ non-state group, or hostile nation. A single computer on the Internet can easily attack millions of other computers. The Internet protocol is designed to be globally interoperable with a range of devices—one of the key reasons for its explosive growth, adoption, and pace of innovation—but as a result it allows promiscuous connections to be made without authentication. Indeed, the Internet protocol was designed virtually assuming that all users were trustworthy. And, far beyond the scale of a single machine, botnets enable hostile actions by millions of machines simultaneously.

Steady progress has been made in the domains of discovery, remediation, and hardening in the traditional computing environment, but a tidal wave of new devices, from smartphones and computerized in-car systems to a wide range of smart sensors and other objects, is coming online. Few of these are being introduced with acceptable levels of cybersecurity. In a globally connected society, users of compromised machines and devices put not only their own systems and information at risk but also those of other Internet users. Compromised devices are vectors for the additional spread of malware, and they can be recruited into botnets and other systematic mechanisms for immediate or eventual (weeks, months, or years later) massive cyberattacks on U.S. companies or U.S. critical infrastructure.

The heterogeneous ownership and control of devices connected to the Internet makes it difficult-to-impossible to implement security fixes rapidly and uniformly. The highly cross-connected (and to some extent dynamic) nature of the Internet's interior dictates that most security measures need to be applied

3. Center for Strategic and International Studies. "The Economic Impact of Cybercrime and Cyber Espionage." July 2013 <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf>.

4. Botnets are sets, sometimes numbering as many as millions, of private computers infected with malicious software and controlled as a group without their owners' knowledge.

5. For example, in November 2010, the arrest in Russia of a single individual caused global email spam to drop (temporarily) by 20%. See: Kramer, Andrew E. "E-mail Spam Falls After Russian Crackdown." The New York Times. Web. 26 Oct. 2010 <http://www.nytimes.com/2010/10/27/business/27spam.html>.

REPORT TO THE PRESIDENT IMMEDIATE OPPORTUNITIES
FOR STRENGTHENING THE NATION'S CYBERSECURITY

at or near the endpoints. The challenge is that they must be adopted by literally billions of users and devices. There are few, if any, interior chokepoints at which it is possible to apply security measures with high effectiveness. For example, not all packets pass through Tier 1 (toplevel Internet network) backbone interconnects; those that do are frequently encrypted, defeating most forms of security that depend on deep-packet inspection; not all Tier 1 providers are U.S. corporations; and, in any case, the U.S. Government largely lacks authorities to compel actions within the private sector.

These realities imply an overarching finding:

Cybersecurity will not be achieved by a collection of static precautions that, if taken by Government and industry organizations, will make them secure. Rather, it requires a set of processes that must continuously couple information about an evolving threat to defensive reactions and responses.

When this feedback loop has a timescale of weeks or years, it may be called “hardening,” which is the essence of currently accepted “best practices.” When it has a timescale of sub-second to minutes, it may be called “dynamic, real-time response,” or “fast reactive response,” or “network-based defense.” But both need to be pieces of a single, unified, national cyberdefense architecture whose top-level paradigm is that flows of information about threats are able to trigger appropriate responsive actions. A national cybersecurity policy needs to be comprehensive in addressing all of the relevant timescales. The emphasis of this report, however, is largely—though not exclusively—on measures such as hardening and other best practices that unfold on the longer timescales.



III. Hardening Efforts Need Attention

Much can be done to make attacks against the U.S. Government, industry, and individuals more difficult and to decrease both the actual and perceived lawlessness of the Internet.

In this activity, Government's role is to encourage and facilitate the broad adoption of known best practices for information technology (IT) management. Several initiatives in President Obama's first term were of this character: the trusted identities initiative,⁶ the three identified priorities for Federal cybersecurity,⁷ the consolidation of Federal access points, the electricity-sector maturity model,⁸ and voluntary steps taken to counter botnets.⁹ In the second term, the President also signed Executive Order 13636¹⁰ and Presidential Policy Directive 21,¹¹ which together supported a number of Executive actions focused on enhancing critical infrastructure cybersecurity, partnership, and standards development.

These are individually useful actions, but there is both need and opportunity for more assertive White House actions that accelerate progress.

Finding: The Federal Government rarely follows accepted best practices. It needs to lead by example and accelerate its efforts to make cyberattacks more difficult by implementing hardening practices for its own systems.

PCAST's recommendations in this area are:

- Announce a firm commitment to phase out within two years use by the Federal Government of insecure and potentially unsupported operating systems, such as Windows XP, in favor of modern systems, such as current versions of Windows, Linux, and Mac OS. These are vastly more secure, and they are likely to be more effectively patched in response to new threats. There is simply no excuse for the Federal Government to be such a poor leader by example. This action was also recommended by the Internet Security and Privacy Advisory Board (established by the Computer Security Act of 1987) by letter to the Office of Management and Budget (OMB) dated March 30, 2012.

6. See link associated with the National Strategy for Trusted Identities in Cyberspace in: Daniel, Michael. "Collaborative and Cross-Cutting Approaches to Cybersecurity." The White House Blog. Web. 01 Aug. 2012 <http://www.whitehouse.gov/blog/2012/08/01/collaborative-and-cross-cutting-approaches-cybersecurity>.

7. The three priorities are trusted Internet connections, continuous monitoring of Federal information systems, and strong (non-password) authentication. An updated White House blog posting is: Daniel, Michael. "Cross Agency Priority Goal: Cybersecurity." Web. 2013 <http://goals.performance.gov/content/cybersecurity>.

8. See link associated with the Electric Sector Capability Maturity Model in: Daniel, Michael. "Collaborative and Cross-Cutting Approaches to Cybersecurity." The White House Blog. Web. 01 Aug. 2012 <http://www.whitehouse.gov/blog/2012/08/01/collaborative-and-cross-cutting-approaches-cybersecurity>.

9. See link associated with End-User Cybersecurity Protection in: Daniel, Michael. "Collaborative and Cross-Cutting Approaches to Cybersecurity." The White House Blog. Web. 01 Aug. 2012 <http://www.whitehouse.gov/blog/2012/08/01/collaborative-and-cross-cutting-approaches-cybersecurity>.

10. Executive Order 13636. "Improving Critical Infrastructure Cybersecurity" Federal Register. vol. 78, no. 33, p. 11739. 12 Feb. 2013 <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

11. Presidential Policy Directive (PPD-21). "Critical Infrastructure Security and Resilience." Web. 12 Feb. 2013 <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

REPORT TO THE PRESIDENT IMMEDIATE OPPORTUNITIES
FOR STRENGTHENING THE NATION'S CYBERSECURITY

- Take steps, for example by Federal procurement preference, that encourage the universal adoption of the Trusted Platform Module (TPM), an industry-standard microchip designed to provide basic security-related functions, primarily involving encryption keys, including for phones and tablets. Computers and devices that incorporate a TPM are able to create cryptographic keys and encrypt them so they can be decrypted only by the TPM. A TPM provides this limited but fundamental set of capabilities that higher layers of cybersecurity can then leverage. Today, TPMs are present in many laptop and desktop personal computers. They are leveraged by enterprises for tasks like secure disk encryption, but they have yet to be incorporated to any significant extent in smartphones, game consoles, televisions, in-car computer systems, and other computerized devices and industrial control systems. This needs to happen for such devices to be “trustworthy” constituents of what is an increasingly interconnected device ecosystem.
- Similarly, encourage the universal adoption of the latest, most secure browsers to facilitate prevention of identity theft. The majority of attacks on computers involve password guessing and “phishing” (in which false information is placed in front of the user to motivate unintended disclosure of sensitive information). Behind the scenes, modern browsers such as Chrome, Safari, and Internet Explorer check for the most common ways of stealing information, and they also help verify that software being downloaded is from a secure site.
- Move toward nationwide availability of proofed identities for people, roles, devices, and software. The April 2011 White House paper, “National Strategy for Trusted Identities in Cyberspace,” offers an overview of identity issues, although its proposed “identity ecosystem” is dauntingly complex and has not yet seen significant adoption. For immediate impact, we recommend instead focusing on readily implementable approaches to creating trusted identities. One such approach is claims-based identity, which grants individuals multiple identities they can use in specific circumstances and is one way to avoid the privacy and civil-liberty issues inherent in schemes such as national identity cards. A claims-based model passes specific “claims” about an individual (e.g., date of birth, age) instead of that individual’s “whole” identity (e.g., all the data on a driver’s license). While voluntary in the private sector, use of proofed identities should be mandatory for transactions and data exchanges within the Federal Government.
- Encourage Federal use of automatically-updating software both for commercial and government off-the-shelf software (COTS and GOTS), and provide or endorse standards (e.g., created by the National Institute of Standards and Technology (NIST) or via the private-sector standards-setting process) for ensuring the transactional security of such updates. Cloud-hosted software, because it is updated uniformly for all users, is desirable in this regard. While some new attacks against software will succeed (“fool me once, shame on you”), old attacks should never succeed (“fool me twice, shame on me”). Leading by example, the Federal Government should embrace this principle.



IV. A National Strategy Can Accelerate the Adoption of Best Practices

4.1 Mandate Processes, Not Checklists, within Regulated Industries

The ability of the U.S. Government directly to impose cybersecurity standards across the millions (soon, billions) of domestic Internet-connected computers and devices is highly limited. Only a relatively tiny number of these devices are Government-owned or identifiably part of an industry that falls under existing Federal regulatory authorities. A perhaps larger, but still very small, fraction of these devices, while privately owned, may be identifiable as national critical infrastructure within the meaning of Executive Order 13636¹² and, as such, may be susceptible to some Federal regulation.

Finding: Many private-sector entities come under some form of Federal regulation for reasons not directly related to national security. In many such cases there is opportunity, fully consistent with the intent of the existing enabling legislation, for promoting and achieving best practices in cybersecurity.

We describe below just how this might work. PCAST's first caution, however, is that it is crucially important that such efforts not overstep their possible usefulness in any of three harmful ways:

- They must not be perceived as an effort to expand Federal regulatory reach to currently unregulated entities. For that reason, scope should be strictly limited to established boundaries of regulation, without advancement of novel legal theories proffered to stretch existing jurisdiction. Even a "voluntary" program for other industries, no matter how helpfully intended, may be perceived by industry as a problematic first step towards the assertion of new regulatory authorities.
- It would be an ineffective approach to create, within the Department of Homeland Security (DHS) or elsewhere, a centralized authoritative description of required cybersecurity measures. Such a list would rapidly become fossilized and bureaucratic, not just unproductive but counterproductive. Many examples of counterproductive mandated "check-off lists" exist.
- There needs to be a recognition that a one-size-fits-all approach will not work and that the focus needs to be on those elements that can have either impact at scale or cascading impact.

Recommendation: PCAST believes that, within already regulated industries, the preferred way to proceed is for the regulator to require not a specific list of cybersecurity measures but an auditable process by which cybersecurity best practices are adopted and continually improved.

12. The referenced Executive Order defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

REPORT TO THE PRESIDENT IMMEDIATE OPPORTUNITIES
FOR STRENGTHENING THE NATION'S CYBERSECURITY

For example, a regulated company should be required regularly to provide answers to these four questions:

1. How does the company determine what are the best practices for its industry?
2. What is the company's present state of conformity to those practices?
3. What is the company's plan and schedule for achieving full conformity?
4. How is the company ensuring that its best practices are improved and updated in response to evolving threats?

Since regulatory agencies will typically have the ability to comment, formally or informally, as to the adequacy of any company's specification, a constructive degree of encouragement could be adjusted on a company-by-company basis. Indeed, in tailoring the appropriate course and timing of actions with regard to a specific company or organization, careful consideration has to be given to the potential magnitude of consequences (including issues such as interdependency), or scaling effect, of a cybersecurity incident at an individual entity. NIST has an important convening role, on an ongoing basis, to assist with the development of an auditable process.

Publicly held companies that do not otherwise come under Federal regulation do come under regulatory authority of the Securities Exchange Commission (SEC), whose mission is to provide a level playing field for investors.¹³ In that context, the SEC has the authority to mandate the disclosure of business risks by public companies under various circumstances (e.g., Form 10Q disclosures). By accounting practice, disclosed risks are "material." There is generally no necessity for a company to disclose risks whose consequences are small.

Cyber, however, is a new frontier. Because cyber risks can cascade, and are correlated across the whole economy, traditional standards of materiality may be naïve. For the purpose of providing investors with necessary risk information, the SEC might justifiably mandate that companies larger than a certain size, or in certain key sectors, should routinely disclose their cyber risk in a format that evaluates their responses against the appropriate industry best practice. The four numbered questions above can provide the appropriate logical structure. Indeed, at the end of 2011, SEC staff issued guidance that is relevant to this area, a small first step. However, stronger action is necessary at the Commission level for full and mandatory effect.¹⁴

We note that New York State's Department of Financial Services has sent formal requests that the state's large banks and three dozen large insurance companies disclose details on their preparedness for

13. The consumer protection mission of the Federal Trade Commission, focused on countering deception and/or unfair business practices, provides another broad umbrella that has been used to encourage companies to do more to strengthen cybersecurity.

14. See, for example: Strohm, Chris. "SEC Chairman Reviewing Company Cybersecurity Disclosures." Bloomberg. Web. 13 May 2013 <http://www.bloomberg.com/news/2013-05-13/sec-chairman-reviewing-company-cybersecurity-disclosures.html>. For a different point of view, see: Mutch, John. "Beware The Coming SEC Regulations On Cybersecurity." Forbes. Web. 15 May 2013 <http://www.forbes.com/sites/ciocentral/2013/05/15/how-to-prepare-for-when-the-sec-comes-asking-about-cybersecurity-risk/>.

cyberattacks—requests that the recipients are legally obligated to answer.¹⁵ This action is consistent with our view of what needs to be done with greater uniformity at the Federal level.

Recommendation: The President should strongly encourage independent regulatory agencies to adopt regulations that require self-reporting of continuous improvement practices along the lines discussed above. Particularly, the Securities and Exchange Commission should mandate, for publicly held companies, the disclosure, as investment risk factors, of the answers to the above four numbered questions.

4.2 Promote Creation of a Cyber-Safety Culture across Industry Broadly

The difference between the Federal Government’s mandating specific, listed cyber practices—however such lists may be developed—versus its mandating auditable processes of continuous improvement, leaving the creation of best-practice specifics to the private sector, is worth further explication here. Either approach, at scale, will spawn the creation of a “compliance business,” comprising specialized firms (or units within companies) that will advise on the details of technical compliance.

List-based mandates are likely to lead to a compliance business that will perceive incentives to minimal compliance. The commercially successful advisors will be those who are able to “check the boxes” for their clients at minimal cost, with the most success at negotiating with regulators, or litigating, the least onerous set of requirements. Check-off lists lead to a race to the compliance bottom. Specifically, PCAST urges DHS and NIST to exercise great caution in developing risk assessments or industry-specific compliance lists. PCAST is particularly doubtful that such assessments and lists can usefully keep up with the evolving threat.

By contrast, continuous-improvement mandates can motivate a race to the top, because expert third parties have incentive to become a part of the consensus process for what best practices should be. Such third parties would be likely to include cybersecurity researchers, management-consulting firms, and investment analysts in the private sector, and should also include leadership by Federal agencies such as NIST.¹⁶ An industry that attempts to “get away with” practices inferior to those of another industry, and without a defensible industry-specific justification, will attract the attention of security professionals and others and produce pressure for improvement.

An analogous situation exists today in the human health and safety compliance business, where it has become accepted that the standard for companies in high-hazard activities should be founded on “safety culture,” not just on checklists, and where there is an active industry of consulting and research that brings together the two threads of safety culture and continuous improvement. Each of these threads has a nuanced and well-studied history: continuous improvement originating in the post-World War II work of statisticians W. Edwards Deming and Joseph M. Juran (who are credited with spurring Japan’s kaizen [continuous improvement] revolution in the 1950s), and safety culture exemplified by

15. Berkowitz, Ben. “NY Regulator Asks Insurers about Readiness for Cyber Threats.” Reuters. Web. 28 May 2013 <http://www.reuters.com/article/2013/05/28/usa-cybersecurity-insurance-newyork-idUSL2N0E919B20130528>.

16. An additional source of third-party expertise is the set of security-configuration guidelines for the prevalent ecosystem products that are published by the Information Assurance Directorate of the National Security Agency. The Federal Government should adopt these guidelines immediately for its own systems. See: The National Security Agency. “Security Configuration Guidelines.” Web. 16 Sept. 2013 http://cee.che.ufl.edu/AICHE_CEE_Klein_DuPont_Extended.pdf.

REPORT TO THE PRESIDENT IMMEDIATE OPPORTUNITIES
FOR STRENGTHENING THE NATION'S CYBERSECURITY

such American companies as DuPont.¹⁷ Federal policy should be designed to provide incentives for the analogous continually improving cybersecurity safety culture, rather than minimal compliance with a mandated, and likely soon-out-of-date, list.

Finding: Industry-driven, but third-party audited, continuous improvement processes are more likely to create an effective cybersecurity culture than are Government-mandated, static lists of security measures.

Recommendation: For the private sector, Government's role should be to encourage continuously improving, consensus-based standards and transparent reporting of whether those standards are being met by individual private-sector entities.

We note the U.S. General Services Administration's FedRAMP program as one effort at defining best practices (in this case, for cloud computing products and services) and using accrediting third-party assessors for auditing conformity to such practices.¹⁸ More recently, in response to Executive Order 13636 and Presidential Policy Directive 21, NIST has initiated a cybersecurity framework process that appears fully consistent with the intent of PCAST's finding.¹⁹

17. Klein, James A. "Two Centuries of Process Safety at DuPont." *Process Safety Progress*. vol. 28, no. 2, pp. 113-122. June 2009 http://cee.che.ufl.edu/AIChE_CEE_Klein_DuPont_Extended.pdf.

18. Federal Risk and Authorization Management Program (FedRAMP). http://www.gsa.gov/portal/category/102371?utm_source=OCSIT&utm_term=fedramp.

19. 18. "NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments." Press release, October 22, 2013. <http://www.nist.gov/itl/cybersecurity-102213.cfm>.



V. Dynamic, Real-Time Response Has Become Essential

The cybersecurity threat has changed dramatically, a shift that has been noted not just within the U.S. Government, but also by the private sector and internationally. While China's highly publicized intrusions have garnered the most attention,²⁰ the change has been recognized earlier and more broadly.²¹ It is now apparent that ongoing, concerted efforts at good hygienic and operational practices, even coupled to improved hardening by the software developers and advanced intrusion detection and anti-malware systems, will not be sufficient to protect computer systems from advanced forms of cyber-attacks.

Specifically, some forms of cyber-attack are designed to propagate at very high rates, and the non-real-time nature of the various forms of hardening, updates, and delivery of signatures means that these approaches do not provide for the rapid and widespread reaction needed to prevent serious damage. This shortcoming has been compounded by the rapid diversification of the types of devices that are attached to the Internet, including phones, tablets, automobiles, and a wide variety of consumer appliances. Most of these devices have not been designed with sophisticated hardening or other types of defense mechanisms. This leaves them particularly vulnerable to dynamic alteration of the applications running on them. These vulnerabilities become all the more worrisome in light of the trend, in the kinds of attacks being mounted, toward destructive malware as opposed to network-based denial-of-service attacks.

The biggest practical challenges lie in predicting or recognizing the attack and determining how to mitigate it in real-time. In this connection, the fact that so much of cyberspace is in the hands of the private sector motivates interest in finding ways to interconnect its monitoring, surveillance, and forensic capabilities with those of the Government. Doing so would be challenging technically, however, as well as subject to legal and policy constraints that currently exist both within the United States and internationally.

20. Examples include: Perlroth, Nicole. "Hackers in China Attacked The Times for Last 4 Months." The New York Times. Web. 30 Jan. 2013 <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&r=0>; Perlroth, Nicole. "Wall Street Journal Announces That It, Too, Was Hacked by the Chinese." The New York Times. Web. 31 Jan. 2013 <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&r=0>; Perlroth, Nicole. "Washington Post Joins List of News Media Hacked by the Chinese." The New York Times. Web. 1 Feb. 2013 <http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html>; Sanger, David E., David Barboza, and Nicole Perlroth. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." The New York Times. Web. 18 Feb. 2013 <http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all>; and Mandiant Corporation. "APT1: Exposing One of China's Cyber Espionage Units." 2013. <http://intelreport.mandiant.com/>.

21. Examples include: For example: Gjelten, Tom. "Cybersecurity Firms Ditch Defense, Learn to 'Hunt.'" NPR Morning Edition. Web. 10 May 2012 <http://www.npr.org/2012/05/10/152374358/cybersecurity-firms-ditch-defense-learn-to-hunt>; Nakashima, Ellen. "Cybersecurity should be more active, official says." The Washington Post. Web. 16 Sept. 2012 http://articles.washingtonpost.com/2012-09-16/world/35494752_1_top-cyber-private-sector-crowdstrike; Perlroth, Nicole. "Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt." The New York Times. Web. 31 Dec. 2012 <http://www.nytimes.com/2013/01/01/technology/antivirus-makers-work-on-software-to-catch-malware-more-effectively.html?pagewanted=all>.

REPORT TO THE PRESIDENT IMMEDIATE OPPORTUNITIES
FOR STRENGTHENING THE NATION'S CYBERSECURITY

For example, the Electronic Communications Privacy Act of 1986 (ECPA, 18 USC 2702) prohibits private-sector entities providing electronic communication services from disclosing customer information (such as identity) to the Government, even when the entity observes illegal activity by the customer, and even when it is in the broader interest of its other customers that law enforcement be informed. ECPA provides only a small number of designated exceptions to this general prohibition (see below). Today, customers include virtually all users of the Internet, and communication services encompass virtually all uses of the Internet. Although the so-called business-records provision of the USA PATRIOT Act (50 USC 1861) may have authorized the release of some customer data to Government, it seems likely to remain the case that use of data available to the private sector will be primarily by the private sector itself. Rather than attempting to prognosticate the likelihood, or even direction, of future legislative changes, PCAST restricts its proposed recommendations to those that seem feasible now.

Finding: To improve the capacity to respond in real time, cyberthreat data need to be shared more extensively among private-sector entities and—in appropriate circumstances and with publicly understood interfaces—between private-sector entities and Government.

By its original intent, ECPA does not regulate communications purely among private-sector entities; it applies only to communications with the Government, and it explicitly exempts disclosures “to any person other than a Governmental entity.” Moreover, it is among private-sector entities that the exchange of threat information is now most badly needed. Some nascent private-sector organizations are attempting to fill this need.²²

Recommendations:

- The Federal Government should act to facilitate the establishment of private-sector partnerships for the real-time exchange of threat data among potentially vulnerable private-sector entities. Data flows among these private-sector entities should not and would not be accessible by the Government. The Federal Government might participate in establishing protocols, or providing technology, for how the data are utilized by the private sector for its own cyberdefense. The protocols or technology utilized should have sufficient transparency to mitigate legitimate concerns about inappropriate Government access to private data.

Finding: Internet Service Providers are well-positioned to contribute to rapid improvements in cybersecurity through real-time action.

Internet Service Providers (ISPs) are well-positioned, both technically and by their relationship with their customers, to contribute to rapid improvements in cybersecurity that exploit dynamic, real-time response possibilities.²³ The ISPs control the actual connection of their customers to the Internet—the so-called first hop. As just one example, ISPs are uniquely able to do ingress validation, checking that the connected machine is identifying itself honestly. In some situations, ISPs have both the means to detect compromised machines quickly (for example, machines recruited into a botnet) and the ability to do something about them—for example, to notify the customer and provide options for fixing the

22. Martinez, Jennifer. “Former DHS deputy secretary launches cybersecurity council.” The Hill. Web. 14 Aug. 2012. <http://thehill.com/blogs/hillicon-valley/technology/316611-former-dhs-deputy-secretary-launches-cybersecurity-council>.

23. Where customers have more than one choice of ISP, they are able to choose the one that offers, in their view, the greatest value or trust. This makes the relationship to some degree voluntary rather than imposed.

problem. Lacking both a legal obligation to act and any protection against subsequent liability, however, such action by ISPs is quite rare. This needs to be changed.

Recommendations:

- The Federal Government should establish policies that describe the desired behavior by ISPs as best (or minimum-acceptable) practices.
- The National Institute of Standards and Technology (NIST) should work with ISPs towards establishing standards for voluntary measures by which ISPs can alert users and direct them to appropriate resources when their machines or devices are known to be compromised.

It would not make sense to take actions that break the business model of ISPs, for example by requiring large new investments in expensive customer service or by creating ill-will with customers. But ISPs could offer, as a competitive or revenue opportunity, additional services that could be provided immediately, even on compromised machines—for example, controlled web browsing and access to email. Many customers might pay another dollar or two monthly for the guarantee of such services, a kind of cybersecurity insurance policy. Analogous products for compromised cell phones and other devices could also be provided.



VI. New Engineering Methodologies and New Software Architectures Are Needed

In the long run, if cyberthreats are to be countered effectively, the Nation's approach to systems architectures must be rethought.

Finding: Future architectures will need to start with the premise that each part of a system must be designed to operate in a hostile environment. Research is needed to foster systems with dynamic, real-time defenses to complement hardening approaches.

These principles apply to all levels of the "technology stack" (i.e., the layers of components or services that make up the connected system in question), and must include the hardware itself, plus the firmware and software layers that are built on top.

Recommendations:

- The Nation's research universities and industry laboratories should be more directly partnered in the creation of high-assurance computing systems, including hardware, firmware, and the complete software stack.
- An organization should be tasked with the development of certifiable maturity levels with respect to threat-aware design processes for companies that design hardware and software. The Software Engineering Institute (SEI), a Federally Funded Research and Development Center with a Department of Defense (DoD) charter, could be so tasked by DoD. A separate hardware- or networking-related activity may also be needed, perhaps at MITRE Corporation's National Security Engineering Center, which also has a DoD charter. Microsoft's publicly available Security Development Lifecycle (SDL) is achieving significant adoption in the private sector and could be a starting point. The certification of maturity levels has proved to be an effective means for driving best engineering practices, and it should be harnessed in service of cybersecurity.
- In addition to these intermediate-term cybersecurity R&D activities, the Nation should invest in high-risk, high-return basic research with a 10-to-20-year time horizon that, if successful, could fundamentally transform the future cybersecurity landscape.



President's Council of Advisors
on Science and Technology

www.whitehouse.gov/ostp/pcast

