ADDITIONAL STATEMENTS

OBJECTION TO NOMINATIONS TO VARIOUS AMBASSADORIAL POSTS

● Mr. GRASSLEY. Mr. President, it is my intention to object to the Senate proceeding to the consideration of Senate Executive Calendar Nos. 756 through 766, Nominations to various Ambassadorial posts. I request that a hold be put on these nominations.

A vacancy has existed since March 31, 1995 on the Board of the Farm Credit Administration. For over a year the White House has had the name of Ann Jorgensen to fill that Republican vacancy. All background work with regard to the nomination has been completed. All that needs to be done is for her name to be submitted to the Senate for confirmation.

I have repeatedly contacted the White House about this nomination and, to date, have not had the courtesy of a reply. The FCA has oversight responsibilities for the farm credit system, the backbone of agricultural finance. It is important for the smooth functioning of the FCS that the FCA have a full complement on its board.

It is my intention to maintain this objection until the White House has disposed of this nomination.●

LEAKING UNDERGROUND STORAGE TANKS

● Mr. SMITH. Mr. President, earlier this week, the House passed H.R. 3391, a bill to amend the Leaking Underground Storage Tank Program.

Given the press of time, the Senate will not be able to address and resolve several potential problems in the legislation before the end of this session. I am sorry this is the case. However, I wanted to call this bill to the attention of my colleagues and point out that the issues raised by H.R. 3391 are serious and deserve the attention of the Senate Subcommittee on Superfund, Waste Control and Risk Assessment, that I chair.

Leaking underground storage tanks have been a major source of groundwater contamination over a number of decades. Frequently, underground tanks that held petroleum products or highly toxic chemicals have eroded with time. These tanks have leaked their contents into the soil, which then washed into aquifers supplying drinking water. This problem is particularly acute in rural areas where a large proportion of the population is dependent on groundwater as their drinking water source.

To curtail the impact of leaking underground storage tanks on the environment and the health of those dependent on groundwater, Congress established the Underground Tank Program in 1986. Significant elements of this program included the establishment of national underground storage tank standards which come into full force in 1998; the establishment of State underground storage tank programs for compliance with and enforcement of the national standards; and the establishment of an underground storage tank trust fund to assist the State programs.

In many ways, the underground tank program provides us a model for cooperative federalism in an environmental cleanup program. There are many lessons to be learned and applied from this cleanup program to other programs like Superfund. Similar to the Superfund Program, however, the underground storage tank program is a discretionary spending program. Therefore, in spite of a dedicated trust fund, it has a significant problem.

The problem, Mr. President, is that after a decade of collecting 1/10th of a cent tax on every gallon of gas sold, nearly $1 billion just sits in the trust fund. I believe that this money should be at work in the States helping to clean up leaking underground storage tanks, and I intend to have my subcommittee staff look further into this issue when the Senate reconvenes next year.●

SURVEYING THE STRATEGIC LANDSCAPE

● Mr. NUNN. Mr. President, the post-cold war era has been in existence for nearly 7 years. Like the period that followed the end of the Second World War, the years since the collapse of the Soviet Union required our Nation to think anew about our security. It has been a time of reorientation and uncertainty as we take stock of our situation and decide on a future course of action. We can no longer, however, afford to continue in a holding pattern that lacks a clear long-term national security strategy. We must put forth the contours of a strategic vision that will guide us through the post-cold war period and that will define and safeguard our vital interests.

THE ROAD AHEAD

The strategic landscape of the post-cold war era includes certain familiar features. One such feature is the resurgence of deeply rooted national, ethnic, and regional rivalries which were unfrozen by the end of the cold war. Amidst this background are other familiar landmarks. The United States stands as the world's lone superpower but due to their economic strength or vast potential, the other great powers, Russia, China, Japan and Europe, also remain in a class by themselves. Great power politics did not end with the cold war. In fact, the international relations of tomorrow may in some ways look more like the 19th century balance of power system than the cold war system that was dominated by two superpowers. We can hope but we should not assume that the semichaotic nature of the post-cold war period we now inhabit will soon transition to a more stable world order. In other words, this may be it.

The end of the cold war brought an easing of the most ominous threat to our security—a Soviet nuclear missile attack on the United States. We are no longer compelled to contain Soviet aggression on a global scale. That struggle absorbed untold national resources; victory came at no small price in terms of blood and treasure. Without question, freedom is in greater supply around the world today thanks to the United States and our allies. The overall prospect for our security has improved. However, while the character of the threats to our security have been dramatically transformed, war and interstate conflict are not obsolete. The means of conflict may have changed, but the sources of human conflict and cruelty remain.

We must, therefore, adapt our security posture to a world in which power, in all its forms, is far more dispersed than it was during the cold war. Technology is also more dispersed, raising the risk that countries or groups hostile to our Nation can more easily acquire the means to harm American interests. It was with a profound sense of irony that those who have devoted so much of their efforts to defeating communism came to the realization that the long-awaited collapse of the Soviet empire—and the easing of the nuclear confrontation between Washington and Moscow that was then possible—actually carried with it a new proliferation threat. The possible leakage of nuclear weapons and materials from the former Soviet Union compound the already complex proliferation threat during a time of rapid change and instability at cold war's end.

We can not afford to wait until we have a clearer picture of the future before taking action. Some of the defining features of the strategic landscape are already clear enough.

First and foremost we need to build consensus in support of a common understanding of America's national interests. During the cold war, there were disagreements about tactics, but the basic sense of mission was clear. This is no longer the case. Liberated from the burden of leading the free world against communism, public interest in foreign affairs has diminished, and consensus about foreign policy has evaporated. Nowhere is the lack of consensus more apparent than in the Congress. As we approach the millennium, we must begin to rebuild consensus with a focused discussion of our fundamental interests.

DEFINING OUR NATIONAL INTERESTS AFTER THE COLD WAR

What are America's vital interests? A bipartisan commission, of which I was a member, recently issued a report brings needed clarity to the discussion of our national interests. The report, America's National Interests, distinguished between vital, extremely important, important, and secondary interests. These distinction are essential to the task of establishing national priorities and building public support for foreign and defense policy. And despite the common use of the term ''vital interests,'' to describe everything from

soup to nuts, the report defines truly vital interests only those conditions that are strictly necessary to safeguard and enhance the well-being of Americans in a free and secure nation.

It should come as no surprise that preventing and deterring the threat of nuclear, biological and chemical weapons attacks on the United States is at the top of the list of vital interests. According to the report, other vital interests are to prevent the emergence of a hostile hegemon in Europe or Asia; to prevent the emergence of a hostile major power on U.S. borders or in control of the seas; to prevent the catastrophic collapse of major global systems (trade, financial markets, energy supplies, environment; and to ensure the survival of U.S. allies.

Other objectives, such as preventing the use of nuclear, chemical, or biological weapons outside our borders or countering proliferation are extremely important, but not vital interests. Similarly, combating terrorism and avoiding major conflicts in important geographic regions are extremely important, but do not directly threaten the American way of life. This hierarchy of interests does not diminish the desirability of other objectives, such as promoting democracy, human rights and open markets. It is in no way a betrayal of our values to acknowledge that our survival takes precedence over our hopes for a better world to come. But we shall have no peace, no prosperity, nor the ability to help others if our own security is threatened by successful attacks on our vital interests. In our complex post cold war world, we must begin to build a national consensus around the bedrock requirements of our security.

PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

The spread of weapons of mass destruction still clouds our security outlook. Possession of nuclear, chemical, or biological weapons by rogue nations or terrorist groups could pose a clear and present danger to our society. U.S. leadership will continue to be the driving force for maintaining norms against either acquisition or use of weapons of mass destruction. The Aspen Strategy Group, which I co-chair along with Ken Dam, recently examined the post-cold war threats posed by WMD proliferation, and found that some significant progress has been made. The Aspen group found:

Important progress has been achieved in restraining—and even rolling back—nuclear proliferation. The nuclear Nonproliferation Treaty has been extended indefinitely. The nuclear weapons formerly controlled by Ukraine, Belarus and Kasakhstan have been consolidated in Russian hands. South Africa has voluntarily dismantled its nuclear arsenal. Brazil and Argentina terminated their nuclear efforts. Only India, Israel and Pakistan are holdouts on the Comprehensive Test Ban Treaty.

While treaties and institutions are only one part of our nonproliferation efforts, they are important tools which can provide a legal and moral framework for practical mechanisms to deter and detect violations of international treaty commitments. The denuclearization of the former Soviet States other than Russia, the U.N. program to eliminate Iraq's weapons of mass destruction, and efforts to freeze and dismantle North Korea's nuclear weapons program would have been vastly more difficult without the international consensus codified in the Non-Proliferation Treaty [NPT]. The Chemical Weapons Convention, while no panacea, can add a valuable barrier against the diversion of commercial chemicals to make weapons. Our security directly benefits from stronger safeguards on nuclear and chemical materials and from robust enforcement of those treaties.

In addition to the direct threat that these weapons pose to our homeland, our abilities to project military force and to forge coalitions as was assembled in the gulf war could be seriously harmed by the possession of nuclear, chemical, or biological weapons by regional adversaries. Thus, our counter proliferation efforts are another important aspect of our overall nonproliferation policy.

Much of our previous efforts to control the spread of these weapons also benefitted from the ability to deny access to the technology and materials required to make them. The effectiveness of those controls has eroded due to expanding commerce in technologies that can contribute to strategic weapons production and due to increasingly porous and unguarded borders. The materials and know-how for weapons of mass destruction are more available than ever to the highest bidder.

A widening circle of States, non-state actors, and ideologically motivated groups may increasingly have the resources and capabilities to acquire the technology and materials necessary to create weapons of mass destruction. Such groups may not need to wield battlefield-ready military weapons to wreak mass destruction—crude bombs and low-tech delivery systems may suffice. Our new strategy must assume that proliferation, like war, is not a relic of the cold war headed for the dustbin of history.

TERRORISM, FANATICISM & LETHAL MATERIALS

Unfortunately, these weapons of unthinkable destructive power already appear within the grasp of individuals and groups willing to do the unthinkable. While terrorism and fanaticism are hardly new, the medium of the terrorists' perverse message is expanding as lethal materials and technology become more readily available. The Unabomber demonstrated the terror one man can inspire, Oklahoma City, allegedly, illustrated the damage two can do, the World Trade Center showed the power of a small, well-organized group and the bombing of an American base in Saudi Arabia drove home the point that terrorists probe for vulnerabilities abroad and at home. Across the world, the Aum Shinrikyo provided a chilling precedent of a doomsday cult viewing nuclear, chemical and biological weapons as their ticket to paradise.

As a nation we have just begun to come to terms with the full scope of the terrorism threat. For many years, terrorists were mainly interested in making a political statement or drawing attention to a cause through discreet acts of violence such as an assassination, a taking of a hostage or some violent event of limited impact. These criminals were conscious of public relations and even viewed certain acts—such as use of chemical and biological weapons—as taboo. The 1990's, however, have seen terrorists acts that appear intended to create casualties of the highest order. These enemies are too often zealots filled with hate for civil society, and who believe their conduct is justified or divinely inspired. Despite the vivid memories of Oklahoma City and the World Trade Center, I am not sure Americans truly comprehend the devastating effect the use a weapon of mass destruction would have on a civilian population at home.

The possibility of terrorist groups gaining access to former Soviet nuclear materials or know-how, and using them to attack the United States is not merely the stuff of paperback thrillers. A report released last summer by a Center for Strategic and International Studies [CSIS] study group on nuclear smuggling concluded that the risk is no hoax. The Director of Central Intelligence at a 1996 hearing expressed his view on the risk of chemical and biological terrorism that ''we have been lucky so far.'' Mr. President, I do not believe we should base our security on luck. It was a little-noticed fact that the judge in the World Trade Center case stated at the defendant's sentencing hearing that he believed the terrorists attempted to augment the blast with the deadly nerve agent, cyanide. Incidents like these have heightened awareness to this threat. We have begun to take some steps required to meet the challenge of terrorism, such as the domestic preparedness provisions of the Nunn-Lugar-Domenici legislation included in the fiscal year 1997 Defense Authorization Act. We now have a very important foundation for this challenge. But I depart the Senate with a sense that this mission is just beginning,

These are the known dangers that are now coming into focus. Unfortunately, we are a nation of soft targets. An effective response is possible, but it requires a willingness to think anew about our security and about the way our Government and our military are organized to defense against the threats of today. We should not assume that the bureaucratic structures of our foreign policy and national security apparatus, nor the force postures that were successful for waging the cold war, are the right ones for the threats we will face in the future.

THE NEW CHALLENGE: SECURITY IN CYBERSPACE

The information age has brought us unimaginable efficiency and productivity, in effect shrinking time and space. In military affairs the power of computers and networks have helped make our armed forces the most powerful in the history of the world. Our forces are able to achieve battlefield dominance through use of information systems that receive, collate, and analyze data in real time. Elsewhere in Government and in the private sector every aspect of our society is realizing the great advantages offered by the computer. Key components of our Nation's infrastructure—government, financial, transportation, power, communication—are becoming increasingly dependent upon information systems and networks. Every day new industries and services are going on-line. This process is fueled by advancing technologies that enhance the capability and power of computing, while simultaneously decreasing their cost.

Yet we are only now beginning to comprehend that the same information networks that we are relying upon to run our society are vulnerable to disruption and penetration. The Defense Department estimates that their computers are probably subjected to as many as 250,000 computer attacks each year. When conducting vulnerability assessments of their own systems the Defense Department successfully hacks into its own system over 65 percent of the time. Already we have seen examples of hackers in foreign nations launching electronic info-war attacks on our Defense Department computers. Experts agree we are only detecting the least competent intruders. The loss of sensitive information is not the only result to fear. Much of our Nation's critical infrastructure could be disrupted by a hacker equipped with little more than bad intentions. Imagine the consequences of the northeast power grid being taken down—if even for only a few days—in the middle of winter. Our communications, medical, transportation, and financial infrastructures are all at risk.

Ironically, our dominance and sophistication creates weaknesses our adversaries can exploit, cheaply and with fear of little detection. In this regard, we are our own worst enemy. Most of the vulnerabilities of our information systems are based not simply upon technological defects, but human ones. Our intoxication with technological advantages has made us blind and deaf to information age vulnerabilities. If we fail to embed a culture of information security early in this revolution, we will create scenarios where info-war could become a great equalizer for our enemies.

Thus, along with the proliferation of weapons of mass destruction and terrorism, has arrived a new method to cause mass disruption. How we police the borderless world of cyberspace is a question we have not yet begun to answer.

INTELLIGENCE AND LAW ENFORCEMENT

Two essential elements of any successful national security strategy, our intelligence and law enforcement capabilities, are both in the process of adjusting to the post-cold war situation. We can not afford a lapse in either. Yet the distinction between warfare and crime is becoming less clear every day, especially when such lethal materials and expertise are being smuggled across borders, when organized crime groups are involved in smuggling everything from weapons of mass destruction, to drugs, to illegal aliens, and when terrorists maintain sophisticated international financial networks.

In light of the new realities, we face, it is imperative that our intelligence agencies work effectively with law enforcement to protect America from the threat posed by the convergence of these formerly distinct threats of proliferation, terrorism, and international organized crime. This intersection of foreign and domestic security has implications for our military and civilian institutions that share responsibilities in the rapidly changing security field. In the process of improving our defenses we must be mindful of our political traditions that separate civilian law enforcement from the military and limit government's intrusion into our lives, but these important sensitivities must not be allowed to paralyze us.

COOPERATIVE THREAT REDUCTION

Perhaps the most urgent nuclear danger of the post-cold war era stems from the potential loss of control over the nuclear assets of the former Soviet Union, which opens a potential Pandora's box of nuclear proliferation nightmare scenarios. Set free with the disintegration of the Russian empire was a vast potential supermarket of thousands of nuclear, chemical and biological weapons, materials and scientists with the know-how to create them.

Our response to that threat, the Nunn-Lugar Cooperative Threat Reduction [CTR] Program, has been aptly described by Secretary of Defense Bill Perry as defense by other means. Since it began in 1990, the CTR program has been instrumental in assuring central command and control over deployed weapons, preventing the emergence of new nuclear weapons states in Ukraine, Belarus, and Kazakstan, and locking up tons of nuclear materials to prevent it from falling into the wrong hands.

History will record the prevention of four new nuclear weapons states from emerging out of the wreckage of the Soviet empire as one of the greatest achievements of the decade, and as laying an important foundation for a post-Soviet world. Yet the CTR program is still criticized as foreign aid. Viewed in an historical context, it is useful to ask how much would we have paid during the cold war to eliminate thousands of Soviet warheads. How much is it worth to prevent countries like Iraq and North Korea, or cults like the Aum Shinrikyo, from getting hold of foreign Soviet nuclear weapons? In my view, the nearly $2 billion spent on CTR is a bargain. At the recent Aspen Strategy Group meeting on the post-cold war era, the overwhelming consensus of this group of experts was that the Nunn-Lugar programs have opened the door to solutions to a wide range of urgent security problems, some of which threaten Russia itself. The group recommended continued strong support for CTR programs.

THE BACKBONE OF THE STRATEGIC AGENDA: NATO, RUSSIA, CHINA, AND NUCLEAR ARMS CONTROL

NATO

The pivotal issue of NATO enlargement has important ramifications for America, the Atlantic Alliance, the countries of central and eastern Europe, and for Russia and the other FSU countries. The decision to move ahead in the immediate future with NATO enlargement raises several questions that need to be addressed as part of our strategic agenda. First, how will NATO expansion affect our vital interests, especially our efforts to stem the proliferation of nuclear weapons and materials from the FSU? Second, how can expansion be conducted without causing Russia to react by redeployment of tactical nuclear weapons and moving further toward a launch on warning hair trigger response. And third, how can the proposed inclusion of the Visegrad nations in NATO be accomplished without threatening the long term security of Ukraine and the Baltics?

RUSSIA AND THE FSU

With their vast territory, their diverse peoples and great military capabilities, the countries of the former Soviet Union can be either major contributors to global stability and peace or a major cause of instability and conflict. The challenge for the United States and its allies is to facilitate the former outcome.

At the Aspen Strategy Group meeting, experts identified the short, medium and long term aspects of this challenge. In the short term, maintaining controls on nuclear assets remains our top priority. There is more that needs to be done to ensure the safety and security of the nuclear materials that we know are sought by Iran and other nuclear renegades.

We must not lose sight of our medium and long term objectives. In the medium term, therefore, we must continue to craft our strategic relationship with Russia and the other FSU countries, including efforts to further reduce nuclear dangers. This effort should include arms control as well as efforts to convert Russia's massive weapons industries to peaceful purposes.

In the long term, we should encourage new thinking about national security and foreign policy in the minds of Russian and FSU leaders. Our long term strategy should, therefore, include sustained efforts to expose FSU policy makers to the logic of cooperative measures such as strategic arms

control, missile defense and the CTR programs, not just their technical implementation. The recent Aspen Strategy Group meeting discussed several proposals to deepen and expand cooperation on threat reduction, and nonproliferation by harnessing economic forces to move obsolete defense industries into productive and profitable civilian activities. Avoiding another cold war is a goal worth pursuing, where success or failure will affect our security for decades to come.

CHINA

With the world's most rapidly growing economy and one fourth of its population, China has joined the ranks of the great powers. China's military modernization and arms policies are already having repercussions throughout Asia. Yet it is an open question whether China will accept the norms and standards that are adhered to by all but a few outlaw states, or will seek revolutionary changes in the existing world order. As important as it is for China to respect international standards for human rights and trade, the future strategic agenda—including nonproliferation, arms control, and regional stability—depends on China's adherence to existing agreements and regimes. Our strategic agenda must not overlook China's ability to make or break the norms and institutions that define the international system.

A major obstacle to China's full incorporation into the international community is the incompleteness of the rule of law in China. With respect to human rights and arms proliferation, a fundamental aspect of our approach should be to encourage China to strengthen its rule of law. This approach would include our concern for human rights, but would also be provide a broader appeal to China's self-interest, because a nation governed by law is more predictable, more attractive to economic investment, and more likely to abide by its commitments.

NUCLEAR WEAPONS AND ARMS CONTROL

The end of the cold war did not render deterrence obsolete. Iraq's nonuse of its chemical and biological warheads during the Gulf War stands as an important reminder that even rogue states are not immune to the logic of overwhelming retaliation. The credibility of our deterrent forces must remain unquestioned. Yet, the period between the end of the cold war and early decades of the next century offers the United States a unique opportunity. Though the transformation of Russia and emergence of China as a global power could pose new security challenges by about 2010, in the interim, the United States faces no peer competitor and is unrivaled in conventional military superiority. I say this having devoted much of my career to the betterment of our Armed Forces. Our current situation offers a window of opportunity to build our qualitative edge in conventional weapons technology to strengthen deterrence for the future.

At the same time, we can continue to reduce the role of nuclear weapons in our defense strategy—if such reductions are matched by the other nuclear powers. If reductions in our own arsenal can persuade others to make comparable cuts, or not develop nuclear weapons at all, we come out ahead. This is the logic of the Comprehensive Test Ban Treaty; the benefits of freezing the nuclear status quo outweigh the costs and leave us in a position of relative advantage.

Similarly, our promising development of needed limited missile defenses should proceed with an awareness of the unintended consequences that could result if Russia and China respond by retaining, redeploying and building enough warheads and missiles to overwhelm any conceivable antimissile system, as they have vowed to do. I have argued for years that it is possible to advance as rapidly as possible with missile defenses in a way that does not result in more nuclear weapons being pointed at us. Putting aside the issue of cost for a moment, a policy that leaves us facing more of the threat we were trying to defend against in the first place is the essence of bad strategy. The error is especially shortsighted if it is possible—as it is in this case—to have missile defense and reduce the numbers of missiles pointed at us. In my view, this can be accomplished by cooperation with Russia on limited defense for both nations and modest amendments to the ABM Treaty.

I do not have any illusions about arms control; treaties are not cost-free and do not necessarily address the root causes of conflict. Some people may, as the critics warn, be lulled into a false sense of security by arms control. But I believe my record shows that I have not been one of them. Our Armed Forces today are second to none and will remain so for the foreseeable future. But to the critics of arms control I ask: What is the better alternative to agreements such as START II, which would eliminate the most destabilizing strategic weapons of all—Russia's land-based MIRVed missiles? Would we be better off without Cooperative Threat Reduction programs that keep nuclear weapons out of the hands of terrorists? Sound arms control agreements can and do enhance our security.

These are critical determinants of our national security for the coming era: proliferation, terrorism, and relations among the great powers. Of course, many other important issues contribute to the overall security outlook—our bilateral relationships with key allies, regional developments in Asia and the Middle East, maintaining our technological lead, and various global issues such as trade, population, immigration, environment, human rights, economic development and the march of democracy. But, as the report on America's National Interests and the Aspen Strategy Group both remind us we must give priority to those core issues that are truly vital to our citizens.

The material follows:

RECOMMENDATIONS OF THE MINORITY STAFF OF THE U.S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS—HEARINGS ON SECURITY IN CYBERSPACE, JUNE 5, 1996

The need to establish a comprehensive plan within which to address the vulnerabilities of our National Information Infrastructure (NII) is paramount. Whether through a White House-led Task Force or some similar mechanism, the interdisciplinary nature of this threat requires a government-wide response that also addresses the exposure of the private sector.

The U.S. must formulate national policy to promote the security of its information infrastructure.

Presently, agencies are greatly limited by pre-existing missions and jurisdictional assignments. Unfortunately, the threat ignores national boundaries and often remains a mystery until it is fully investigated. Based upon the multidimensional nature of the threat posed to our information infrastructure, there exists a need to establish a free standing entity that can conduct operational responses to computer attacks, and task different agencies within our government.

The Staff recommends the creation of a National Information Infrastructure Threat Center that will include representatives from the law enforcement, intelligence and the Defense communities, as well as liaison with the private sector. This center should have ''real time'' 24 hour operational capabilities as well as serve as a clearing house for intrusion reports.

No intelligence, counter-intelligence or law enforcement agency has yet produced an NII threat assessment. More importantly, the intelligence community is having difficulty collecting the data necessary to even prepare such an estimate. Collection of data must become a high priority within the intelligence community.

The Staff recommends that the Director of Central Intelligence complete an NII threat estimate. The estimate should have an unclassified version that can be made available to private industry.

The uneven response in the international community to the threat posed to information infrastructures has created difficulties enforcing anti-intrusion legislation. Only a handful of countries presently have meaningful computer crime investigative capability, and the absence of uniformity has given would-be attackers refuge from detection or prosecution.

The Staff recommends that the U.S. promote the creation of an international computer crime bureau with emergency response capability. This Bureau may be assigned to Interpol and would provide education and awareness training to foreign law enforcement agencies in order to promote the creation of dedicated computer crime units or similar capability as well as uniform investigative and computer forensic practices. This Bureau would also have operational response, like a CERT, in support of computer crime incidents. The Bureau would also collect data on vulnerabilities and disseminate countermeasures as well as serve as an international clearinghouse for intrusion incidents.

Our government must foster a security culture that appreciates the vulnerabilities of our National Information Infrastructure (NII). We need to maintain a better pool of security professionals and, generally, improve the security consciousness of our users and our managers. There are several specialties in the computer career field for government employees including computer operators, computer technicians, computer programmers and computer analysis. There is

no specialty in the computer career fields for network administrators, computer security personnel, nor in the criminal investigative career field for computer crime investigators.

In order to ensure that computer security positions are filled with personnel that possess the requisite experience and training the Staff recommends the creation of a Government Computer Security Specialist Career Field that will include potential for career progression and incorporate specialized computer security training.

In order to promote a stable pool of information security managers within the U.S. government, the Staff recommends the creation of a Government Computer Systems Administrator Career Field that will include potential for career progression and incorporate specialized computer security training.

In order to promote and improve our government's computer crime investigative potential, the Staff recommends the creation of a Government Computer Crime Investigators Career Field that will include the potential for career progression and specialized computer crime investigation training.

Vulnerability testing and assessment of government and government interest computer systems is the best method of enhancing awareness of the vulnerabilities of our information infrastructure. Presently, only the Defense Department has an aggressive vulnerability program.

The Staff recommends that the federal government promote regular vulnerability assessments, or ''red teaming,'' of government agencies, especially agencies outside of the Department of Defense. The Staff further recommends that an agency be designated to perform such vulnerability assessments in the same manner that the Defense Information Systems Agency (DISA) perform such assessments for the armed services.

One of the most significant voids in computer security is the lack of reporting of attempted and even successful penetrations of government systems as well as other systems of national interest. Mandating the reporting of intrusions in government systems will foster a greater security culture with the NII. Further, it is important to give private industry a mechanism within which it can report intrusions without fear of inciting customer insecurity.

The Staff recommends that the U.S. government mandate the reporting of intrusions and attempted intrusions in all government and government interest systems. The Staff further recommends that federal agencies develop protocols and procedures for reporting computer intrusions, and subsequent referral of same to proper criminal or other appropriate agencies like the proposed National Information Infrastructure Threat Center.

The Staff further recommends that the federal government encourage private industry and the private sector to report intrusions into private information systems. The Staff would further recommend that the government promote private industry reporting through creation of anonymous clearinghouses or similar methods.

Logon warning banners that advise users of government computers that there is no expectation of privacy, though recommended by the Department of Justice, are not mandatory on government computer networks. The logon banners put users on notice that they have no reasonable expectation of privacy on government systems and the use of the system constitutes consent to monitoring. Presently, when intrusions occur on government systems, lack of such a logon banner hampers investigative efforts and response.

The Staff recommends logon warning banners become mandatory for all government and government interest systems.●

NATIONAL SECURITY AND THE INFORMATION AGE

● Mr. NUNN. Mr. President, technology has long been an instrument of power and change. From the invention of the printing press to the advent of the industrial revolution to the development of nuclear weapons, technological advances have profoundly altered our society and changed the course of our history. Today, we find ourselves in the midst of one of the most far-reaching technological developments of all—the information age.

OUR INFORMATION INFRASTRUCTURE

Advances in computing and networking have affected every aspect of our society—from civilian government and the military, to public utilities, health care, communications, transportation, and financial systems. Computer networks and the ever-increasing power of the information systems they connect, are compressing time and space, creating vast efficiencies in the delivery of goods and services. Government is more productive and connected, business is more robust, versatile, and cost-effective, and individuals now have access to large caches of information and each other.

The rush to connect seems to reach new and unimaginable heights each day with the announcement of a more powerful computer or some new innovation. Just 5 years ago the number of users on the Internet totaled 2 to 3 million. Today, over 55 million log-on worldwide and the number grows. Computer links that stretch around the world transcend national and regional boundaries: Beijing and Baltimore are within a keystroke of each other. Equally impressive is the expanding technology that supports this revolution. Today's home computers are literally hundreds of times more powerful and versatile than the mainframe systems that NASA used to send a man to the moon. Connectivity between networks has similarly increased: In 1980, most modems required nearly 3 hours to transmit a 200 page book; today's commercially available modems can transmit the same book in 0.06 of a second.

Along with the great promise of the information age, however, has arrived new dependencies. Our banking and financial systems, though more efficient, rely almost totally upon daily electronic fund transfers in excess of $1 trillion. Our transportation system—air, rail, and road—is able to receive and analyze vast amounts of data but must also be certain of the accuracy of the information directing its critical operations. Energy and communication networks are more responsive but are similarly reliant upon the redundancy of electronic networks. And the information revolution in military affairs, though establishing the unquestionable preeminence of our force structure, has fostered a dependency upon 2 million interconnected DOD computers.

How would we get by if the information infrastructure of any of these critical systems proved unreliable?

As we rush to connect to the information superhighway, are we sufficiently addressing the potential weaknesses created by our growing dependency on computers and networks? To what extent can the vital services supported by our information infrastructure be disrupted? How can we be assured that the information stored—especially data related to our national security—retains its availability, reliability, and confidentiality?

THE THREAT FROM CYBERSPACE

Ironically, the same technological advances that have brought us the advantages of the information age, have also given us the tools to disrupt and exploit it. In the early 1980's only the very technically competent had the expertise to break into computer systems. Not only were there fewer hackers, there were not as many targets.

Today, the situation is reversed: while the hacker tools are becoming more sophisticated, they are also becoming more available and user-friendly, requiring little expertise. Logic bombs, viruses, password sniffers and other tools that can disrupt and destroy computer networks, are now widely available on the Internet. For instance, last year ''point and click'' computer security program—Security Administrator Tool for Analyzing Networks or ''SATAN''—was disseminated on the Internet. Now this computer program, which provides its user with automated intrusion capability into many networks, is available to millions.

In hearings of the Permanent Subcommittee on Investigations earlier this year experts demonstrated how many of our critical computer networks were neither secure nor confidential. A report issued this year by the General Accounting Office estimated that the unclassified but sensitive networks at the Defense Department are likely experiencing as many as 250,000 computer attacks per year. Vulnerability studies of DOD networks suggest that these network attacks could be successful more than 65 percent of the time. Over 90 percent of all Department of Defense voice and data traffic transits these networks, and the data includes sensitive research data and valuable intelligence information. Furthermore, these systems support critical defense missions related to troop movement and operational plans, procurement, and weapons systems maintenance.

Statistics from the civilian area are equally troubling. A recent FBI survey that included corporations, financial institutions, universities, and health care institutions revealed that 42 percent of those responding experienced