E.L. WIEGAND PRACTICE GROUPS OF THE FEDERALIST SOCIETY

INTERNATIONAL & NATIONAL SECURITY LAW NEWS

Critical Infrastructure Protection: A New Era of National Security

Walter Gary Sharp, Sr.*

Computers and computer-dependent systems permeate everyone's daily life. From local, state, and federal government decision makers to warfighters, businessmen, lawyers, doctors, bankers, and individuals – everyone relies upon information and information systems that involve the acquisition, transmission, storage, or transformation of information. For as little as five or ten dollars a month, anyone with a computer has access to instantaneous world-wide communications and a wealth of resources on the Internet. Computerized sensing and control devices now monitor transportation, oil, gas, electrical, and water treatment systems throughout our nation instead of human watch standers. Satellites serve as the backbone of our telecommunication systems and our economic well being. The Global Positioning System (GPS) guides virtually all of the commercial aircraft in the world.

The Department of Defense is heavily dependent upon timely and accurate information, and is keenly focused on information operations and information assurance. Military commanders in Bosnia receive real-time satellite imagery. Marine warfighters are training on Wall Street to learn how to respond during information-intense situations; Navy commanders are focusing on network centric warfare; Army planners believe the use of a tactical internet will have profound implications for battle tactics; and Air Force information warriors now have their own squadron. Over 95% of Department of Defense telecommunications travel over commercial systems, and the interdependence of our civilian infrastructure and national security grows dramatically on a daily basis. In a few short decades, the global networking of computers via the Internet will very likely be viewed as the one invention that had the greatest impact on human civilization – and perhaps the greatest challenge to our national security.

All of these computers and computer-dependent systems are vulnerable to physical and electronic attack – from the computers on which individuals store and process classified information, privileged attorney-client information, or proprietary data, to our nationwide telecommunication and banking systems. Indeed, the year 2000 problem demonstrates that we are

continued on page 3

In This Issue

Editor's Letter

In this issue of the International and National Security Law Practice Group newsletter, we approach the problems of national security from both a traditional and a futuristic track. In both instances, developments in current events call for new considerations of the law and legal policies.

National security has always encompassed at the minimum the threat of physical attack across our borders. The most immediate form of this threat during the Cold War took the form of intercontinental ballistic missiles, which accordingly spawned the legal field of arms control and international security agreements. The most controversial of these efforts has been the Anti-Ballistic Missile (ABM) Treaty of 1972. This treaty paradoxically sought to make the United States secure by forbidding it to secure itself from missile attack. The subsequent demise of the Soviet Union coupled with the continued proliferation of weapons of mass destruction has seriously challenged the initial premises underlying the ABM treaty. The issue has the attention of both the Congress and the President, and has prompted the first contribution to this issue of the International & National Security Law News. We reprint here a recent letter from President Clinton to Congressman Gilman of the House Committee on International Relations, addressing the Administration's intended approach to the ABM Treaty and succession problems. An opposing view appears in the Executive Summary of a memorandum commissioned by the Heritage Foundation from the law firm of Hunton & Williams, which will be presented to Senate Majority Leader Trent Lott later this summer.

Beyond the more conventional threat of physical attack, attention has been growing to the dangers of hostile acts in cyberspace. Professor Walter Gary Sharp is a leader in the nascent field of law that concerns our vulnerabilities in communications, commerce, and computing and how both government and the private sector might legally act to protect them. His article in this issue addresses the basic problems of critical infrastructure protection and where we stand in recognizing and facing the problem. Professor Sharp will also be taking part in panels at this fall's Lawyers Convention where he will speak to these and other topics.

I encourage all of you to attend this year's Lawyers' Convention as well as to submit articles or letters to the editor. Our future issues may report on recent Practice Group events such as our forum this June on the proposed International Criminal Court, as well as the proceedings planned for the Lawyers' Convention, including panels on privatization of Intelsat and Critical Infrastructure Protection. All submissions are welcome, and stand a good chance of being published.

Ted Cooperstein

WE WELCOME RESPONSES AND SUBMISSIONS.

Contact:

Ted Cooperstein
tcoop@earthlink.net

Critical Infrastructure Protection
continued from page 1

even vulnerable to our own misfeasance and poor planning. A single non-nuclear, electromagnetic pulse can destroy or degrade circuit boards and chips, or erase all electronic media on Wall Street, in the Pentagon, or your local bank. The loss of a single satellite can terminate service for over 90% of the 45 million pagers in the United States, as well as interrupt service for thousands of cable television stations and credit card transactions. GPS signals can be spoofed or degraded, or used as part of highly accurate targeting systems. Advanced computer technology can help build nuclear weapons. Internet and computer crime is so simple that two teenagers in Cloverdale, California with a mentor in Israel can break into sensitive national security systems at the Department of Defense. Information warfare experts can use global television to selectively influence political and economic decisions or produce epileptic-like spasms in viewers. Cyber warfare of the 21st century could significantly impact the daily lives of every man, woman, and child in America.

Developing Economic Potential

Although the telephone was invented in 1876, the personal computer in 1975, and the Internet in the 1970's, the world wide web, as we know it today, was not invented until 1991. By the year 2002, Americans will spend nearly $38 billion online annually. The enormous economic potential of the world wide web was quickly recognized by the United States Government.

On 15 September 1993, President Clinton established the "United States Advisory Council on the National Information Infrastructure" by Executive Order 12864. This Advisory Council was tasked to advise the Secretary of Commerce on a national strategy and other matters related to the development of the National Information Infrastructure (NII). The final report of the Advisory Council was transmitted to the President on 30 January 1996. The Council's report, "A Nation of Opportunity: Realizing the Promise of the Information Superhighway" (available at GPO) made a series of detailed recommendations that addressed four issues: reducing legal, regulatory, and policy barriers on the key areas of American life and work that will be impacted by the NII; gaining universal access to the NII for all; developing rules of the road regarding intellectual property, privacy, and security on the NII; and identifying the roles of the key stakeholders in developing the NII.

On 1 July 1997, President Clinton approved another report entitled "A Framework for Global Electronic Commerce." This report set forth the Administration's vision of the emerging global electronic market-place with minimal regulation and no discriminatory taxes and tariffs. In developing our economic potential, however, we also increase our vulnerabilities.

Identifying National Security Vulnerabilities

As the United States Government studied the tremendous economic potential of the Internet, it began to realize the significant national security vulnerabilities inherent in our reliance on computers and computer-dependent systems. On 15 July 1996, President Clinton signed Executive Order 13010 (available at www.pccip.gov), establishing the "President's Commission on Critical Infrastructure Protection" (CIP). This Commission was the first national

effort to address the vulnerabilities created by the new information age.

Executive Order 13010 declared that certain "national infrastructures are so vital that their incapacity or destruction [by either physical or cyber attack] would have a debilitating impact on the defense or economic security of the United States." The Executive Order detailed eight categories of critical infrastructures: telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue); and continuity of government. The President acknowledged in the text of the Executive Order that because so many of these critical infrastructures are owned and operated by the private sector, "it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation."

The President's Commission was chaired by retired Air Force General Robert T. Marsh, and was comprised of members of the federal government and industry. Its work was guided by a Steering Committee of senior government officials and an Advisory Committee of key industry leaders. The Commission was tasked to develop a comprehensive national strategy for protecting critical infrastructures from physical and electronic threats. Because threats to our nation's critical infrastructure were considered very real, the Executive Order also established an "Infrastructure Protection Task Force" (IPTF) as an interim coordinating measure. The IPTF was created within the Department of Justice to increase the "coordination of existing infrastructure protection efforts in order to better address, and prevent, crises that would have a debilitating regional or national impact."

A hundred-page unclassified version of its report entitled "Critical Foundations: Protecting America's Infrastructures" (available at GPO and www.pccip.gov) was released on 13 October 1997. The President's Commission found no evidence of an "impending cyber attack which could have a debilitating effect on the nation's critical infrastructures." It did, however, find a widespread capability to exploit our infrastructure vulnerabilities that is real and growing at an alarming rate for which we have little defense. The Commission also identified potential threats that included insiders, recreational and institutional hackers, organized criminals, industrial competitors, terrorists, and states. Because our nation's critical infrastructures are mainly privately owned and operated, the Commission concluded that "critical infrastructure assurance is a shared responsibility of the public and private sectors," and the only sure way to protect infrastructures is through a real partnership between infrastructure owners and the government.

The Commission made a series of seven findings. First, information sharing is the most immediate need. Second, responsibility is shared among owners and operators and the government. Third, infrastructure protection requires integrated capabilities of diverse federal agencies, and special means for coordinating federal response to ensure these capabilities are melded together effectively. Fourth, the challenge is one of adapting to a changing culture. Fifth, the federal government has important roles in the new infrastructure protection alliance with industry and state and local governments. Sixth, the existing legal framework is imperfectly attuned to deal with cyber threats. Seventh, research

and development are not presently adequate to support infrastructure protection. To prepare a policy framework for its recommendations, the Commission also adopted seven principles: build on that which exists; depend on voluntary cooperation; start with the owners and operators; practice continuous improvement; coordinate security with maintenance and upgrades; promote government leadership by example; and minimize changes to government oversight and regulation. The Commission's recommendations addressed what actions it believed the federal government should take, what actions industry should take, and what actions that government and industry must take in partnership.

Key to the Commission's national strategy is the international and domestic legal regime required to protect against cyber threats. The objective of the Commission's legal initiatives was to sponsor legislation to increase the effectiveness of federal infrastructure assurance and protection efforts. Eighteen specific recommendations were made by the Commission that were intended to strengthen existing legal frameworks for federal response to and deterrence of incidents and the adequacy of criminal law and procedure, as well as to change those laws that inhibit protective efforts and information sharing.

The report of the President's Commission has been criticized by some in government and industry for not providing complete or detailed solutions to our infrastructure vulnerabilities after fifteen months of work. It is, however, an extraordinary effort that gives our national leadership a recommended conceptual and organizational framework to analyze, manage, and defend against the threats to our critical infrastructure. It is also the template upon which the President has designed his plan for critical infrastructure protection.

Defending our Critical Infrastructure

On 22 May 1998, President Clinton issued two Presidential Decision Directives (PDD) that will build the interagency framework to strengthen and coordinate our critical infrastructure defense programs. PDD 62, Combating Terrorism, is the broader of the two directives and focuses on the growing threat of all unconventional attacks against the United States such as terrorist acts, use of weapons of mass destruction, assaults on critical infrastructures, and cyber attacks. It establishes the position of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. Richard Clarke has been appointed to fill this National Security Council position, which is intended to bring a more systematic, program management approach to counter-terrorism, protection of critical infrastructure, preparedness, and consequence management. The National Coordinator will report to the President through the Assistant to the President for National Security Affairs.

PDD 63, Critical Infrastructure Protection (a PDD 63 White Paper is available at www.pccip.gov), builds upon the recommendations set forth in the report of the President's Commission on Critical Infrastructure Protection. It calls for immediate action by the federal government and a national effort between government and industry to swiftly assure the continuity and viability of our critical infrastructures. The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism designated pursuant to PDD 62 is responsible for coordinating the implementation of PDD 63. The

President's first, and perhaps most important, of ten principles set forth to guide the interagency in addressing and eliminating potential vulnerabilities is for those involved to consult with and seek input from the Congress on approaches and programs to meet the objectives of PDD 63.

President Clinton has declared in PDD 63 a national goal of significantly increased security for government systems by the year 2000 and a reliable, interconnected, and secure information system infrastructure by the year 2003. To achieve this goal, PDD 63 organizes the federal government around four components: lead agencies for sector liaison, lead agencies for special functions, an interagency working group for critical infrastructure protection coordination, and a National Infrastructure Assurance Council. Unlike most Presidential decision directives which focuses only on government organization and interagency coordination, PDD 63 is remarkable in its efforts to organize a public-private partnership to reduce critical infrastructure vulnerability.

For each of the eight major sectors of our economy that are vulnerable to infrastructure attack, a single U.S. Government department is designated to serve as the lead agency for liaison to cooperate with the private sector. These sector liaisons will coordinate with private sector representatives to address problems related to critical infrastructure protection, to develop a sector component of the National Infrastructure Assurance Plan, and to develop and implement a Vulnerability Awareness and Education Program for their sector. By way of example, the Department of Commerce is the lead agency for the information and communications sectors, and the Department of Treasury is the lead agency for the banking and finance sectors. A National Plan Coordination (NPC) staff will integrate these sector component plans into the comprehensive National Infrastructure Assurance Plan and coordinate the analyses of the U.S. Government's own dependencies on critical infrastructure. PDD 63 specifies that the NPC shall be an office of the Department of Commerce beginning fiscal year 1999. On 22 May 1998, the Secretary of Commerce named Jeffrey Hunker, formerly Deputy Assistant to the Secretary of Commerce for economic policy development and special initiatives, as Director of the national Critical Infrastructure Assurance Office (CIAO). The Director of the CIAO will report to the PDD 62 National Coordinator and will be responsible for the duties assigned by PDD 63 to the NPC staff.

Similarly, for each of the functions that must be chiefly performed by the federal government, four lead agencies for special functions have been designated. The Department of Justice is the lead agency for law enforcement and internal security, the Central Intelligence Agency is the lead agency for foreign intelligence, the Department of State is the lead agency for foreign affairs, and the Department of Defense is the lead agency for national defense. The departmental representatives from these twelve lead agencies, as well as representatives from other relevant departments and agencies, will meet to coordinate the implementation of PDD 63 under the auspices of the Critical Infrastructure Coordination Group (CICG), which will be chaired by the PDD 62 National Coordinator.

The National Infrastructure Assurance Council will consist of a panel of major infrastructure providers and state and

local government officials. Its purpose is to enhance the partnership of the public and private sectors, and it is authorized to make reports to the President as it believes appropriate. The Chairman of the Council will be appointed from industry, and the PDD 62 National Coordinator will serve as the Council's executive director.

Every department and agency of the federal government is responsible for protecting its own critical infrastructure, and must develop a plan to do so within 180 days from the issuance of PDD 63. The PDD 62 National Coordinator is responsible for coordinating the analyses required by the departments and agencies, and the CICG will sponsor an expert review process for those plans. These plans must be fully implemented no later than 22 May 2000, and are supposed to serve as a model to the private sector on how best to protect critical infrastructure. Also within 180 days, the Principals Committee must submit to the President a schedule for completing the National Infrastructure Assurance Plan.

PDD 63 also authorizes the Federal Bureau of Investigation to establish a National Infrastructure Protection Center (NIPC) to provide a national focal point for gathering information on threats to critical infrastructures. The NIPC will serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. It will also provide the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts. Should the threat be foreign, then the President may place the NIPC in a direct support role to either the Department of Defense or the Intelligence Community. The NIPC was actually created on 27 February 1998, and Michael Vatis was appointed to serve as its chief.

Finally, PDD 63 encourages the owners and operators of the critical infrastructures to create a private sector Information Sharing and Analysis Center (ISAC). The design of the ISAC, and its relationship to the NIPC, was left to the determination of the private sector, however, the PDD 63 National Coordinator is required to identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Implications for the Legal Community

The implications for the legal community are profound. In many respects, international and domestic law has been overwhelmed by a revolution in technology that is driving an unparalleled evolution in national security and online commercial law which involves state and local governments, industry, and individual citizens at all levels.

Americans have felt safe at home during the 20th century from foreign attack, and armed conflict has been the province of the federal government and the military industrial complex. Wars were fought elsewhere because the United States has the ability to project its great military power overseas and protect American soil from attack. Our economy has thrived and computer technology has flourished. As the United States became the world's greatest military and economic power, its computer-dependent infrastructure also became the world's most vulnerable and lucrative target. Our military and economic strength forces those who wish to do us harm to attack our soft underbelly – the computer and computer-dependent systems throughout our nation that were initially built with an open architecture and without security foremost in mind. This soft

underbelly that supports a war effort may have always been a lawful target under the laws of armed conflict, but without today's Internet technology, enemy states could not reach these targets on American soil. Today, however, hostile states can easily target America's heartland with a $900 computer and techniques readily available on the Internet. Given that over 95% of Department of Defense telecommunications travel over commercial systems, and the growing interdependence of our civilian infrastructure and national security complex, lawyers must evaluate whether the rules of military necessity and collateral damage under existing laws of war, jus in bello, are adequate in the information age.

National security lawyers must also try to define what is a use of force in cyberspace. An unauthorized intrusion by individuals or terrorists into a national security system is criminal activity under the jurisdiction of the Department of Justice. In contrast, the same type of intrusion by a state, or a state sponsored individual or terrorist, may be an unlawful use of force under the Charter of the United Nations that gives rise to a state's inherent right of self-defense. Lawyers must define when espionage and intelligence gathering by a state within a national security computer system, otherwise lawful under international law, becomes a hostile act or a demonstration of hostile intent that authorizes either an electronic or a conventional, steel-on-target response. The law of conflict management, jus ad bellum, should be reviewed and refined to prevent future conflict.

Lawyers throughout the federal, state, and local governments must review existing legislation, and propose new legislation if necessary, to ensure that the United States has a coordinated approach toward the prevention, mitigation, response, recovery, and reconstitution of damage to our critical infrastructure. Department of Justice lawyers and prosecutors in all fifty states must initiate legislative changes that will strengthen our ability to investigate, prosecute, and deter computer crime. Multinational mutual legal assistance treaties are needed to enhance international cooperation and eliminate safe havens that may exist around the world. While we strengthen these laws, we must also ensure that we protect the privacy rights of all consumers and operators, and that we do not restrict an online free market by overregulation. We must also ensure that existing and new legislation clearly provides for procedures for the government and industry to test their own systems without fear of violating the law.

Lawyers are also challenged with the new application of commercial law to online and electronic storage applications. Liability for the buying and selling of goods and services online raises many issues involving online contracts, digital signatures, and electronic payments. Internet provider liability issues based on theories of direct infringement, contributory infringement, and vicarious liability abound because of the ease with which copyright protected works can be duplicated and distributed on the Internet. The trend in the courts appear to limit the liability of internet service providers (ISPs) for content-based liability in defamation suits, but ISPs need to be careful about the nature of their service contracts with publishers to ensure they keep their distance from an editorial role that may give rise to liability.

Business lawyers and trial attorneys must consider the trustworthiness and admissibility of electronic records and emails in an online world. Corporate

lawyers must be concerned about the liability of their principals and board of directors for failing to maintain legally acceptable standards of care in protecting their computers and information systems from theft, data manipulation, or destruction. Similarly, lawyers for insurance companies should be proactive and develop standards of care and security practices that are prerequisites to coverage. Intellectual property lawyers must be concerned about the unauthorized and misleading use of similar domain names and URLs. Civil rights lawyers must address online First Amendment issues raised in recent legislation attempting to protect children from sexually explicit materials and predators, and privacy issues that arise when employers track Internet usage and electronic communications of their employees.

A resolution to the national debate over encryption will have significant ramifications for law enforcement and private industry – in the meantime, international travelers must be careful carrying common software packages, such as AOL 4.0 or PGP, because United States law prohibits their export from the United States without an export control license. Depending upon the jurisdiction where they practice, lawyers must be concerned about breaching their ethical duty of confidentiality when sending electronic mail over the Internet. They must also be aware of issues that involve the unauthorized practice of law that may arise when advising clients with a multistate presence. Similarly, lawyers who have a federal practice such as immigration law that market over the Internet must be concerned about the unauthorized practice of law when they advise clients in another state via email. Lawyers who advertise on the web must also be concerned about unethical advertising issues in some states when using key words that suggest specialties. The new national security and online commercial law issues that are evolving have the potential to touch every lawyer, regardless of whether they are in government service or private practice – and the burden is on the entire legal profession to help create a plan that will protect our critical infrastructure while protecting individual and business rights in cyberspace.

Analysis and Conclusion

The President's Commission on Critical Infrastructure Protection concluded that our vulnerability to cyber attack by criminals, terrorists, and hostile states is real and growing. The Commission's report provided a series of detailed recommendations that would provide a strategy to defend our critical infrastructures. PDD 63 embraces the Commission's report by establishing a public-private partnership, and the structure within the federal government to lead industry by example as to how best to protect our critical infrastructure. The President has demonstrated by his actions and PDD 63 his commitment to working with the private sector and Congress.

In fact, Congress deserves as much of the credit as any government agency or office for identifying the vulnerabilities of our infrastructure and shaping the solution we now see in PDD 63. Many of the initiatives and conclusions of the Commission's report and PDD 63 were shaped and influenced, if not originated, by Congressional hearings. Without the leadership and initiative of Senator Jon Kyl and Congressman Porter Goss, to name only two who have been actively involved, the United States would be much further

from developing a plan to protect our nation's critical infrastructure.

The two most difficult issues facing the United States concern information sharing and encryption. Information must flow both ways between the government and private industry to ensure the United States has an effective early warning mechanism against an organized cyber attack. Private industry must have encryption to ensure the integrity of electronic transactions, and United States companies must have the economic and competitive advantage of being able to enter the international market. Encryption will also help make our critical infrastructure more secure. Law enforcement and intelligence agencies, however, have a legitimate need to be able to conduct electronic surveillance in the age of sophisticated digital encryption. Within very carefully crafted constitutional, statutory, and regulatory safeguards and procedures, both the law enforcement and intelligence communities already have the right to conduct electronic surveillance as a matter of law under appropriate circumstances – but with the technology of digital encryption, they will not have the technical capability to do so without a system in place that allows them access to a key.

Unfortunately, the principal reason why there is not yet a solution for either the information sharing or encryption issue is in the lack of trust that private industry has in government oversight. There has also been disagreement as to who will bear the cost to private industry of implementation. The solutions will not be easy. What is clear, however, is that both the government and private industry have competing equities in developing a solution to each of these issues, and that both government and private industry will have to compromise to reach a solution. What is also clear, is that not having a solution to the information sharing issue leaves critical infrastructures more vulnerable, and not having a solution to the encryption issue places American businesses at an economic and competitive disadvantage.

Just as with the report of the President's Commission, many people in government and industry will, undoubtedly, criticize and find what they view as faults with PDD 63. Indeed, it is not perfect, and perhaps never intended to be. As always, hindsight and experience will likely prove there was a better approach. The report of the President's Commission and PDD 63 is, however, an extraordinary accomplishment. Together, they have given us the ability to grasp an extremely complex problem and have given us a solution that assigns relatively clear responsibilities within the government. PDD 63 will move the Executive, Congress, and private sector forward in partnership to define the National Infrastructure Assurance Plan that will effectively protect our great nation's critical infrastructure.

*Walter Gary Sharp, Sr., an Adjunct Professor of Law at Georgetown University Law Center, is the Director of The Aegis Center for Legal Analysis, Aegis Research Corporation, Falls Church, Virginia. *The opinions and conclusions expressed herein are those of the author and do not necessarily reflect the views of any governmental agency or private enterprise.*

Editor's Note: A panel on Critical Infrastructure Protection and its legal implications will take place during the Federalist Society's National Lawyers Convention on Friday, November 13, 1998 at 11:00 a.m. at the Mayflower Hotel in Washington, D.C..

Anti-Ballistic Missile Treaty: A Letter from the White House

The following letter was written to The Honorable Benjamin Gilman, Chairman of the House of Representatives's Committee on International Relations.

Dear Mr. Chairman:

Thank you for your letter concerning the Anti-Ballistic Missile (ABM) Treaty succession arrangements. As I said in my letter of November 21, 1997, the Administration will provide to the Senate for its advice and consent the Memorandum of Understanding (MOU) on ABM Treaty succession, which was signed on September 26, 1997. Moreover, the MOU will settle ABM Treaty succession. Upon its entry into force, the MOU will confirm Belarus, Kazakhstan, Russia, and Ukraine as the successor states to the Soviet Union for purposes of the Treaty and make clear that only these four states, along with the United States, are the ABM Treaty Parties.

In your letter of March 3, you state that if the Administration is unable to identify any country in addition to the United States that is clearly bound by the Treaty, then you would have no choice but to conclude that the Treaty has lapsed until such time as the Senate approves a succession agreement reviving the Treaty.

Following the dissolution of the Soviet Union, ten of the twelve states of the former Soviet Union initially asserted a right in a Commonwealth of Independent States resolution, signed on October 9, 1992, in Bishkek, to assume obligations as successor states to the Soviet Union for purposes of the Treaty. Only four of these states have subsequently participated in the work of the Standing Consultative Commission (SCC), and none of the other six has reacted negatively when we informed each of them that, pursuant to the MOU, it will not be recognized as an ABM successor state. A principal advantage of the Senate's approving the MOU is that the MOU's entry into force will effectively dispose of any such claim by any of the other six states.

In contrast, Belarus, Kazakhstan and Ukraine each has ABM Treaty-related assets on its territory: each has participated in the work of the SCC; and each has affirmed its desire to succeed to the obligations of the former Soviet Union under the Treaty.

Thus, a strong case can be made that, even without the MOU, these three states are Parties to the Treaty.

Finally, the United States and Russia clearly are Parties to the Treaty. Each has reaffirmed its intention to be bound by the Treaty; each has actively participated in every phase of the implementation of the Treaty, including the work of the SCC; and each has on its territory extensive ABM Treaty-related facilities.

Thus, there is no question that the ABM Treaty has continued in force and will continue in force even if the MOU is not ratified. However, the entry into force of the MOU remains essential. As I pointed out in my letter of November 21, the United States has a clear interest both in confirming that these states (and only these states) are bound by the obligations of the Treaty, and in resolving definitively the issues about ABM Treaty succession that are dealt with in the MOU. Without the MOU, ambiguity will remain about the extent to which states other than Russia are Parties, and about the way in which ABM Treaty obligations apply to the successors to the Soviet Union. Equally important,

maintaining the viability of the ABM Treaty is key to further reductions in strategic offensive forces under START II and START III.

I appreciate this further opportunity to clarify the record in this area.

Sincerely,
Bill Clinton

The Collapse of the Soviet Union and the End of the 1972 Anti-Ballistic Missile Treaty

The following is the Executive Summary of a legal memorandum from the law firm of Hunton & Williams to The Heritage Foundation.

This memorandum of law examines the following questions: (1) whether the 1972 Treaty on the Limitation of Anti-Ballistic Missile Systems ("ABM Treaty") between the United States and the now-defunct Union of Soviet Socialist Republics ("U.S.S.R." or "Soviet Union") continues to bind the United States as a matter of domestic and international law; and (2) what would be the legal impact of action by the United States Senate denying its advice and consent to certain ABM Treaty-related agreements signed by the Secretary of State Madeleine Albright with four former Soviet republics in September 1997. These agreements would, among other things, transform the ABM Treaty from what was a bilateral treaty between the United States and the Soviet Union into a multilateral treaty among the United State, Russia, Belarus, Ukraine, and Kazakhstan. In addition, they would revise the ABM Treaty's provisions to reflect and accommodate its new status as a multilateral agreement, and would introduce a number of additional restrictions on activities related to ballistic missile defense (BMD).

The United States and the Soviet Union entered into the ABM Treaty in 1972. The ABM Treaty barred the deployment of a defensive system for protecting the national territories of the United States and the Soviet Union against missile attack. By so doing, the ABM Treaty served to codify a policy that, 25 year later, leaves the United States completely vulnerable to ballistic missile attack.

We believe that the ABM Treaty no longer binds the United States as a matter of international or domestic law. This is because the Soviet Union has disappeared, and there is no state, or group of states, capable of implementing the Soviet Union's obligations under the ABM treaty in accordance with that agreement's terms. Therefore, in view of the relevant facts, and the applicable doctrines of domestic and international law dealing with state succession issues, the ABM Treaty cannot now be said to be in force. That Treaty expired with the Soviet Union, and any new treaty regarding ballistic missile defenses between the United States and any of the former Soviet republics can be effected only through renewed negotiations and the agreement of both the United States and one or more of these states. As a matter of United States law, the United States Senate would have to consent to such an agreement before it could be ratified by the President.

Our conclusions are based upon the following facts and analysis.

Facts

• The United States and the Soviet Union signed and ratified the ABM Treaty in 1972. They agreed to constrain severely the ability to deploy anti-ballistic missile systems to defend their respective territories from ballistic missile attack by imposing a broad array of proscriptions and limiting BMD deployments to two permitted sites per treaty partner.

• The Treaty was modified by a 1974 Protocol, which was ratified in 1976, that reduced the number of allowed ABM sites from two to one per treaty partner.

• The Soviet Union collapsed in 1991, and 15 independent states emerged.

• Since 1993, the United States has proceeded to explore ways to resolve the ABM treaty-related succession issues and to determine whether the rights and obligations of the Soviet Union under the Treaty could be assumed by one or more of the states that emerged following its collapse.

• The United States, Belarus, Kazakhstan, Russia, and Ukraine signed agreements on September 26, 1997, that would, if ratified, effectively multilateralize the ABM Treaty. The President has agreed to submit these agreements for the Senate's advice and consent, although they have not yet been submitted.

• President Clinton asserted that the original ABM Treaty would remain in force even if the Senate rejects the agreement to multilateralize the Treaty. He asserted this in two letters, one dated November 21, 1997, and a second dated May 21, 1998, to Representative Benjamin A. Gilman, Chairman of the House Committee on International Relations.

Analysis

• The President's claim that the ABM Treaty would remain in force even following Senate rejection of the agreement to multilateralize the Treaty raises the question of whether the ABM Treaty is currently in force and legally binding on the United States.

• The resolution of this question must be sought in the rules of international law, as those rules may be applicable in the United States, and in the norms of American constitutional law. When these sources are consulted, a compelling argument emerges that the ABM Treaty no longer binds the United States.

• A review of the ABM Treaty's provisions, its negotiating history, and the subsequent performance of the treaty parties suggests that the obligations assumed by the United States and the Soviet Union under that agreement did not survive the Soviet Union's dissolution. This is because key terms of the ABM Treaty were drafted in a manner that makes them incapable to being performed by any parties other than the United States and the Soviet Union. These key terms depended on the following assumptions:

1) That the geographic expanse of the two states would remain as it was in 1972;

2) That the strategic relationship between the two states would remain essentially as it was in 1972; and

3) That the Treaty would remain a bilateral agreement.

• It has long been recognized that treaties are a species of contract between states. As is true with any contract, the performance of obligations under a treaty may be rendered impossible when one party to the agreement disappears or loses its independent existence. The collapse of the Soviet Union was just such an instance, and it has rendered impossible the performance of the ABM Treaty.

As applied in the treaty context, a state's treaties do not survive its dissolution under this doctrine unless there is a successor state that (1) can be said to continue its predecessor's international legal personality, and (2) can perform the treaty in accordance with its original terms. There is today no post-Soviet state or combination of such states that can be said to continue the Soviet Union's international legal personality or that could perform the totality of its obligations under the ABM Treaty as it was originally drafted.

• The doctrines generally applied to resolving questions of treaty succession suggest that the ABM Treaty did not survive the Soviet Union's dissolution. Two competing doctrines -- the "continuity" model and the "clean slate" model -- are generally applied in determining questions of treaty succession. The continuity doctrine presumes that the treaty rights and obligations of a predecessor state pass to its successor states. However, whether a treaty actually survives under this model depends upon the type of treaty, as well as the type of dissolution suffered by its predecessor state. By contrast, the clean slate doctrine assumes that new states begin afresh, and that the treaties of any predecessor will apply to them only if both the new state and its predecessor's treaty partners agreed (or at least acquiesced) to being bound by a renewed treaty arrangement.

The application of either model to the ABM Treaty leads to the conclusion that it did not survive the Soviet Union's collapse. The ABM Treaty cannot be said to have survived under the application of a continuity model because it was a political treaty that was "personal" to the Soviet Union. None of the former Soviet republics (including Russia) can be said to continue the U.S.S.R.'s international legal personality.

Under the clean slate analysis, the model generally preferred in the post-World War II era, the ABM Treaty also cannot be said to have survived the Soviet Union. Each of the former Soviet republics is a newly independent state, and can accede to the benefits and burdens of the Soviet Union's treaties only upon a renewed agreement with the Soviet Union's former treaty partners. Despite some ambiguous actions and statements, the United States has refused such an agreement to date. Indeed, in the more than six years since the Soviet Union's demise, the State Department has listed the status of the ABM Treaty as unresolved.

•The United States cannot now be bound by the ABM Treaty without the advice and consent of the Senate. Because the ABM Treaty did not automatically survive the Soviet Union's collapse, it cannot now be revived without the advice and consent of the United States Senate. Because of the ABM Treaty's unique purpose and assumptions, extensive negotiations with the Soviet Union's successor states would have to be undertaken, and the original treaty substantially modified, before the original bargain obtained by the United States in 1972 could be revived. The amendments in this Treaty, and particularly any new treaty's character as a multilateral (as opposed to a bilateral) instrument, would represent changes so fundamental that they can be effected only with the advice and consent of the Senate under the Constitution's treaty-making power.

Conclusion

When the Soviet Union dissolved in 1991, the ABM Treaty became impossible to perform in accordance with its original

provisions. Because of the unique terms and conditions of the ABM Treaty, and the underlying assumptions of the parties, none of the states that emerged from the Soviet Union, either alone or with others, could carry out the totality of the Soviet Union's obligations under the ABM Treaty. Consequently, the obligations of the United States under the Treaty were discharged at the time the Soviet Union disappeared. Although a number of the former Soviet republics have indicated that they are prepared to undertake the Soviet Union's role in the ABM Treaty regime, this willingness alone is insufficient to bind the United States. Transforming the ABM Treaty from a bilateral accord, applicable to the entire Soviet territory, into a multilateral convention, applicable only to a portion of the former Soviet territory, and redrafting in the process a number of key substantive Treaty provisions fundamentally alters the bargain originally struck by the United States and the Soviet Union in 1972. The President cannot, of his own authority, accomplish these results.

Accordingly, the United States can again be bound to the ABM Treaty only if two-thirds of the Senate agrees to the revisions required by the transformation of the ABM Treaty, and the President then chooses to ratify them.

The Federalist Society's 1998 NATIONAL LAWYERS CONVENTION

Thursday, November 12 through Saturday, November 14
The Mayflower Hotel
Washington, D.C.

featuring a general session on

"Law's Future: Is Modern Technology Pressing The Limits Of Traditional Legal Ideas?"

International & National Security Law Practice Group Breakout Session includes two panels:

"Time for a Change? Pro-Competitive Privatization of the Intergovernment Satellite Organization"

"Critical Infrastructure Protection"

Thursday, November 12
Practice Group Breakout Sessions
Practice Group Membership Meetings
Practice Group Cocktail Receptions

Friday, November 13
Practice Group Breakout Sessions Continue
Practice Group Membership Meetings
Convention General Session Begins
Twelfth Annual Lawyers Banquet

Saturday, November 14
Leadership Meetings
General Session Continues
1998 Convention Luncheon
Closing Reception

Watch For Registration Materials In Early September.

International and National Security Law Property Rights Executive Committee

Mr. Edwin Williamson
Chairman
Mr. Theodore Cooperstein
Vice Chairman, Publications
Professor Robert N. Davis
Vice Chairman, Programs
Mr. Nicolas Gutierrez
Vice Chairman, Membership
Mr. Ed Hearst
Vice Chairman, Committee Oversight
Mr. Paul Schott Stevens
Vice Chairman, Bar Activities
Hon. Carol Crawford
Chairman, Trade & Investment Subcommittee
Professor John Norton Moore
Chairman, International Organizations Subcommittee
Mr. Grover Joseph Rees
Chairman, Human Rights & Immigration Subcommittee
Professor Michael Scharf
Chairman, International Tribunals Subcommittee
Professor Robert Turner
Chairman, National Security Subcommittee
Professor Michael Young
Chairman, Trade & Investment Subcommittee

Views expressed in signed articles are those of the author and do not necessarily reflect those of the Federalist Society or its Practice Groups.
The E.L. Wiegand Practice Groups have been made possible by a generous grant from the E.L. Wiegand Foundation, Reno, Nevada.

The Federalist Society for Law and Public Policy Studies
1015 18th Street, N.W., Suite 425
Washington, D.C. 20036
(202) 822-8138
fedsoc@radix.net

J. MADISON

The Federalist Society for Law and Public Policy Studies
1015 18th Street, N.W., Suite 425
Washington, D.C. 20036

NONPROFIT ORG.
U.S. POSTAGE
PAID
WASHINGTON, DC
PERMIT NO. 5637