Fixing America's Cybersecurity:

A Plan for

Cyber Policy and Organization

Prepared for the

Trump-Pence Transition Team

Rev. 4.0 (1-13-2017)

Fixing America's Cybersecurity:
A Plan for Cyber Policy and Organization

Preface

Cyber espionage, cyberwarfare, and attacks on vital domestic systems are among the most serious and dynamic threats facing the United States. Current policy, organization and programs have failed to meet these growing threats and need to be radically changed to successfully manage these critical challenges. The Trump administration will take America's cybersecurity into the next generation, but can only succeed by building a stronger bi-partisan political consensus concerning these threats and making needed organizational and policy changes.

Continued failure in the area of cybersecurity will have ongoing and potentially disastrous consequences. Cyberespionage continues while threats of major cyberwarfare are dramatically increasing. American companies cannot compete on a fair playing field internationally, or even domestically, when their operational data and intellectual property are stolen and vital power, water, and communications systems are held hostage to foreign cyber armies. Just as America failed to heed advanced warning of terrorist attacks on the United States, the nation has also failed to adequately protect its vital cyber interests.

The following plan includes several essential actions that should be taken within the first 100 days of the Trump Presidency, and defines a long-term path to meet these challenges.

Introduction

A. The Cyber Landscape

The cyber landscape includes all of the infrastructure, information, and intelligence relating to, or derived from, cyber activity. Recognizing the character of the cyber landscape and addressing the challenges it poses are matters for Presidential leadership, Congressional support, and private sector inclusion. No one branch of government or organization alone can define and meet the challenge.

America inhabits a cyber landscape that defies national boundaries. Modern life is so completely conducted through computers and devices of every size and function that the

cyber landscape is at the top of, and dominates, a pyramid of familiar and conventional technological and non-technological landscapes. It requires changes to traditional modes of analysis that have worked in other domains, including distinctions between offense and defense, access and assurance, and intelligence operations and information warfare. This context stretches the language, analogies, and understanding of modern society, while the complexity of the cyber landscape dictates that there can be no single cyber policy for all contexts and contingencies.

The cyberlandscape consists in three distinct tiers:

Infrastructure: The infrastructure of the cyber landscape comprises privately and publicly-owned energy supply systems, electric power grids, communications networks, data centers and software on which the government and citizenry all depend. This heterogeneous infrastructure incorporates a vast spectrum of subsystems ranging from old, pre-Internet technology that is inherently cyber-safe, through the extremely cyber vulnerable and out-of-date, to cutting-edge technologies, which, if combined appropriately, holds the promise of improved cyber security.

Information: Infrastructure exists for the purpose of storing, transporting, and transforming information. Information in this cyber landscape crosses borders and sectors and comprises the spectrum of highly essential to trivial content, and from personal through economic or business-related, to defense or national security information. The cyber landscape is such that the traditional boundary between foreign and domestic disappears for most practical purposes. The American government must accept this reality and the legal and policy regimes as well as organizational arrangements must reflect it.

Intelligence: Great value is derived through the analysis and contextualization of information gathered in the cyber domain from both open and closed sources. Intelligence products of this type have become increasingly essential to national security and law enforcement. Data collected by companies such as Google, Facebook, and Twitter, run the gamut from the innocuous to the personal, and are often used to create new products or to enhance marketing of existing ones. Sinister uses of cyber information are also a reality. Legislation is needed but inevitably will affect U.S. businesses and individuals and, therefore, must be carefully crafted.

The cyber landscape is highly dynamic. As the technologies that defined this area in the 1960s now seem antique, the technologies of today will continue to be superseded. The large installed base embodying existing technologies now limits the speed with which

fundamental technology-based security improvements can be achieved. One focus of policy must be to guide technology deployments to achieve an installed base that is more conducive to security improvements in place without introducing new vulnerabilities. The cyber landscape will certainly be different five or ten years from now, and America's cyber programs must be structured in light of the evolving trends, and not be a static concept of today's threats and technologies.

B. The Cyber Challenge

Cybersecurity is one of the greatest challenges facing America today, and yet for almost eight years the White House has failed to provide strong public, intergovernmental, business, or even executive branch leadership on these issues. The cyber domain is a vital component – and generally a vulnerability – of all sixteen critical infrastructure sectors in the United States. Current policy is based on misperceptions of cyber threats and assigns responsibility to agencies incapable of meeting the challenges. As a direct consequence of these failures, Americans' privacy and security have been repeatedly violated; national security threatened; and commerce disrupted. The threat of greater cyberwarfare looms larger every day.

In recent years, China, Russia, Iran, North Korea and others have attacked U.S. government agencies, businesses and citizens in cyberspace with relative impunity. China has stolen billions of dollars' worth of intellectual property, technology, and research from American firms and institutions, costing tens of thousands of U.S. jobs. Iran has disabled the online banking system with denial-of-service attacks repeatedly over two consecutive years, and has even broken into a hydroelectric dam in New York State. North Korean intimidation shut down a U.S. film release, while infiltration of America's government and military networks by Russia and others grows ever more brazen. In addition to nation-state threats, terror and other non-state groups, such as ISIS, are committed to leveraging and developing capabilities in the cyber domain.

Why Has America Failed to Meet the Cyber Challenge?

Cybersecurity must address true nature of cyber threats. It will require, bi-partisan, national consensus to do so. The lack of such consensus to date has prevented enhancement of cybersecurity and development of effective national policies. Without such understanding it has been impossible to develop policies and programs to deal with present and foreseeable future realities. To enhance cybersecurity, it is essential to identify and deal with the real threats as well as ongoing problems and policy recommendations

previously made. Still missing however, is a basic statement of why these policies have failed to meet the challenge. Major reasons for prior failure are:

- **The Real Threat is Largely Ignored:** Cyberspace has not been treated as an important national resource. As the Internet and cyberspace grew from a 1960s Defense Department experiment to a vital national resource security problems were widely recognized but effective solutions required more political will, technical focus, and effective collaboration with the private sector than was mustered Current programs are inadequate, and largely ineffective in meeting the evolving challenge.

- **The Internet is Inherently Vulnerable.** The Internet still operates on protocols developed in the 1960s that are inherently highly vulnerable and not appropriate for the role the internet plays in 21st century society, commerce, and national security. A modern Internet architecture is needed to meet the current challenge, and in the meantime we need to utilize automated systems to detect and deal with evolving cyber threats in real time.

- **Effective, Comprehensive National Cyber Policy:** It is essential to assign Federal government cybersecurity responsibilities Existing Presidential Directives such as PPD-20, PPD-21 and PPD-41 do not assign critical cybersecurity missions to government agencies capable of marshalling the resources needed to discharge them. That is simply not the case today. Cyber defense and offense cannot be separated.

- **Cybersecurity is Grossly Underfunded:** For over a decade policy has been made on the incorrect assumption that private industry, led by the technology sector, would develop means to address major vulnerabilities or that "the market" would respond to consumer demand for increased security and thus would achieve a certain degree of self-correction. This never happened, and partly because they were based on this assumption, federal programs have proved to be inadequate.

- **The United States has Failed to Include Industry as a Full Partner:** Solving cybersecurity problems requires a strong partnership with the

technology sector, the financial sector, and others. This partnership involves funded programs, data sharing, security clearances and other key elements. Without a full and genuine partnership government efforts are doomed to failure. Corporate actors have many incentives that inhibit this cooperation, including potential liability for revelations that they are not meeting a higher standard of care, and differences over past government efforts to develop back-door access to information. Strong, informed, and discerning leadership capable of making key and durable policy trade-offs and commitments is a necessary basis for this partnership to succeed.

- **Law Enforcement is Not Adequately Supported:** State and local law enforcement agencies suffer acutely from weaknesses in information management, delivery, and analysis, as well as in technical knowledge training and development. While breaches of these agencies have not been prominent in the news they are a real possibility as they increase their reliance on technology. More immediately, state and local agencies lack competence and resources to keep up with crimes committed or abetted through the cyber domain or to access cyber evidence for investigating and prosecuting ordinary crimes. Significant additional support is required from the federal government to address these deficiencies.

- **Existing Statutes are Inadequate:** Statutes written during the Cold War cannot accommodate the realities of cyberwarfare and cybersecurity. Failure to understand and incorporate into law and policy the unique, borderless qualities of the domain imperil offensive and defensive cyber operations, as well as the integrity of existing legal structures. Valid concerns about privacy and individual rights as well as fears of an intrusive government must be addressed in order to move forward to an effective policy based on a coherent legal regime.

C. What America Must Do

America must lead the world in cybersecurity and cyber capabilities. To get the cybersecurity problem under control requires a number of crucially important The Trump

Administration must take several critical steps to make the nation more secure and resilient in the cyber domain:

- **NSC Responsibility: Get the Cybersecurity Problem Under Control:** Because the National Security Council (NSC) is the President's instrument for managing the national security process, the President should appoint a senior NSC staff member with the responsibility to take charge of an ongoing analytic, policy, and programmatic operation capable of meeting the real threats with effective solutions. The proper analogy is that America must face cybersecurity as it did the threat of strategic nuclear warfare.

- **Build a Strong Political Consensus to Support Cyber Security**. A reformed statutory basis and stronger relationships with the private sector and state and local government agencies is necessary means that no amount of greater perspicacity and coherence within the Executive branch can succeed on its own. To build a strong and enduring consensus, the administration must head off potential turf wars among cabinet departments (and their congressional allies) and reach out to opinion leaders in corporate America, academia, and political leaders in Congress and the States.

- **Meet the Challenge of Cyber Conflict:** The nation needs the strongest offensive capabilities possible to facilitate a full suite of law enforcement activities domestically, as well as espionage, information and perception operations, and targeted access activities overseas. Integration of cyber defensive and offensive missions and operations is essential, and must be accomplished within the Department of Defense.

- **Replace Out-Dated Critical Infrastructure:** A modern architecture for the Internet needs to be developed. Better standards are needed for critical infrastructure sectors, as is a greater level of support to make vital networks as secure and resilient as possible. Automated systems for the detection of cyber threats and deploying countermeasures on a real-time basis are essential. Significant capital expenditure must be authorized to

enable replacement rather than maintenance of vulnerable legacy systems inside the federal, state, and local governments.

- **Empower the Private Sector:** The private sector must be empowered to work in concert with the military, intelligence, and law enforcement services to respond to new and known cyber threats. Included here are, not only the technology firms and service suppliers, but also the financial sector, insurance companies, and health care operations which have major data operations and constantly see threat data.

- **Build a Cyber Workforce:** America requires a workforce capable of understanding and confronting risks and threats arising from the cyber domain. The government must create the adequate incentives in both pay and recognition for our nation's most talented cyber-experts, the front-line of the future cyber workforce, to address the nation's greatest challenges.

- **Build the Partnership with Industry:** The technology sector, financial sector and others are essential partners in meeting the challenge of effective cybersecurity. They must be empowered to work in concert with the military, intelligence, and law enforcement services to respond to new and known cyber threats. This will require funding, security clearances, and a classified network for data sharing.

- **Create a Responsive Security System:** Personnel working in industry, the financial sector, and law enforcement need timely and cost-effective access to cyber data. A far larger number need to be cleared at the "Secret" level, which is far less-costly and more rapid than Top Secret or SCI access. Cyber data needs to be downgraded to this level, and a new classified network (CYBERNet) created to support these sectors for the timely sharing of critically important cyber threat data. Costs of clearance processing should be a part of future government contracts.

- **Protect Digital Privacy:** Increasing hacks and theft of data, as well as legitimate surveillance programs important to national security have

raised concerns among many Americans. New programs need to protect privacy interests as well as meet intelligence and law enforcement needs.

- **Recognize that the World is Going Dark:** Computer systems and applications are rapidly adopting encryption schemes to meet user demands for privacy and security. Legislation to prevent this development or work around it is doomed to failure, as this is a worldwide phenomenon and a technology path that cannot be stopped. America must support specialized technical programs that meet this reality.

- **Support Law Enforcement:** State and local law enforcement are also important partners in cybersecurity. In addition to adopting a joint task force model, the federal government will enhance data sharing and technical support. Robust funding for a national forensics and training laboratory available to all U.S. law enforcement agencies will help them overcome technological obstacles to their investigations.

- **Internet Governance:** The growing field of Internet governance addresses several issues – some real and some imagined. America must resist efforts purported to wrest "ownership" and "control" of the Internet. Greater state control of the Internet is not needed and could be counterproductive. America should support efforts designed to increase global security, including robust privacy protections built into all cyber activities, as well as severe sanctions on nations that fail to prosecute cybercrime.

- **Repudiate Bad Deals:** Agreements such as the Wassenaar Arrangement do not serve America's interests and only harm the technology sector. Experts agree that sections of this Agreement, never approved by the Senate, may cripple our ability to develop important security software.

Protect America's Intellectual Property: America can no longer allow other nations to steal the intellectual property of U.S. companies. The U.S. will partner with and empower American companies to increase security against all cyber threats including the theft if intellectual property by electronic means.

1. Getting the Cybersecurity Problem Under Control

Current national policy on cybersecurity falls short. Despite some attention to cyber threats, the Government has failed to assign responsibility to agencies capable of managing and implementing the needed solutions, or adequately funding programs to accomplish these goals. Cybersecurity includes effective cyber offense and defense capabilities; protecting connected infrastructure; securing the privacy of user data; protection of servers and systems from hostile attack; maintaining the integrity of the Internet infrastructure itself; and deterring capable foreign actors including foreign governments from exploiting system vulnerabilities.

We recommend that the United States take the prospect of cyberwarfare seriously, as the nation did with strategic warfare in an earlier generation, and use the successful model developed for the strategic nuclear threat in dealing with the problems of cybersecurity. This includes:

- **Create a Cyber Threat Assessment and Analysis Capability to Support Coherent Policy and Coordinated Action:** An ongoing analytical and policy development process, directed from the White House that fully engages and supports the research community.

- **Assign Key Missions and Responsibilities Consonant with Capability:** Presidential action that assigns critical cyber defense and offense missions to the Department of Defense. This is the only government agency actually capable of performing these missions in terms of programmatic infrastructure, and having the legal authority do to so. It is also the case that defense and offense cannot be separated and left to two separate departments. DHS, Commerce and other federal agencies will continue to have significant supporting roles, described in greater detail in the Appendix to this report.

- **Adequately Fund Essential Cybersecurity Programs:** The Trump Administration must work with the Congress to provide needed funding for not only cybersecurity research, but development of operational programs for cyber offense and defense. Work in this area must recognize that what is needed is a highly dynamic process, where new cyber threats continue to evolve and a robust research program developed that supports operational programs. Existing programs are grossly underfunded, incomplete and not well coordinated.

- **Forge a New Partnership with the Commercial Sector:** Effective cybersecurity cannot be achieved without full partnership with the technology sector, the financial sector and others. This includes needed funding, timely data sharing, security clearances and other elements to make the process operate effectively.

- **Update the Legal Regime:** Current federal law with respect to military operations, intelligence operations and privacy predate cyberspace and must be revised to take account of cybersecurity challenges. Making America and its systems safe is the highest priority for the future.

- **Support Law Enforcement:** State and local law enforcement face increasing cybersecurity challenges and need a cooperative mechanism as well as technical support to fight cybercrime and deal with new devices containing sophisticated security features. They also need security clearances and inclusion in the classified data sharing network.

Experts generally agree that cybersecurity problems will not be totally "solved," but that solutions to most severe threats can be implemented. The continuous development of new and more sophisticated attacks poses an ongoing threat. An effective response requires active management of vulnerabilities, surveillance of threats, and rapid response capabilities in real-time.

Solving cybersecurity problems also requires engaging the commercial sector as a full partner in the process. For years, the government failed to bring the private sector into the process of planning or implementing effective cybersecurity. Important issues of funding, security clearances, and data sharing – to name a few – were never fully resolved.

Simply analyzing and understanding the problem is not enough. Describing the problem in the hope that either the private sector or some government agency "pick up the ball and run with it" hasn't worked and won't. The Defense Department and other federal agencies assigned key missions must have the legal authority, resources and management infrastructure to accomplish their task. Along with this they need an explicit partnership with the private sector to make this happen.

Recommendations:

1.1 Designate a Senior Cybersecurity Manager: Within the Executive Office of the President designate a senior official with overall responsibility to direct and coordinate America's cybersecurity efforts. This could be under the NSC or follow the model of the Office of National Drug Control Policy (ONDCP), established as the Office of National Cybersecurity Policy (ONCP). The Director, ONCP should be charged by the President with the ongoing task of overseeing the analytic process as well as operational programs to meet America's cybersecurity challenge.

1.2 Institute an Ongoing Analytic Process: Initiate a major analytic, policy development and programmatic assessment of cyber threats and all related issues. This should be undertaken by the Department of Defense; the Intelligence Community, the Justice Department, the Department of Homeland Security and the Departments of Commerce and State. Supporting this effort should be experts from within the government as well as federal research institutions such as The RAND Corporation, the Institute for Defense Analyses as well as key technology firms such as Google, Microsoft, and others.

1.3 Assign Critical Cyber Defense and Offense Missions to the Defense Department: Obama Presidential Directives PPD-20, PPD-21 and PPD-41 should be revoked and replaced. The primary responsibility for consolidated cyber offense and defense should be assigned to the Department of Defense (DoD). Defense Agencies such as the National Security Agency (NSA) and the Defense Advanced Research Projects Agency (DARPA) should be tasked with assisting in the development of a comprehensive plan working in cooperation with the Undersecretary of Defense (Policy). The Joint Chiefs of Staff (JCS) can implement the plan with the operational activities such as U.S. CYBERCOM. DoD is the only department with the program management infrastructure to accomplish this, as well

as legal authority under U.S.C. Titles 10 and Title 50. Supporting roles for DHS, Commerce and others will be coordinated by the White House. A plan for the transition to this new organizational structure is a high priority for the first 100 days of the Trump administration.

1.4 Draft a New Executive Order for Cyber: Following the model used by President Reagan with E.O. 12333, replace the defective set of existing Presidential directives with a new Order that assigns roles and missions to federal departments and agencies capable of performing them to keep America safe from cyber threats.

1.5 Fund Critical Cybersecurity Programs: Adequate funding for essential research, development and operational programs that make America safe in the cyber realm is critical. Internet protocols, some of which date to the early days of the ARPAnet, need to be replaced with a modern system architecture far less prone to hostile exploitation. Automated systems utilizing supercomputers to detect and respond to new exploits and cyber attacks in real-time must to be developed on an urgent basis. This is likely to require an additional $4.5-billion over the next five years.

1.6 Secure Government Data: Hacking and theft of government data needs to cease as quickly as possible, whether at DoD, OPM, or any other agency. A "crash" program, possibly under the management of a joint program office (JPO) utilizing encryption and other needed technologies should be implemented. Data resident on legacy systems which cannot support necessary software should be hosted elsewhere.

2. The Future of Cyber Conflict and Cyberwarfare

The national security community views cyberwarfare as a new conflict domain, in terms of both technology as well as rules of engagement and operations. In many respects this is an area that is not yet well-settled. The Department of Defense, the military services and the Intelligence Community have taken some important steps recognizing this area but this is still a relatively new enterprise, and much needs to be accomplished to face the mounting challenge.

Unlike other technologies, which evolved principally in the demanding context of war, cyber technologies are in a state of constant and unpredictable evolution, making what appeared in science fiction new or soon to be new realities. This fact makes it extraordinarily difficult to manage the cyber landscape much less develop rules that are appropriate to, and beneficial for, it.

Further, cyber conflict differs from kinetic warfare, in that most hostile cyber operations begin as covert or clandestine activities where immediate attribution may not possible and the initial attack is not regarded as cyberwarfare. In the cyber area there are grey boundary lines between what is domestic and what is international, as well what is defense or offense. How America responds to such attacks raises major organizational and technical issues, pitting the legal authorities, mission, and capabilities of the Defense Department, the Intelligence Community, and DHS.

In terms of national policy there is need to consider what strategy, organization and policy best meet this evolving challenge. The Obama policy largely separating cyber defense from cyber offense, an approach that is not used in any other aspect of warfare, has been a mistake that perpetuates a critical error made in interpreting the Homeland Security Act of 2002. Since cyberattacks differ substantially from kinetic attacks some in the national security community failed appreciated this major threat. To keep America safe major changes in national policy and supporting legislation are needed.

- **Cyber Offense:** The nation needs the strongest offense possible, ranging from covert operations to cyberwarfare. This is an increasingly critical national security mission. It is also necessary to empower the private sector to work in concert with the military and intelligence services to meet new cyber threats.

- **Cyber Defense:** Cyber defense can no longer be separated from cyber offense. Actual integration of missions and operations is essential, and needs to be accomplished within the Department of Defense. Better standards are needed for critical infrastructure as is a greater level of support to make vital networks more secure and resilient. A device that decides whether you live or die should not be accessible from the Internet, or be connected with reliable security features.

Of major importance is the ongoing debate regarding what specific operations are included in the general category of "cyberwarfare" covered by U.S.C. Title 10 (military operations) and what operations covered by U.S.C. Title 50 (intelligence operations) are required as levels of authorization for any offensive action. Under the current legal regime these issues are critical and not widely understood, even among many of those directly involved. Experience shows that most cyberattacks begin as clandestine operations, with timely attribution often difficult or impossible, and they fall into the category of espionage.

Most recently such attacks have not only targeted financial services but also sensitive corporate and personal information as well a federal records of civilian and military personnel. Here the U.S. clearly needs the flexibility to respond rapidly in the most appropriate manner, and needs to retain the option of plausible deniability, afforded under Title 50 as well as the ability to engage in a larger scale cyber offense falling under Title 10.

Serious threats to critical national infrastructure remain. These concern the electric power grid, other SCADA systems, the financial and health sectors, as well as all aspects of communications and networked information technology. In many ways these cyber threats have far more serious consequences than any kinetic attacks on national infrastructure short of nuclear war. They cannot be left in the hands of DHS, which is ill-equipped to deal with them – both in terms of management; funding; technical expertise; and legal authority.

Likely adversaries include both nation states as well as non-state actors, and timely attribution may not be possible where cyber attacks are involved. In the area of offensive cyber operations the U.S. needs to explore the best models for meeting new cyber threats. Here national policy and organization are evolving, and the legal regime under the existing Titles 10 and 50 may need to be revisited in light of the new threats and technologies.

Recommendations:

2.1 Integrate of Cyber Defense and Offense at the Department of Defense: As part overall analytic, policy development and programmatic assessment recommended above an effective plan for the integration of critical cyber defense and offense mission under the Department of Defense should be undertaken. With White House Guidance the planning effort will be accomplished by the Under Secretary of Defense (AT&L) and Under Secretary of Defense (P), supported by the relevant Defense agencies. Critical here are the development of management skills and programmatic infrastructure needed to accomplish these key missions. This assessment should also evaluate whether existing Defense agencies such as DARPA and NSA can meet this challenge or a new Defense agency would be needed.

2.2 Identify Critical Technology Requirements: Many cybersecurity problems exist as a result of an antiquated Internet architecture still utilizing old protocols and legacy hardware in many places. The Directors of DARPA and NSA should be tasked with the development of a plan to upgrade the Internet and associated systems to a new architecture that is far less vulnerable to exploits, hacking and other cyber threats. Also of importance here is the development of autonomous systems for the real-time detection of new exploits and response to cyber attacks.

2.3 Return the US-CERT to the Defense Department: The U.S. Computer Emergency Response Team began as a highly effective Defense Department (DARPA) program. It is currently a DHS element and not capable of meeting the full set of evolving cyber challenges. It should be returned to DoD, and given the needed management as well as resources needed to meet these challenges. Further, CERT operations need to be coordinated with the work of NSA, the commercial sector, law enforcement and others with respect to new vulnerabilities.

2.4 Integrate the ICS-CERT into the Defense Department: The Industrial Control Systems Cyber Emergency Response Team can play an effective role in coordinating response efforts with industry, law enforcement and the Intelligence Community. It is currently unable to do so effectively as a DHS element and should be transferred to the Department of Defense as well.

2.5 Fund Critical Cybersecurity Programs: Increased funding for essential research, development and operational programs that make America safe in the cyber realm is critical. Initially this will require reprogramming of existing agency funds, and subsequently in budget requests for future fiscal years. This is likely to require an additional $4.5-billion over the next five years. It will also require explicit guidance from USD (AT&L) to ensure the research and development programs are consistent with new national guidance and coordinated among the relevant agencies.

2.6 Separate the Positions of Director, NSA and Commander, U.S. CYBERCOM: While the co-joined relationship between NSA and CYBERCOM his highly beneficial to America's cybersecurity, a single individual should not try to accomplish both important and demanding jobs at the same time. At the same time there is an issue that the DIRNSA reports through the Secretary of Defense to the Director of National Intelligence (DNI) and the Commander, CYBERCOM reports through the Joint Chiefs of Staff which could be a source of organizational conflict.

3. Building a New Partnership with Industry

Beginning in the 1960s the Defense Advanced Research Projects Agency (DARPA) created the ARPAnet, later the Internet, and what is now known as cyberspace. DARPA did so entirely through contracts with the technology industry and research institutions. This technology base which developed and greatly expanded over the last four decades is critical to solving the range of cybersecurity problems facing America now.

While America's technology industry has been responsible for the myriad of development in cyberspace the U.S. failed to include them as a full and effective partner in meeting the cybersecurity challenges as they evolved. If America is to meet these critical challenges this failed policy must change, and must change quickly. The most important changes are not difficult and can be accomplished in a reasonably short time. The most important elements of the new partnership with industry include:

- **Funded Research and Development:** America cannot depend on private industry funding important research and development in cybersecurity. The *Federal Cybersecurity Research and Development Plan* (2016) states only broad and vague goals with no path for achieving them. An actual plan with significantly increased federal funding for cybersecurity research is needed.

- **Support to University Research and Education:** It is essential that America promote education in computer science and related areas to meet the job requirements in the cyber area. An initiative similar to the National Defense Education Act (NDEA) could be useful in meeting this need. Public Law 107-305, *Cyber Security Research and Development Act (2002)* sought to accomplish this in part, but has been grossly inadequate.

- **Expanded Clearances for Industry:** Access to timely cyber threat data and related information is essential for the technology sector as well as the financial sector and others. Clearing a far larger number of personnel

at the Secret level is far less costly than higher levels and would greatly expedite the process. It can also be accomplished far more quickly than access to Top Secret and SCI data. Other key elements such as the financial sector, which may not have classified contracts, also require a pool of cleared personnel to they can access classified data networks at the Secret level.

- **Downgrading Vulnerability and Threat Data**: A large percentage of cyber-related and vulnerability data does not need to be maintained at Top Secret or compartmented levels. It can be downgraded to Secret and disseminated in a timely manner to the defense industry, the financial sector, law enforcement and others. It is also far less costly and burdensome to process and maintain this data at the Secret level as well.

- **Establish a Secure Network for Vulnerability and Threat Data:** The technology industry, as well as others such as the financial sector, law enforcement and others would greatly benefit from timely access to important data through a secure network at the Secret level, similar to SIPRNet which supports the Global Command and Control System, the Defense Message System, and numerous other classified warfighting and planning applications, nominally "CYBERNet." The new network must also include a contingency plan for any endpoint compromise.

- **Management Initiatives:** Essential for cybersecurity initiatives are qualified managers, and in many cases skilled technical personnel lack management skills and cannot automatically be promoted effectively. America must look to solving this management problem, with needed training programs as well as utilizing retired military officers who have these essential skills.

- **Promote an Industry Consortium:** Encourage technology firms to focus on cybersecurity problems as a cooperative and collaborative effort to the extent possible, and not a totally competitive environment. Public Law 113-274, *Cybersecurity Enhancement Act of 2014* encourages the public and private sectors to "work together" but provides no mechanism or funding to accomplish this.

Recommendations:

3.1 Expand the lndustrial Base: As part overall analytic, policy development and programmatic assessment recommended above the Under Secretary of Defense (AT&L) should develop a plan for significant expansion of the industrial base supporting America's cybersecurity efforts to include expanded Defense agency funding, security clearances, secure computer networks and other essential elements of an expanded effort. Firms in the financial sector and others need to be included as part of this base.

3.2 Downgrade Threat and Vulnerability Data to the Secret Level: Just as the U.S. downgraded almost all satellite imagery data under President Reagan to the Secret level, the Defense Department and the Intelligence Community should develop a plan to make available timely threat and vulnerability data at the Secret level, or potentially as Unclassified where possible and not harmful to national security interests. The Unclassified National Vulnerability Database (maintained by DHS and NIST as part of US-CERT) should be upgraded and expanded to the extent possible at this level.

3.3 Increase the Cleared Workforce: A far larger number of personnel working in the technology sector need to be cleared at the Secret level, even in advance of future funding and contracts. Their access to timely data is critical to solving America's cybersecurity problems. The cost of personnel security processing at this level is far less than that required for Top Secret and compartmented programs, and can be quickly accomplished in less than the 24 months now being experienced for higher clearance levels. Beyond the technology sector, it is essential to provide clearances to key personnel in the financial sector who do not generally have DoD or IC contracts, but are critical to solving the cybersecurity problem. At the same time a smaller set of managers and potential managers should be processed for Top Secret clearance (with SSBI) so that they can be indoctrinated for such programs when needed.

3.4 Establish a Secure Network for Vulnerability and Threat Data: The Defense Department, as the executive agent, should establish a secure network for the dissemination and sharing of timely cyber threat and vulnerability data at the Secret level – CYBERNet. This can be done along the model of SIPRNet which supports

the Global Command and Control System, the Defense Message System, and numerous other classified warfighting and planning activities. This network would also support the needs of the financial sector, law enforcement and others.

3.5 Expanded Federally Funded Research and Development: As part overall analytic, policy development and programmatic assessment recommended above the Under Secretary of Defense (AT&L), in cooperation with the Director of National Intelligence (DNI), should develop a plan for significant expansion and coordination of funded research and development in cybersecurity. Existing programs at DARPA and NSA need to be significantly expanded and focused on evolving threats in the cyber domain. Other agencies within DoD and elsewhere, such as the National Science Foundation (NSF) can be important parts of this process, but existing "stovepipes" need to be eliminated and a coordinated research agenda developed. This is likely to require an additional $4.5-billion over the next five years.

3.6 A New Initiative for University Research and Education in Cyber: Just as America responded to the 1960s challenge of "space race" it is essential that America promote education in computer science and related areas to meet the job requirements in the cyber area. The Trump Administration should explore with the Congress an initiative similar to the National Defense Education Act (NDEA) to provide funding for college and graduate student education in this critical area. Additionally, additional University Affiliated Research Centers (UARCs) should be established, focused on Cyber, to increase both research and government capabilities in the Cyber realm.

3.7 Management Initiatives: Explore options for meeting the critical need for qualified management for cybersecurity initiatives, including the use of active and retired military who have greatly needed skills and often security clearances. Possibilities may exist under the Interagency Personnel Act (IPA) as well as direct hires of retiring officers.

4. Privacy in the Era of Big Data

Central to the issues of cybersecurity as well as the needs of the Intelligence Community and law enforcement in an era where terrorism is major concern is the concept of privacy embodied in the Fourth Amendment to the Constitution and the subject of several court cases. Public awareness of privacy issues has been greatly heightened recently, due to publicity over various hacks into computer systems, and leaks with respect to government surveillance programs. A related controversy has arisen over whether firms such as Apple should be forced to help the government hack the iPhones used by the terrorists and other criminals.

Along with the development of the Internet has been the dramatic rise of social media as a major means of communications and information sharing worldwide. This new medium has become central to all aspects of modern life and has brought with it a host of privacy and security issues that are a central part of the cyberlandscape which must be addressed.

It is simply not possible implement truly effective cybersecurity programs needed to keep America safe and provide the level of personal privacy users are now demanding while acceding to every demand made by groups across the political spectrum. There has always been a dynamic tension between legitimate needs for data and individual rights, and it is increasingly becoming an issue in the cyber domain.

Recent publicity over foreign hacks of e-mail related to the 2016 Presidential election has further heightened public awareness of both the security and privacy issues. These hacks violated the privacy of various individuals and demonstrated the lack of essential security measures at the service providers and showed what some believe to be an attempt by a foreign state to interfere with the U.S. electoral process.

A wide range of groups including, civil liberties organizations, the financial community and others, have brought increasing attention to the vulnerability of personal data transmitted by all of the devices currently in use as well as data maintained by the commercial suppliers of network services. The world has entered an era where the vast

majority of personal data is being maintained on vulnerable servers as well as large-scale data commons over which the users have no control. Major concerns here include:

- **Legitimate access to data:** Intelligence and law enforcement authorities need timely access to data, including metadata, for cybersecurity missions to make America safe.

- **Insertion of false data:** Closely related to manipulation of data, many technical experts believe that the insertion of false data to be potentially the most serious threat to cybersecurity.

National policy needs to revisit the statutes in each of these areas as well as operational programs designed to protect the privacy of users in each category.

Recommendations:

4.1 Explore Options for Metadata Collection: The National Security Council (NSC) should task the Department of Justice and the Director of National Intelligence (DNI) to provide a set of statutory and executive policy options for future metadata collection in light of the evolving legal regime which continues to expand the concept of Fourth Amendment privacy protection.

4.2 Study of Exploits and Other Malware: The NSC should task the Under Secretary of Defense (AT&L) and the DNI to provide a comprehensive study of the future of computer exploits, other malware, and required research and development activities. The study effort should include government personnel as well as supporting contractor, research centers (FFRDCs), as well as technology sector companies.

4.3 Study of Legitimate Access Alternatives: The NSC should task the Under Secretary of Defense (AT&L) and the Director of National Intelligence to provide a comprehensive study of the what technical options exist to enable legitimate access to connected devices such as computers and cell phones for intelligence and law enforcement, as well as alternatives where such future access is not possible.

4.4 Dealing with Data Breach: As theft and misuse of data have become an increasing cybersecurity issue, the White House and should explore a potential "data breach

law" and other regulations to protect important user data which ties into the economy, such as banks collecting user deposit information in a way which is encrypted and presumably safe. This could be done as an amendment to the Computer Fraud and Abuse Act (CFAA) currently in existence.

4.5 Study of Governmental and Commercial Data Mining: Concerns over the collection and use of data derived from the Internet, including e-mail as well as commercial transactions and social media has been of great concern. Within the U.S. these concerns have largely been over government surveillance programs, while in Europe governments are constitutionally tasked to enhance privacy with no regard to national security, which is an unbalanced approach. It is important to track these concerns and progress in this area. The White House Director, ONCP should direct the Department of Justice, along with the DNI to provide an analysis of this area and implications for future policy and law.

4.6 Disruption of Malware Markets: It is unfortunately the case that markets on the "dark web" exist for the sale of malware. The relevant elements of the Intelligence Community and DoD should explore opportunities to detect and disrupt these markets where nefarious actors purchase such code.

5. Going Dark – Implications of an Encrypted World

In the age of "big data," the U.S. Intelligence and law enforcement communities, as well as the media and others, are engaged in an ongoing debate about the use of encryption and what "going dark" really means in technical and legal terms; what impact this will have on their operations; as well as what can be done to mitigate the problem. The expanding use of encryption technology stands to impede lawful operations by both intelligence and law enforcement agencies that meet even the most stringent interpretations of the Fourth Amendment right to privacy.

While an earlier legal regime that permitted controls over encryption technology is no longer viable various solutions have been proposed that would force companies to enable access to user data to the government pursuant to a legal process. Thus far no such solutions have been enacted in the U.S., although proponents continue to press for them under the belief that the Congress can legislate effective solutions in a world market over which they have no control. In the future commercial firms may simply not be able to comply with court orders given the state of the evolving technology.

In an earlier "analog world," users were largely in control of their own personal data which often existed as paper files which they could control. With the transition to the digital world, almost all personal data now reside on servers and systems over which users have no control and are subject to hacking, theft and other forms of misuse. As awareness has grown, so has the demand for security and solution which involve encryption. The technology path that has become increasingly responsive to this user demand. Looking five or ten years into the future it becomes important to recognize how the likely technical solutions that will be implemented and unintended consequences which will impact on legitimate government requirements.

As a result of this increased awareness, demands for greater privacy and security are having a significant impact with suppliers of both devices and software moving to meet this demand with new products employing various encryption schemes and other security features. They do so at a time when the available technology supports increasingly effective encryption and when the legal regime cannot control its application. In most

cases, the new types of protection can be provided to users at zero marginal cost and free from any effective restrictions other than export control.

Recommendations:

5.1 Expanded Research on Differential Privacy: As part overall analytic, policy development and programmatic assessment recommended above the Under Secretary of Defense (AT&L) should develop a plan for significant expansion of funded research and development that supports individual user privacy. DARPA's recently launched BRANDEIS Program is one example of how this might be achieved.

5.2 Study of End Point Technologies: Even though encryption will become increasingly pervasive, there are "end point" in the process were a device has not yet been encrypted or has been decrypted. The Director of National Intelligence (DNI), in conjunction with NSA and DARPA should undertake an assessment of the technologies that could be developed to access likely end points over the coming decade.

5.3 Unlocking Connected Devices: Increasingly devices such as laptops and cell phones will be either encrypted or "locked" with user passwords. Issues for the legal regime remain as to whether users can be forced to provide passwords or whether commercial firms can be forced to develop tools to "unlock" devices by court order, if technically possible. A comprehensive study of the legal and technical issues should be undertaken, including the Department of Justice, the FBI, DARPA, NSA and potentially others.

6. Supporting Law Enforcement

Cybersecurity in America is not exclusively a matter for the federal government. State and local law enforcement agencies face a growing set of challenges in this area as well. A rapid rise in cybercrime has been accompanied by increasing use of network resources by criminals, terrorists, and other subjects of concern. Criminal investigations now involve an ever larger number of connected devices, such as computers and cell phones, which have been "locked" to inhibit easy access – even with appropriate court-issued warrants.

Virtually all state and local law enforcement agencies lack the technical resources of the federal government to deal with this growing challenge. While the FBI, ATF and other federal agencies currently provide some level of assistance to these non-federal agencies, much more needs to be done to meet this challenge.

Federal support to state and local law enforcement is not a new challenge or unique to the cyber area. There are several examples where this has been successful in the past. The El Paso Intelligence Center (EPIC) was initially established in 1974 as a joint activity to meet America's needs in the area of border protection and drug trafficking and expanded during the 1980s. Following the 9/11 terrorist attacks on the U.S. in 2001, a number of joint terrorism task forces (JTTFs) and joint regional intelligence centers (JRICs) were established under federal auspices to integrate both federal and local resources to combat ongoing terrorist threats.

Local and state governments are often unaware of what data is available through lawful process. Additionally, many companies are frustrated by requests from a multitude of state, local, and federal agencies. The JTTFs should be tasked to facilitate state and local lawful requests to data and serve as a Single Point of Contact (SPoC), similar to the UK system. SPoCs should all be trained, certified, and accredited and assigned to specific companies within the JTTF area of responsibility so as to ease the burden of the companies receive the lawful requests.

The federal government has also undertaken important research in the cyber area of considerable use to state and local law enforcement. Included here are the detection of "insider threats;" software to deal with human trafficking operations; detection of money laundering and other cybercrimes; as well as the ability to access parts of the "dark web." A key element of the new Trump policy will be to increase vital research in these areas.

Experience gained in these activities is useful in exploring the best way to support law enforcement in dealing with the evolving set of cyber challenges. To what extent the existing centers can provide the needed infrastructure should be a subject of study for the Trump administration. Specific needs of state and local law enforcement in the cyber area include:

- **Data Sharing and Access to Data:** State and local law enforcement authorities need timely access to threat data and should be included in the cyber data network (CYBERNet) recommended above. They also have data on cybercrimes and other local threats that can be added to the network. This will also require an increased number of Secret level clearances for law enforcement and secure facilities for them to operate, all of which can be accomplished at a relatively limited cost.

- **Technical Forensic Support:** Law enforcement agencies across America are facing a rapidly increasing number of devices used in crimes, such as laptops and cell phones, which have been locked, password protected, or contain encrypted data. To the extent such problems can be solved, they require sophisticated resources which are generally not available at the local level. A central technical forensic support center maintained by the federal government to support law enforcement is needed.

Another area of note is Rule 41 of the Federal Rules of Criminal Procedure, which expanded law enforcement's ability to engage in hacking and surveillance, a proposal that comes from the advisory committee on criminal rules for the Judicial Conference of the United States. This amendment to Rule 41 created new avenues for government surveillance and granted judges the ability to issue a warrant to remotely access, search, seize, or copy data "concealed through technological means" or are on protected computers.

Recommendations:

6.1 Collaboration using the JTTF or JRIC Models: Following the 9/11 terrorist attacks a number of "joint" centers including federal, state and local law enforcement and intelligence personnel were established for the sharing of data and coordination of counter-terrorist operations. This concept has general been seen as successful and can be applied to cybersecurity issues. The Departments of Justice, Homeland Security and Defense should explore the use of existing centers (JTTF and JRIC) for cybersecurity issues as well as the creation of new centers, if needed.

6.2 Establish SPoCs at the JTTFs: The JTTFs will facilitate and serve lawful requests to companies within the JTTF area of responsibility to both empower local and state law enforcement and ease the burden on companies.

6.3 National Forensics Laboratory: The "unlocking" of computers and cell phones is becoming a larger problem and beyond the capability of almost all local law enforcement agencies. The federal government should establish and maintain a central laboratory for cyber purposes as a "service bureau" for state and local law enforcement needs.

6.4 Cyber Data Network: State and local law enforcement authorities need timely access to cyber threat data and must be made an integral part of the recommended Secret-level network – CYBERNet. This will also require clearing a significant number of police officers at the Secret level who will access the network and on-line capabilities. Hardware and software needed to access CYBERNet should also be provided in keeping with federal security guidelines.

6.5 Guidelines for Rule 41 Application: Clear guidelines for the application of Rule 41 of the Federal Rules of Criminal Procedure (as amended) should be developed so that there are adequate methods for seeking warrants against anonymized criminal activity while keeping constitutional protections against unreasonable search and seizure preserved.

7. Internet Governance

Within the past few years, lawyers and diplomats have largely invented a field now known as "Internet Governance." which includes several issues, both real and imagined. With the transition from the Defense Department's ARPAnet to the public Internet after 1989, worldwide proliferation of connected networks took place at a lightening pace with little or no intervention on the part of any federal agency or international organization. It was simply a more efficient communications technology that worked.

The Internet is an American invention increasingly seen as a global resource. In the view of many nations, the Internet has become so important as to require state control or at least greater state control than now exists. Exactly why is not entirely clear. Some advocates see a need for Internet regime construction and seek to define regime rules and procedures as well as underlying principles and norms for which there is no obvious need. In reality nations control Internet-related policies within their own borders, such as laws prohibiting online gambling, protecting intellectual property, or blocking/filtering access to certain content.

Some authoritarian governments censor political and social content much as they do in traditional media. They see the Internet as expanding the possibility of popular communications, thus posing a threat to centralized control and dictatorship. China, Cuba, and Iran, for example, have been the most repressive countries in terms of Internet freedom. It is within their right to do so, even though the United States can advocate greater openness and freedom.

As contentious public policy issues have emerged, particularly in regard to the balance between security, including law enforcement and national security, and privacy, the concept of Internet governance has conflated management of the technical resources necessary for network stability and expansion with discussion of behaviors emerging from the *use* of the Internet in what is known as the content layer.

As the Internet grew globally the concept broadened considerably. At the 2005 UN-sponsored World Summit on the Information Society (WSIS), Internet governance was defined as "the development and application by governments, the private sector and civil

society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet."

America is an international actor and has little choice but to address these issues on an ongoing basis. While the 2005 WSIS established the Internet Governance Forum (IGF) to open an ongoing, non-binding conversation about the future of Internet governance, it accomplished nothing of operational significance. Actual Internet governance is conducted by an international set of groups including governments, the private sector, and research communities that create shared policies and standards that maintain the Internet's global interoperability. To maintain interoperability, key technical and policy aspects of the core infrastructure are administered by the Internet Corporation for Assigned Names and Numbers (ICANN), which oversees the assignment domain names, Internet protocol addresses, and other key parameters.

Originally funded under a DARPA research contract, ICANN has been the subject of criticism, controversy and litigation. The notion that whoever controls the ICANN contract somehow "controls" the Internet is a myth. The assignment of domain names and IP addresses is largely a bookkeeping exercise. Actual control of the Internet would consist of the ability to prevent use or abuse of this worldwide network and the withholding of any particular name or block of IPs could not accomplish this purpose. In technical terms it is simply a laughable proposition and should be seen as such.

The Obama administration's decision to terminate the federal contract with ICANN last year was portrayed as an effort to reduce, not increase, state control over the Internet. In reality it did neither. The claim that this would help make the Internet more resilient in coming decades is also nonsensical. Some on the left even claim that the most important features of the Internet users care about – openness, diversity, and fundamental resilience—are likely be better protected with less American control than with more.

Many experts emphasize that Internet governance is not the product of an institutional hierarchy, but rather comes from the decentralized, bottom-up coordination of tens of thousands of mostly private-sector entities across the globe, often referred to as "stakeholders" including network and server operators, domain name registrars, standards organizations, and Internet service providers. Governments and civilian organizations participate with the stakeholders in the development of technical policies.

America needs to provide guidance to those engaged in the process so that it preserves the values and opportunities the U.S. sees as essential to ongoing Internet operations, recognizing that no one government, company or organization owns, runs or

controls the Internet, which has no official governing body. Each connected network establishes its own policies in keeping with a set of agreed upon protocols. These protocols and agreements have emerged over time and have come from this industry. They were never imposed by government fiat or regulation.

The Trump administration should adopt a policy that adheres to the old adage "if it ain't broke don't fix it." Now that ICANN has become an autonomous not-for-profit organization, answering to stakeholders across the Internet community, including a governmental advisory committee, a technical committee, industry committee, Internet users, and telecommunications experts, the extent to which this contractual change will make any operational difference remains to be seen. In all likelihood it will not. ICANN will continue to exist as largely a bookkeeping enterprise for domain names and IP addresses with no ability to exert actual control over ongoing Internet operations.

There is also need for security certificate authorities to be independent organizations, and not governments, since governments could effectively falsify websites to censor or collect information on the populace. This is most likely the case now in Iran and China, and quite possibly other nations as well.

Recommendations:

7.1 Monitor ICANN Operations: It would be difficult to reverse the Obama administration's decision to end the ICANN federal contract as the transfer has already taken place, and probably not worth the bother. At present the best approach would be simply to monitor ongoing operations to see if any unanticipated problems arise.

7.2 Ensure that U.S. International Obligations Respect U.S. Interests. To accomplish this goal requires close interdepartmental coordination in a process led by the senior White House official for cyber policy. Actions of the State Department, Office of the U.S. Coordinator for International Communications and Information Policy need to be made consistent with the goals and objectives of overall U.S. policy for cybersecurity. The U.S. Coordinator should be actively engaged with the senior White House official for cyber to avoid international representations and agreements adverse to America's interests.

7.3 Require Independent Security Certificate Authorities: To prevent governments from engaging in actions such as the falsification of websites to censor or collect information security certificates should be issues by independent, non-governmental authorities.

8. Repudiate Bad Deals

A paradigm shift in defense technology is under way. America's post-WWII supremacy in both civil and military technologies is increasingly challenged by the pacing of competitor states, such as China and Russia, and last-century strategic thinking about how to sustain the U.S. advantage is no longer effective. In the past, overmatch depended on the development of proprietary technologies within America's own defense industrial base, and defending exclusivity of those capabilities through aggressive export control regimes.

The U.S. is not only suffering from bad deals made by prior administrations in the area of international trade, but also from international deals such as the Wassenaar Arrangement which is not only adverse to American industry but also puts the nation in a far weaker position to deal with the actual issues of cybersecurity to make America safe.

In 2013 a meeting of the 41 nations involved in the Wassenaar Arrangement which sought to control the export of encryption technology, as an arrangement on export controls for conventional arms and dual-Use Technologies. This raised serious concerns both in the U.S. as well as Europe and elsewhere over the utility of the proposed rules and a range of possible consequences for software development critical to national and related cybersecurity requirements. At the time the Department of Commerce indicated that monitoring and enforcement of these proposed rules would require significant resources and served no useful purpose. This did not, however, deter the Obama administration.

At a joint Congressional hearing in 2015 both government and industry representatives aired their specific concerns about this agreement. The list of controlled technologies had been amended in 2013 to include surveillance systems for the first time, in response to reports linking exports of Western surveillance technologies to human rights abuses in countries such as Bahrain and the UAE, Turkmenistan, and Libya. These reports were largely debunked, and the proposed controls would not solve the problem if it did exist.

The stated objective of the proposed rules was to control the distribution of surveillance and network exploitation tools narrowly enough that it would leave vital

security research tools and related software unregulated while stemming the proliferation of the targeted software. To what extent this is even possible or more likely counter-productive is a central concern of what is clearly a "bad deal."

There is fundamental consensus on the objective of limiting the use of surveillance technologies where employed for human rights abuses. The real question, however, is whether or not any export control regime can seriously limit the use of such technologies for this purpose. The 41 nations subscribing to the Wassenaar Arrangement represent approximately 20 percent of the nations in the world. It is also the case that many of the surveillance technologies and software tools that would be subject to the proposed export controls are widely available on the Internet and can be further developed and implemented on a host of nations not subscribing to Wassenaar.

The intent for the incorporation of the language in the 2013 plenary was to provide legal tools to combat the sales of enabling software to repressive government regimes. If implemented, however, can this objective be achieved? Virtually all experts agree that it would not. Foreign governments and nefarious group seeking to obtain such software can obtain it irrespective of any export controls implemented by the Wassenaar signatory states. At the same time the proposed export controls and licensing regime proposed would likely have a series of unintended consequences, the most serious being a highly adverse impact on the development of essential cybersecurity software.

Recommendations:

8.1 Repudiate the Wassenaar Arrangement: Experts from industry, the Departments of Commerce, Homeland Security and Defense universally agree that it would not accomplish its stated objective and would be harmful to American industry and cybersecurity efforts. A bipartisan Congressional committee also agrees. Those aspects of the Agreement dealing with security software, "intrusion software," and software development tools are a quintessential bad deal and should be repudiated.

8.2 Provide Technical Support for New Deals: The disastrous agreement reached at Wassenaar in 2013 resulted from a State Department official engaging in negotiations with no serious technical support from either the Defense Department, any other federal agency with cybersecurity expertise, or the technology sector. Any future negotiation must be fully supported by technical experts. A useful model is the technical support provided to U.S. negotiations in arms control, such as SALT.

8.3 Avoid Deals that Treat Software as Hardware: Software and hardware are fundamentally different that cannot be subjected to an export and control regime designed for shipment of specific physical objects. Further, software and software development tools cannot be made the subject of an export control regime which seeks to control their development for purported "humanitarian" purposes. Even if such a purpose is valid, actual controls are impossible to enforce and at the same time can deal a fatal blow to cybersecurity efforts which need these development tools.

9. Protecting America's Intellectual Property

America has not only suffered from a loss of manufacturing industry and jobs, it can no longer allow other nations to steal the intellectual property (IP) of U.S. companies. The U.S. will partner with and empower American companies to increase security against all cyber threats. New technologies will be required to detect the theft of American intellectual property and defensive measures are needed protect it against theft and exploitation of stolen IP. A new legal regime will also be needed to punish or sanction those stealing American intellectual property that lie beyond the jurisdiction of U.S. courts.

Over the last several years the nature of intellectual property itself has radically changed. One result of the technology revolution has been the conversion of almost all media to digital form. Analog media such as paper files, newspapers, books, audio recordings, video, and all manner of entertainment in physical form have largely disappeared. Physical media are increasingly replaced by digital files which exist on net-connected servers and devices making them appealing targets for computer theft.

Making matters worse, computer theft of intellectual property can be accomplished by individuals and organizations outside U.S. jurisdiction, and often with the tacit or even explicit support of a foreign host government. For decades now China has protected the theft of U.S. intellectual property, including software and entertainment media. Those engaging in this theft, often with family or political ties to the Chinese leadership, have been protected and U.S. efforts to stem this tide have been ineffective. The cost to U.S. firms and individuals is well into the billions of dollars each year. It needs to stop. Protecting America's intellectual property effectively includes:

- **Technical Protection of Data and Systems:** Digital files of U.S. firms and individuals need to be protected from foreign hacking and theft with encryption and other security technologies. New technology must ensure that once legally sold, it is not cracked and otherwise stolen and resold.

- **Holding Thieves and Supporting Nations Responsible:** Aside from international conventions which have proved to be increasingly useless,

> America must hold those who steal the nation's intellectual property responsible through sanctions and other direct economic actions. Allowing China to ignore the issue is no longer acceptable.

Several international treaties and conventions provide protection for intellectual property once created. The Berne Convention for the Protection of Literary and Artistic Works, for example, is the most important international treaty. The U.S. acceded to that treaty in 1989 as did of China in 1992 and Russia in 1995. Now almost all of the world's most important countries now belong to the Berne Union. Unfortunately China and others simply elect to ignore it when it suits the economic interests of well-connected citizens.

For over a century the U.S. resisted joining the Berne Union, partially due to a desire to maintain the formalities U.S. law required. Congress needed to amend the Copyright Act to dispose of the many formalities that Act required. Likewise, foreign government cannot impose similar formality requirements on U.S. copyright owners as a condition to filing suit in their national courts, even though they can impose those requirements on their own nationals.

Other key characteristics of the Berne Convention are the concepts of "minimum standards" and "national treatment." "Minimum standards" are the baseline that all nations must provide to non-domestic claimants. The "national treatment" principle states that owners of intellectual property should enjoy the same protection for their works in other countries as those countries accord without a requirement formalities such as a copyright notice or a registration requirement. Foreign nationals must be afforded the same rights and treatment that a domestic copyright holder would receive.

Recommendations:

9.1 Review and Enhancement of Cyber Investigation and Response Capabilities: America should review and enhance of cyber investigation and response capabilities within the existing ICE-HSI led IPR Center.

9.2 Create a New Regime for the Protection of Intellectual Property: The Department of Justice and the Department of State should explore possible changes to the Berne Convention that would provide any intellectual property protection in the digital world. A critical question remains as to whether the traditional concept of copyright still has a place in the modern world or not. Possibly this is now a

problem that cannot be solved through traditional means of national and international law.

9.3 Explore a Sanction-Based Approach: As an alternative to international treaty and convention the Department of Justice and the Department of State should explore possible use of economic sanctions against nations that overtly or tacitly support the theft of intellectual property.

9.4 Explore a Technology-Based Approach: Apart from any legal approach to stopping the theft of intellectual property, the technology industry should be asked to develop a set of potential alternatives for both protecting IP in digital form from theft, and also from unauthorized distribution of IP by digital means.

10. Updating the Law for Cybersecurity

Fixing America's cybersecurity not only involves some daunting management and technical challenges, but also faces a legal regime designed for an earlier era. Years ago geography was relevant; warfare was entirely kinetic; distinctions between espionage and military operations were clear; and America's adversaries were actual nation states. In the Internet age all of this has changed. Cyber operations against America transcend geographic boundaries and are perpetrated by nations as well as non-state actors. The distinctions between criminal acts, espionage and cyber warfare are often unclear.

At the same time the threats to American national security have also changed. The terrorist attacks of 9/11 were the first time the Continental United States had been attacked since 1814, and this came from a non-state actor. Since 9/11 a major concern has been with future terrorist attacks on the U.S., and far less with an invading foreign army or nuclear strike. Clearly the national security structure set out in the 1947 National Security Act has been inadequate for the new threats facing the nation – both from terrorists and cyber attacks.

The 1947 Act left the U.S. without a domestic intelligence service and restricted both the newly created CIA and the FBI from performing this function. The 2002 Homeland Security Act attempted to address some of the shortfalls identified after 9/11 but created an artificial distinction between "national security" and "homeland security" which continues to raise problems in responding to the set of threats still facing America. This is a particularly difficult problem in addressing the operational issues in cybersecurity.

The body of law covering cybersecurity and related concerns includes:

- **The Constitution:** The Constitution itself actually says very little about national security and nothing about intelligence. In the modern era it must be interpreted and applied to the problems at hand. In 1787 electricity hadn't yet been invented, let alone the Internet.

- **Federal Statutes:** A number of laws apply to cybersecurity issues such as the 1878 Posse Comitatus Act; 1947 National Security Act; 1978 Foreign

Intelligence and Surveillance Act (FISA); 2002 Homeland Security Act; 2004 Intelligence Reorganization and Terrorism Prevention Act (IRTPA); 2008 FISA Amendments Act; and several others.

- **Presidential Directives and Agency Regulation:** These include both Executive Orders, such as E.O. 12333 as well as Presidential Directives, such as PPD-20, PPD-21 and PPD-41. The latter three signed by President Obama are largely misguided and ineffective in solving the cybersecurity problem.

- **Case Law:** Recently individuals as well as civil liberties organizations have challenged various statutes as unconstitutional and violations of privacy guarantees under the Fourth and Fifth Amendments to the Constitution. By and large they are winning and by most estimates will continue to do so.

Even though near term actions can be taken under existing law, making America truly safe will ultimately require new law consistent with the Constitution. This is not a new or unique situation and here the Trump administration can work effectively with the Congress to modernize the legal regime to meet these new challenges. Fortunately the area of cybersecurity has not been one of partisan divide – indeed, bipartisanship among the key Congressional committees in this critical area has been the case for several years.

Recommendations:

10.1 Repeal 1878 Posse Comitatus Act: Largely unknown other than to legal experts, this law is an artifact of post-Civil War reconstruction and no longer serves any useful purpose. On the contrary, it inhibits the use of military resources in the event of natural disaster as well as cybersecurity operations where Defense agencies and military resources can play an important role.

10.2 Amend the National Security Act of 1947: This landmark law provides the overall structure for national security in America, creating the National Security Council, Department of Defense, the Central Intelligence Agency, and the U.S. Air Force among other things. At the same time, it failed to provide for a domestic intelligence capability and enforces the artifacts of geography that have become irrelevant in the cyberworld. Important as it has been, it needs updating. The nation should seriously

address the need for an effective domestic intelligence service, as is the case with all other developed nations.

10.3 Amend the 2004 Intelligence Reorganization and Terrorism Prevention Act (IRTPA): While this law created the position of Director of National Intelligence (DNI), it failed to include that position in the Cabinet. This should be changed. Intelligence has become an increasingly important function to the security of the nation, with an annual budget in excess of $80-billion. The DNI position should be elevated to Exec. Level 1 and the DNI made a Cabinet officer.

Study Team

David Aitel	*Immunity, Inc.*
Lillian Ablon	*The RAND Corporation*
Sophia d'Antoine	*Trail of Bits, Inc.*
Edward Doyle	*Center for Advanced Studies on Terrorism*
Thomas Garwin	*Center for Advanced Studies on Terrorism*
Daniel Guido	*Trail of Bits, Inc.*
Richard Harrison	*American Foreign Policy Council*
Susan Hennessey	*Brookings Institution*
Gregory Larsen	*Institute for Defense Analyses*
Eric Ormes	*J.P. Morgan Chase*
Harvey Rishikof	*Crowell-Moring*
Nicholas Rostow	*Yale Law School*
Ryan Stortz	*Trail of Bits, Inc.*
Mara Tam	*QxNch*
Abraham Wagner	*Columbia Law School*
Rand Waltzman	*Carnegie Mellon University*
Walter Weiss	*Senate Select Committee on Intelligence Staff (Prior)*
Kevin Yorke	*New York County District Attorney's Office*
Pieter 'Mudge' Zatko	*Cyber-ITL*

Research Assistants

Jacob Arber	*Columbia Law School*
Christine Chen	*Columbia Law School*
Theodore Rostow	*Yale Law School*
Kathryn Witchger	*Columbia Law School*

Affiliations listed are for identification purposes only. No institution has funded this effort in support of the Trump-Pence Transition.

Fixing America's Cybersecurity:

A Plan for

Cyber Policy and Organization

APPENDIX

Leveraging Technology to Achieve America's Goals

Prepared for the

Trump-Pence Transition Team

Rev. 4.0 (1-13-2017)

Fixing America's Cybersecurity

APPENDIX

Leveraging Technology to Achieve America's Goals

Background

There are two essential matters that ensure the U.S. Government functions effectively: people with technical proficiencies to get the job done and a government that fully leverages modern technology. This Appendix to the main report *Fixing America's Cybersecurity* reviews key agencies and offices within the Executive Branch of the Government and suggests actions which meet the specific goals and objectives outlined in the report.

Executive Office of the President

National Economic Council (NEC)

Many administrations choose to combine the Domestic Policy Council and the NEC to maintain U.S. global technological leadership. The Trump Administration needs to ensure White House officials responsible for domestic or international economic affairs – whether related to trade, capital markets, or macroeconomic affairs – have a solid grounding in technology policy issues. These issues are not only vital in securing U.S. technological leadership, but also in creating small business opportunities, helping U.S. companies access key foreign markets for tech goods and services, and safeguarding America's place as an attractive destination for foreign investment.

National Security Council (NSC)

It is critical that the NSC's core mission, to coordinate U.S. national security activities, is informed from the ground level about how information and communications technology (ICT) serves U.S. security objectives. This means NSC senior officials should have a comprehensive understanding of the digital arena and be conversant in technological policy issues. Officials should safeguard U.S. leadership in technology, an open internet, free cross-border data flows, a global approach to cybersecurity, and partnership with the private sector, voluntary industry-led standards, and a robust advanced manufacturing industrial base among other issues.

We encourage consideration of people with past private sector experience in the technology space for positions that focus on cybersecurity or international economics. These positions include:

- Senior Director and Cyber Coordinator,
- Special Assistant to the President and Cybersecurity Coordinator,
- Special Assistant to the President for Economic and Technology Policy (either through NEC or NSC), and
- Deputy National Security Advisor for International Economics.

Office of Management & Budget (OMB)

As the implementation and enforcement arm of Presidential policy government-wide, OMB is in a unique position to leverage technology to encourage cross-agency collaboration and to integrate the latest private sector innovations into government practice. For example implementing advanced data analytics, data center consolidation, and cloud technologies could save billions of dollars and improve cybersecurity in key government systems. OMB leadership must, however, have sufficient facility with technology to accelerate presidential priorities across government.

Office of Science and Technology Policy (OSTP)

The OSTP has successfully coordinated with the NSC on interagency technological policy issues and brought in technologists to contribute to policy discussions. We strongly advise continued coordination between these agencies to avoid dysfunctional overlaps. OSTP has also been, and should remain, a critical coordination point for public-private partnerships on research and technology. Accordingly, it is vital that this office is headed by someone with a deep understanding of the U.S. innovation ecosystem, including the roles and resources of industry, academia, and government. This person should:

- Have a proven track record of success in entrepreneurship and/or innovation (e.g., started a new company, initiative, or product);
- Be well-respected and influential in science and technology circles;
- Understand how technology affects today's society; and
- Know the public policy and government levers that can harness technology for the public interest.

U.S. Trade Representative (USTR)

U.S. innovation, economic growth, advanced manufacturing, and job creation are dependent on American companies' ability to easily access new markets abroad. Trade policy must be inclusive and create opportunities not only for large companies, but also for small businesses and workers in all industries. Technology is central to achieving that objective because it underpins the operations of companies in every sector, creates opportunities for entrepreneurs to reach global markets, and enables workers to improve skills. We strongly encourage the Trump Administration to ensure that USTR is infused with technological expertise and organized in a way to advance that agenda. This is particularly important given that foreign government actions are both restricting U.S. digital exports, and disrupting trade flows with non-market based industrial policy. These trade barriers and disruptions can have a significant negative impact on American jobs.

The Internet and U.S. tech leadership are threatened abroad like never before, and we need people at USTR who can fight to preserve U.S. interests. Appointees should advocate for balanced policies that provide effective, high-quality patent protections, and strengthen advanced manufacturing in the U.S. This means the government must:

- Appoint at least one Deputy U.S. Trade Representative with significant private sector background in these issues;
- Establish a new Assistant U.S. Trade Representative for Digital Trade;
- Grow the recently created Digital Trade Working Group;
- Equip negotiators with internet (not only telecommunications) expertise;
- Ensure the Office of General Counsel evaluates trade enforcement actions involving tech sector issues; and
- Secure strong intellectual property rights protections for US companies and entrepreneurs.

Federal Trade Commission (FTC)

In order to be effective the FTC must balance protecting consumer interests with encouraging innovation and competition in our dynamic economy. This requires a special emphasis on creating comprehensive cost-benefit analyses, establishing clear evidence before making decisions regarding competition and consumer harm, and practicing "regulatory humility." The FTC also collaborates with federal and state partners across the country and competition regulatory agencies around the world to advance crucial American consumer protection and competition priorities. These partners look to the FTC for leadership. The FTC's mission to protect consumers and promote competition continues

to play a crucial role in the American economy. Appointees should be prepared to lead global debates and protect innovation.

In order to advance consumer interests in a rapidly changing economy, the FTC needs personnel focused on understanding the complex issues behind the dynamism of 21st Century markets. The FTC will benefit from leadership who can:

- Maintain and increase technological competency among staff who are faced with complex products in dynamic markets; and
- Recruit personnel to the Office of Policy and Planning who possess an understanding of technology markets to continue the FTC's important policy advocacy and research efforts.

The FTC should pursue a flexible enforcement approach focused on encouraging industry's adoption of commercially reasonable practices through education and strategic guidance, with a particular eye toward aiding small- and medium-sized businesses.

Federal Communications Commission (FCC)

The FCC must successfully collaborate with the private sector to fulfill its duties regulating interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. We urge that nominees for FCC Commissioner seats.

- Understand he vital role of competition in the communications sector;
- Appreciate the limits of FCC authority across its areas of responsibility;
- Establish a data-driven evidence base before setting *ex ante* policies;
- Know the communications industry landscape and the role the FTC plays in realizing inter-connected smart communications technologies; and
- Support future technological developments that rely on a robust communications infrastructure.

Federal Departments

Department of Commerce (DOC)

National Telecommunications and Information Administration (NTIA): In pursuing its mission to encourage investment and job creation in the United States, it is essential that the Department of Commerce does not separate economic issues from digital issues. This is particularly important given that this agency deals with trade promotion and market access, privacy and data protection, cyber-security, the promotion of advanced manufacturing, and intellectual property protection. As the National Telecommunications

and Information Administration (NTIA) is one of the president's key advisors on telecommunications and information policy, NTIA appointees should be prepared to lead global debates on internet governance.

National Institute of Standards and Technology (NIST): Likewise, the National Institute of Standards and Technology (NIST) plays a key role in cybersecurity, the development of industry standards, and basic research. NIST Cybersecurity Framework and federal agency information security standards came from collaboration with the private sector; continued collaboration is essential to ensuring that U.S. standards and policies advance U.S. economic objectives. NIST has also been particularly helpful in establishing a National Network for Manufacturing Innovation (NNMI) that supports critical industry-wide research and next-generation manufacturing technology.

International Trade Administration (ITA): The International Trade Administration (ITA) plays a key role in data protection regulation issues, including the U.S.-EU Safe Harbor Framework and its successor the EU-U.S. Privacy Shield Framework. ITA appointees must be

- Able to view the digital dimensions of their standard international trade and market access responsibilities,
- Conversant in issues related to data protection, localization laws, advanced manufacturing, and the Internet of Things (IoT).

Bureau of Industry and Security (BIS): The Bureau of Industry and Security (BIS) advances U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system, while reforming controls to keep pace with advancing technology, and promoting continued U.S. strategic technology leadership. Specifically, we recommend continuing the Export Control Reform (ECR) Initiative to include additional reform such as simplification of the encryption regulations. We also recommend further reform of the Wassenaar arrangements to address human rights concerns without inadvertently restricting the export of critical cybersecurity tools.

Patent and Trademark Office (PTO): The Patent and Trademark Office (PTO) issues patents that protect new inventions and facilitates the commercialization of new technologies. Rapid innovation in the technology sector means that most of the largest patent holders in the US are tech companies. High-quality patents are critical to the growth and success of small American businesses and tech startups. At the same time, poor-quality patents can impede innovation and drain valuable resources from the technology sector. Appointees to the PTO should be well versed in issues related to technology intellectual property and committed to issuing and ensuring high quality patents.

Office of Innovation and Entrepreneurship (OIE): The Office of Innovation and Entrepreneurship (OIE) has launched numerous offices and initiatives devoted to the

innovation economy and works to foster a more advanced U.S. economy focused on turning new ideas and inventions into products that spur job growth, create competition, and promote economic development. Commerce has focused on supporting U.S. innovation across the globe, and developing stronger trading partnerships that bolster entrepreneurs. One vehicle for this is the Presidential Ambassadors for Global Entrepreneurship (PAGE). The PAGE initiative consists of leading American entrepreneurs who provide their insights and leadership to developing the next generation of entrepreneurs.

The Department of Commerce has a vast array of tools at its disposal to encourage investment and job creation in the United States. We encourage retaining four significant organizational structures to aid in ensuring those tools are well deployed:

- Continue the training of Foreign Commercial Service Officers to be "digital attachés" placed in key international posts (ASEAN, Brazil, China, the EU, and Japan);
- Retain the Digital Economy Board of Advisors;
- Appoint a Chief Data Officer at the Department to assist in the negotiation of international data transfer frameworks (e.g. EU-U.S. Privacy Shield); and,
- Retain the position of "Senior Adviser for Digital Economy," to head the Digital Economy Leadership Team and the support international competitiveness of U.S. companies.

Department of Defense (DoD)

Cyberspace is a domain of 21st century warfare – equal to air, sea, land, and space. Information dominance enables DoD success across those co-equal domains. Information technology platforms and services are the key element in this success, whether functioning offensively or protecting vital national security assets. The DoD is the world's single largest consumer, and to that end, holds the greatest buying power. The rest of government looks to DoD as a leader and frequently follows its practices.

It is a national security imperative that DoD leaders understand and implement the best ICT utilization and acquisition practices to ensure favorable outcomes. From the Secretary of Defense, to service CIO's, Combatant Commanders, platoon leaders, and the individual service member – all use technology daily to complete their mission sets, from the smallest administrative task to the largest operational and strategic goals. We urge the Trump Administration to seize the opportunity of a new start and make information technology education, understanding, and utilization an inherent part of the warfighter's instruction, training, and mindset.

DoD has a long history of developing new technologies, and innovative thinking. This past year the Defense Innovation Advisory Board was launched to connect our nation's leading technology CEO's and innovators to advise the Secretary of Defense on ways to bolster the Department's innovation footprint. DoD's Defense Innovation Unit Experimental (DIUx) serves as a bridge between those in the U.S. military solving some of our nation's toughest security challenges and companies operating at the cutting edge of technology. DIUx has established hubs in major tech centers such as Silicon Valley, Boston, and Austin. The Manufacturing Industrial Base Policy (MIBP) office is also critical to ensuring that our military can rely on a robust, domestic, advanced manufacturing industrial base. DoD has also developed the Defense Digital Service (DDS), an agency within the Pentagon to cultivate some of our nation's best technical talent to tackle projects that are paramount to the nation's security.

The Defense Advanced Research Projects Agency (DARPA) is an important source of research and development expertise. DARPA funding to the technology sector results in innovations that maintain our military and security leadership.

Similarly the National Security Agency (NSA) also maintains a serious research and development program that is essential to the nation's cybersecurity.

Additional funding for critical research to both DARPA and NSA is essential to meeting the Trump administration's goals in this area. The Manufacturing Industrial Base Policy (MIBP) office is also critical to ensuring that our military can rely on a robust, domestic, advanced manufacturing industrial base.

Director of National Intelligence (DNI)

Along with the DoD the Director of National Intelligence (DNI) plays an important role in the national security arena. In addition to coordinating seventeen individual Intelligence Community agencies, the DNI also sponsors path-breaking research and development activities in support of U.S. intelligence missions. The DNI has also established activity parallel to DoD's DARPA – the Intelligence Advanced Research Projects Agency (IARPA). Projects at IARPA need to be coordinated with those at both DARPA and NSA to meet evolving cybersecurity requirements.

Department of Education (ED)

In order to prepare today's students for tomorrow's workforce, we must have a strong education system that recognizes the importance of both academic and technical skills. Today's K-12 and higher education institutions are leaders in developing innovative delivery models, using technology to improve student outcomes, and encouraging students to take ownership of their own success. For example, career and technical education

programs provide students with industry-recognized credentials and connect high school students with postsecondary opportunities and careers.

Personalized learning technologies allow educators to tailor instruction to meet individual students' needs. We must support state and local education agencies in their efforts to customize education as they know the local and regional needs best. The Department of Education can be a great resource in disseminating the latest discoveries in best practices, while helping communities create solutions to difficult educational issues without unduly influencing local decision-making. For example, the Department, under Trump leadership, should give close consideration to encouraging all schools to offer computer science education.

The Privacy and Technical Assistance Center (PTAC) is the key resource on student data privacy rules and expectations for school districts, school service providers, and parents. Without PTAC schools would be lost. The Office of Innovation and Improvement provides key leadership in investigating best practices from innovative strategies being developed around the country. The Office of Educational Technology (OET) has focused on collaborating with leading institutions and developed policies to promote the use of technology for transforming education. Given the importance of technology education today, the OET could play a pivotal role shaping policies that will bolster student achievement through tech-enabled tools in the classroom. The OET is a key office and must be led by a person with a depth of expertise in technology as well as instruction. There are also key roles within the Department, like the Chief Privacy Officer, that must be filled by a person with strong expertise in technology.

Department of Energy (DoE)

The mission of the Department of Energy (DoE) is to ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges through transformative science and technological solutions. Over its thirty-five year history, the DOE has shifted its emphasis and focus as the needs of the nation changed. Today's electrical grid is undergoing an unprecedented evolution that is driven by consumer-led deployments of distributed energy resources (DERs), including distributed solar, energy storage, electric vehicles, controllable loads, and energy efficiency. These innovations present the unique opportunity to modernize our aging grid and support diversification of our electricity supply, while improving customer choice, increasing reliability, and maintaining public safety, all at an affordable cost.

The Trump Administration should continue to emphasize the central role of the DoE and help take its focus and responsibility into the next phase. Technology and innovation can only help the U.S. create sustainable solutions to grow manufacturing and blue-collar jobs if it continues to receive support. DoE's Office of Science and the network of national

labs are key parts of our country's innovation infrastructure in areas such as high performance computing.

Federal Energy Regulatory Commission (FERC) decisions and orders apply to the independent system operators (ISOs) and regional transmission organizations (RTOs) that run much of the U.S. power grid. About 70 percent of the country is served by ISOs and RTOs, which fall under federal jurisdiction. The two appointments to the ISO and RTO in the very near term should be prepared to modernize the grid and support the significant progress made to diversify and sustain U.S. global competition.

Department of Health and Human Services (HHS)

The Department of Health and Human Services (HHS) must grapple with the incredibly important challenge of rising costs in the U.S. healthcare system. America's healthcare spending is expected to reach $3.5 trillion in 2017, representing 18% of the entire U.S. economy. This spending number is further projected to reach 20% of the economy by 2025.

A 21st century healthcare system must integrate and embrace the innovative ICT available to improve patient care and lower costs. Today, the connected health sector stands at the precipice of incredible growth and has the potential to create many high-paying jobs across the U.S., which will benefit the American patient. HHS should implement policies that permit caregivers and patients to flexibly utilize these advanced products and services across public and private systems and practices. The Trump administration's appointments to this integral agency will have the ability to shift the U.S. government away from dated policies that hold these innovations back.

Department of Homeland Security (DHS)

The Department of Homeland Security faces many challenges today in its mission to secure our nation. Technology plays a vital role in helping DHS to secure both cyberspace and critical infrastructure; prevent terrorism; enhance security; manage our borders; administer immigration laws; and ensure disaster resilience. DHS's missions are wide-ranging and technology is essential to DHS's mission. We recommend the following to support and strengthen DHS:

- Continue to empower DHS and its many stakeholders to share cyber threats and secure IT systems and networks as cyber threats evolve;
- Continue outreach to the private sector through programs such as the Homeland Security Innovation Programs to acquire innovative technology;

- Continue engagement with the private sector to implement the U.S. Customs and Border Protection (CBP) 2016 Customs Reauthorization Bill that addresses trade facilitation, trade enforcement, and other trade tools that impact the technology sector; and,
- Attract and develop a skillful cyber workforce.

We strongly advise that the Trump Administration keep and fill these positions with individuals from the private sector with a strong background in business transformation, cyber and technology to continue to transform and mature the agency and ensure long-term mission success.

Department of Labor (DoL)

The Department of Labor is dedicated to fostering, promoting, and developing policies to support and advance our nation's workforce. As technology becomes more entwined in all facets of our economy and we collectively face an IT skills gap with more technology jobs available than there are technologists, the Department of Labor has an important mission to align educators, businesses, and government to meet the imperatives of the growing digital economy.

As digital technology introduces new business models and the nature of work shifts, the Department of Labor is increasingly involved in setting the rules for employers and employees. Thus, senior appointees to Department positions should have public and private sector experience and a familiarity with the key labor and technology issues.

Department of State (DoS)

DoS has a crosscutting role in digital affairs: the portfolios of its staff touch every aspect of these issues from national security to internet freedom and human rights online. DoS dialogue with various countries (e.g., India, Japan, and Korea) has broadened to include issues such as internet governance and data localization so much so that its mission also encompasses digital diplomacy. DoS is key in ensuring that other countries value "open and interoperable" communications networks. The Chief of Mission positions for countries like China, France, and Germany have helped advance diplomatic and foreign policy efforts in information technology issues. Close coordination with the Department of Commerce on cybersecurity and privacy issues–specifically, the NSTC subcommittee on commercial privacy–has helped ensure the success of digital economy officers, cyber officers, and digital attaches around the world.

State should continue to designate the Under Secretary of State for Economic Affairs as the ombudsperson under the EU-U.S. Privacy Shield. This position plays a central role in responding to concerns brought by EU persons about U.S. intelligence

activities. Since the United States and the European Union will be conducting a Privacy Shield compliance review in the summer of 2017, we urge the Trump Administration to ensure that the Ombudsperson role is filled by a strong person to carry out the role.

The State Department has also built the Global Entrepreneurship Program (GEP) to enhance entrepreneurship through support from the private sector and the federal government. It has made "economic statecraft" a major pillar of the U.S. foreign policy agenda. The GEP has worked closely with entrepreneurs, startup incubators, investors, and corporations around the world to strengthen economic opportunities.

With that in mind, we urge building out a number of critical roles, specifically:

- The Digital Economy Officer program, which places economic officers at key posts abroad to build greater awareness of digital issues into the overseas missions and regional and country desks; and,
- The Coordinator for Cyber Issues position, which reports directly to the Secretary of State and is charged with advancing U.S. interests on issues of cybersecurity, cyber operations, and intellectual property protection, (this includes the task of leading a dialogue with China regarding issues of hacking and commercial espionage).

Retaining and filling these positions with individuals from the private sector with a strong background in technology issues will directly support President-elect Trump's vision of bolstering U.S. cybersecurity.

Department of Transportation (DoT)

Technology is the perfect platform for DoT to fulfill its mission of building a fast, safe, efficient, accessible and convenient transportation system for the American people. It is time to build smart by focusing on infrastructure investments that incorporate Internet of Things (IoT) technology and artificial intelligence to improve performance.

Cities are today's laboratories for innovation: local governments are actively partnering with the tech sector to find solutions to city challenges. In 2016 the DoT held its first Smart City Challenge. DoT is helping local governments define what it means to be a "Smart City" and fully integrate innovative technologies – self-driving cars, connected vehicles, and smart sensors – into their transportation network.

The National Highway Transit Safety Administration (NHTSA) should continue to shape the evolving safety requirements of autonomous and connected vehicles. The Federal Aviation Administration (FAA)–the nation's leading regulator of unmanned aerial systems (UAS)–will require staff that work cooperatively with industry, state and local governments to empower the safe and economically viable use of UAS technology.

President-elect Trump discussed improving the environment of our urban centers. In our view, the Administration will find that mayors, the private sector and universities are eager to collaborate on the deployment of new technologies to make cities work better for citizens. In order to better secure and improve America's vital networks, DoT appointees should have both knowledge of the inter-connected nature of smart transportation and an understanding of critical cybersecurity considerations when building infrastructure.

Department of Treasury (DoTR)

DoTR is a key player on several critical issues to the nation. In the area of tax, it is essential the incoming team come prepared to modernize our tax code in order to enhance the global competitiveness of U.S. companies and promote innovation and growth. Appointees must understand the global challenges facing U.S. technology companies from taxation on the digital economy and misguided, unilateral actions from other jurisdictions.

In addition, as technology introduces new business models and revolutionizes the customer experience, DoTR must critically examine issues created by the global movement of capital. Currency management is changing with the introduction of virtual currencies such as Bitcoin and DoTR must regulate such currency transaction reporting. Broadly, appointees should have knowledge of the cross-border nature of innovation, the sharing economy, and the digital nature of capital management.

Environmental Protection Agency (EPA)

The Environmental Protection Agency is committed to protecting human health and the environment for all Americans. Technology continues to play a leading role in advancing EPA's mission by delivering sustainable IT products and services to consumers, businesses and the federal government. These innovations save energy, decrease waste and emissions, advance American competitiveness and improve the health and well-being of American communities.

The incoming EPA leadership team should hold a strong background in science and should seek to protect human health and the environment by adopting a risk-based approach to environmental considerations. Appointees should have a strong understanding of the benefits of technology, and focus on the sector's best practices regarding customer demands for energy-efficient and sustainable products and services. Appointees should also recognize that it is often to the benefit of American industries, including the tech sector, for the U.S. to continue to stake out global leadership positions on select topics.

General Services Administration (GSA)

The U.S. government is the largest single customer of information and communications technologies (ICT) in the world and GSA plays a critical role as the

government's centralized buying authority. GSA manages schedules of goods and services and a suite of government-wide acquisition contracts (GWACs) that serve as the primary sourcing vehicles for the acquisition of ICT hardware, software, services and solutions. GSA is also essential to technology policy as the only organization in the government that can set a government-wide acquisition policy. GSA is also a leader in the early adoption and implementation of technological solutions.

As the owners and managers of the government's real property, GSA has also been a leader in the deployment of technology to better manage buildings, environmental controls, and security concerns, to name a few. Because the Office of Management and Budget has little or no resources to implement and manage the operation of its policy initiatives, GSA frequently pilots, implements, and deploys new policies and technology solutions that have a government-wide application.

The Trump Administration should support GSA in its central role, while ensuring it is not positioned to impede or inordinately control the digitization of government, the modernization of government IT, or the discretion of each agency and department to identify technological solutions for its specific mission needs. At the same time, in order to conserve government finances, the Trump Administration should also ensure that GSA redoubles its efforts to follow the laws and regulations that require the government to use commercial IT and to purchase items and services in a neutral manner through full and open competition.