

Originally Processed With FOIA(s):
2005-0336-F

FOIA Number:
2005-0336-F

FOIA MARKER

**This is not a textual record. This is used as an
administrative marker by the George Bush Presidential
Library Staff.**

Record Group/Collection: George H.W. Bush Presidential Records
Collection/Office of Origin: Science and Technology Policy, Office of (OSTP)
Series: O'Neil, John F., Files
Subseries: Reports and Publications Files

OA/ID Number: 62101
Folder ID Number: 62101-002

Folder Title:
Remarks by Michelle van Cleave

Stack:	Row:	Section:	Shelf:	Position:
	0	0	0	0

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
01. Remarks	Economics and Trade and the Intelligence Community (12 pp.)	4/21/90	(b)(1)	

Collection:

Record Group: Bush Presidential Records
Office: Science and Technology Policy, Office of (OSTP)
Series: O'Neil, John F., Files
Subseries: Reports and Publications Files
WHORM Cat.:
File Location: Remarks by Michelle van Cleave

Date Closed: 6/1/2010	OA/ID Number: 62101-002
FOIA/SYS Case #: 2005-0336-F	Appeal Case #:
Re-review Case #:	Appeal Disposition:
P-2/P-5 Review Case #:	Disposition Date:
AR Case #:	MR Case #:
AR Disposition:	MR Disposition:
AR Disposition Date:	MR Disposition Date:

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P-1 National Security Classified Information [(a)(1) of the PRA]
P-2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P-3 Release would violate a Federal statute [(a)(3) of the PRA]
P-4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P-5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
P-6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Removed as a personal record misfile.

Freedom of Information Act - [5 U.S.C. 552(b)]

(b)(1) National security classified information [(b)(1) of the FOIA]
(b)(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
(b)(3) Release would violate a Federal statute [(b)(3) of the FOIA]
(b)(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
(b)(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
(b)(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
(b)(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
(b)(9) Release would disclose geological or geophysical information

*2 min/double
spaced page*

MICHELLE VAN CLEAVE
REMARKS PREPARED FOR DELIVERY
19 MARCH 1990
AMERICAN DEFENSE PREPAREDNESS ASSOCIATION
CONFERENCE ON SDI
GLOBAL STABILITY AND DETERRENCE

Over the past quarter century, we have witnessed more advances in science and technology and as a result more changes in day-to-day life than during any other 25-year period in history. Our engineering skills are changing the world profoundly, in ways and with a speed that is nothing short of amazing.

We can see this in our everyday lives. Personal computers. Camcorders. CD players. Answering machines. Beepers -- where would we be without beepers? Automatic Teller Machines: just push a button and money pops out. Faxing, a newly invented word, overnight became the default option in business communications. Cellular telephones have give new meaning to the idea of taking business on the road. And VCRs! VCRs are wonderful machines, invented to keep you from ever missing another installment of "L.A. Law."

In modern America, technology has become pervasive and personal. Increasingly we look to technology to provide the answers to our wants and needs. The belief that technology will be able to provide these answers is based on repeated experience of seeing what technology in fact can do.

Yet with all of our technological prowess, the United States has no operational means of defending against a strategic nuclear attack. Just how can that be? Well, everyone in this room is familiar with the long and involved reasons why that is true. But on its face, that strategic technological inability strikes me as extraordinary.

The interaction between public policy on the one hand and science and technology on the other is the focus of the work of the White House Office of Science and Technology Policy. Allan Bromley, Assistant to the President for Science and Technology Policy, likes to explain the responsibilities of OSTP as twofold:

1. Science and technology for policy: the need to provide the President with accurate, objective information on S&T as it affects public policy.
2. Policy for science and technology: the political or policy decisions that affect the health and productivity of science and technology in America.

As potentially the single largest research endeavor ever undertaken by the federal government, the Strategic Defense Initiative may be viewed from these two perspectives. What can the research and development efforts that comprise SDI contribute to U.S. deterrent strategy (S&T for public policy), and what policies are required to sustain and exploit SDI programs (policy for S&T)?

Science and Technology for Policy

A decade ago, President Reagan came to office warning about the growing window of strategic vulnerability. Specifically he was pointing out the danger inherent in the vulnerability of U.S. land-based ICBMs and strategic bomber bases to the increasingly accurate Soviet rocket forces.

But I believe that in addition to well founded concerns over the survivability of U.S. nuclear deterrent forces was the broader and more disturbing reality of the total vulnerability of our cities, our people, and our allies. Out of these concerns -- some strategic, some moral -- emerged the strategic defense initiative. It was a challenge to the American science and technology community to find a way to enhance deterrence, to be sure; but on a more basic, commonsense level it was a challenge to find a way to protect us.

Those of us who worry about deterrent strategy as a part of our professional lives will quickly observe that this is a distinction without a difference. Enhancing deterrence means ensuring that no aggressor will believe he can successfully attack. To deter war is to protect lives.

Yet at its inception, SDI was not understood or specifically structured to make incremental contributions to deterrence. Originally there were no clearly defined serial objectives short of a multi-layered, fully robust defense. Since then, we have made significant progress. The publication of the JCS Phase I criteria lent an important nearer-term focus for strategic defense programs. And the work underway pursuant to NSD-14 should make the near-term deterrent value of SDI even clearer.

But I would note that even today, it is curiously difficult to find government-sanctioned critical analyses of the integration of offense and defense into an overall deterrent strategy.

Perhaps in part because we have been so slow to highlight the incremental contributions SDI can make to deterrence, the critics of the program have erected the straw man of a perfect shield as a way to ridicule SDI -- with some measure of success.

Since the program's inception in 1983, we have heard a lot of nonsense disguised as technical commentary about SDI. But internally, as this audience is well aware, SDI has been

exhaustively reviewed -- the DSB, WHSC, and recently the JASONS - with consistent reports of steady progress -- no technological showstoppers -- and fully meriting both the investments made to date and continued support for the future.

The SDI program now has completed over 400 tests and experiments, including the miniaturization of component technologies and a vast reduction in unit costs, with a record number of major tests planned in 1991 (about 16; cf 11 in 1990 and 4 in 1989). It will not come as a surprise to this audience that the future pace of SDI's progress is limited far less by technology than by dollars.

Ballistic missile defense requires sensors to observe the attack, interceptors to destroy the ballistic missiles and warheads, and battle management system elements to efficiently and effectively operate the system architecture. The level of effort required to validate the needed technology is not the same for all concepts. And different technologies are maturing at different rates, as is to be expected. Some problems are readily solved, others are more difficult. But not all elements need be brought on line at the same time. Deployment schedules can be tailored to take the variables into account, consistent with the contribution each strategic defense component makes to deterrence and to other defense objectives -- and consistent with the funding the Congress in its wisdom may choose to provide.

President Bush has directed the defense community to prepare for an initial deployment decision in 1992. And I am pleased to report that there is no technical reason to date why we should not be able to meet the President's deadline.

Policy for Science and Technology

In addition to its direct contribution to deterrence, the Strategic Defense Initiative is an excellent example of the high and largely unanticipated returns we as a nation derive from funding new research and technology initiatives. I believe your conference will include an overview of the spin-offs from SDI programs in weapons research but also in broader terms of human welfare, industrial efficiency, and economic value. To support, exploit and protect such endeavors requires sound policy for science and technology -- the second mission of the President's Science Office.

At a time of declining defense budgets and heightened international instabilities, it is especially critical that we not lose sight of our future security needs. In particular, we need to focus attention on cutting edge technologies that lend themselves to wide application, because potential adversaries are certain to be doing the same. While there have been public reports that the Soviets may be cutting their military spending this calendar year, I would note that there have been no reports of any reductions in Soviet investment in advanced weapons R&D.

And as you are well aware, Soviet strategic modernization of all three legs of the triad continues apace.

In line with this, the 1990 Defense Planning Guidance stresses the need to increase research funding and to exploit U.S. technological advantages. And it is in the nature of long-lead R&D work that if it is disrupted, time lost now cannot be recovered by future budget add-ons.

After 7 years of creative, exciting, and -- I suspect -- sometimes frustrating work, it is very clear that the technology development programs being pursued under SDI are needed to respond to new challenges and to take advantage of emerging technologies. And so long as the United States continues to rely on superior technology for deterrence, we must pursue the kinds of R&D efforts that provide such advances -- the kinds of R&D efforts epitomized by SDI.

At the same time, we must continue to protect those critical technologies against hostile exploitation.

As you may know, there is a major effort underway within the United States government to review our policy toward technology transfer controls, in large measure driven by the President's interest in finding ways to encourage the independence and democratization of Eastern Europe. At the same time, the principal mission of COCOM -- to deny adversaries access to militarily sensitive Western technologies -- remains essential.

One new policy approach that is gaining currency is the idea that we should determine what technologies are really most important, protect them very well, and let the rest go. But there is an inherent risk in following that course. Narrowing the number of secrets we have enables our adversaries to focus their acquisition efforts more efficiently. And the changing international climate that has brought us to our feet in celebration has also brought increases in hostile intelligence activity.

Judge Webster has revealed that "around the world, our stations are reporting more aggressive actions, more robust intelligence collection efforts and more efforts to recruit our embassy and our intelligence personnel than we have seen in a long time...Technology transfers is one of the big issues in the world today, and as less money is dedicated to that particular effort inside the Soviet Union, [the Soviets can be expected to apply] more and more effort ...to obtain that kind of technology through clandestine means. That's what we are experiencing."

In short, military technology competition continues with muffled intensity -- and promises to grow, as interaction between East and West expands, borders become more permeable, international business activity more pervasive, and opportunities for intelligence and technology acquisition more commonplace.

Conclusion

Today, the economic and social structure of much of the communist world has been torn apart. Some would argue that the Cold War is over, and that SDI is but a relic of that war. Those same critics point with derision to anyone who would suggest that our future depends on the United States remaining strong. They believe the joyous events in Eastern Europe belie the rationale for a strong defense.

I would argue that it is no accident that freedom is triumphing on the heels of an America renewed in strength and purpose. As Richard Pipes recently reported, President Reagan signed a classified policy document in 1982 which defined the central objective of U.S. policy toward the Soviet Union as pushing that country in the direction of internal liberalization. Central to that policy was a strong national defense.

I can think of no reason why that objective should not still be valid. The world today is in the midst of instability and change. What is needed above all is a cool head and a quiet strength to help shephard through new governments and anxious peoples struggling to enter the Twenty-first century as modern, free societies.

The cutting edge technology programs under the SDI umbrella will help ensure the continued technological superiority of the United States. And the deployment of strategic defenses can help provide the strategic stability essential to fostering a continued global movement toward freedom and peace.

MICHELLE VAN CLEAVE
ASSISTANT DIRECTOR FOR NATIONAL SECURITY AFFAIRS
WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY
REMARKS PREPARED FOR DELIVERY
INTERNATIONAL SECURITY SYSTEMS SYMPOSIUM
WASHINGTON, D.C.
OCTOBER 28, 1991

NATIONAL SECURITY AND STRATEGIC ECONOMIC INFORMATION

On the eve of the coup in Moscow, the White House released a document entitled the National Security Strategy of the United States. The preface, signed by President Bush, issues a challenge to the nation. "We must not only protect our citizens and our interests," the President says, "but help create a new world in which our fundamental values not only survive but flourish. We must work with others, but we must also be a leader."

In other words, the national security strategy of the United States requires a strong national defense and protection of our interests at home and abroad, to be sure; but equally it demands American leadership to promote and consolidate our values of liberty, individual dignity and free enterprise throughout the world.

During the next two or three days, you will be examining pressing issues of international economic and business security, some of which I want to touch upon in my remarks this morning. But it is the prerogative -- some would say the duty -- of the keynote speaker to provide a broader framework for the discussions to follow.

And so while the specifics of the symposium to follow will properly concern the protection of the nation's strategic economic information, I think we must begin by considering the historic changes we are witnessing, the pervasive importance of our values of freedom and democracy to all matters of national policy, and the vital mission of America in the century to come.

STRATEGIC VISION

In the scenes of the streets of Leningrad, in the barricades before the White House of Moscow, throughout the reborn countries of Latvia, Lithuania, and Estonia, in the many Republics now defining their own path, we have seen the triumph of the human spirit over the forces of tyranny. All the power of the Red Army and the Communist Party and the KGB ultimately proved hollow against the determination of these brave people to live free.

And yet it was not so long ago that many were arguing that stability and preservation of the status quo were our most important objectives in Europe. We were told that the Soviet Union's hold over its neighbors must not be threatened; that this was the unhappy but necessary price we had to pay for peace.

For many years, the nations of Central and Eastern Europe submitted to this fate. Czechoslovakia's President Vaclav Havel, whom we welcomed to the White House last week, explained in his essay, "The Power of the Powerless", that the communist system of control succeeded because of the consent of the governed. Not in the positive sense that you and I use those words, but the negative consent of default: Not enough people would stand up and say no.

Yet thankfully, in the final analysis, the people of Central and Eastern Europe did find the courage to say no. They found the courage to reach for the values embodied in the great documents of our liberties and political beliefs. As a result, the Berlin Wall has fallen; and now the Federalist Papers are being widely read throughout the former Soviet Union.

The courage of those who said no should cause us to reflect with some seriousness upon the values that must guide our policies. One lesson is that America's policy of peace through strength, ridiculed by some as misguided Cold War thinking, has proven as right and as great a force for good as we always believed it to be. But another lesson is that a great nation does not lead merely by reacting to threats, but rather by defining opportunities to achieve valuable goals.

LOOKING TOWARD AMERICA'S CENTURY

Today there is great hope throughout the world, as the opportunities for freedom and economic growth have never been greater. And in the aftermath of these remarkable changes, some are saying that history is over, and that no serious threats to American interests remain. Others have been accused of inventing or exaggerating threats in order to justify old jobs or new ambitions. Most people are simply confused. This is understandable, given that we are poised at a defining moment in history, when an aggressive empire has fallen and a totalitarian claim on the spirit of man has failed.

In the midst of all this uncertainty, knowing with any precision where or when threats to our security may emerge may well be an impossible task. But certainly history teaches that power and ambition, greed and false ideals bring conflict and war -- human foibles that have not gone away. The twentieth century in particular has been marked by aggression, tyrannies, and statist ideologies. As a result, this century tens of millions have died, scores of millions have fled as refugees, and hundreds of millions more have lived with suffering and oppression. Self-destructive socialist economic policies have

brought starvation, poverty, sickness and desperation. And immeasurable creativity and joy have been lost.

The future that each of us would wish for, the future that together as a nation we would work for, is a future in which these evils are held firmly in check; a future in which freedom is both a universal ideal and a universal norm. As the twentieth century draws to a close, our challenge is to exploit the opportunities ahead to ensure that history will record the next hundred years as truly America's century.

To this end, we need to identify those forces and challenges which could threaten American values. And in setting national security strategy, I believe we should measure the seriousness of these threats by the extent to which they would impede the opportunities which will be presented to advance our values in the coming American century. Against this standard, I would like to discuss some of those threats as they relate to our nation's economic strength.

THE THREATS WE WILL FACE

Throughout the Cold War, the Soviet Union was far and away the greatest threat to the United States and our allies, principally owing to its unsurpassed military arsenals, both nuclear and conventional. The other pillar of Soviet power during the Cold War was its militant intelligence gathering and active measures, which had as their target not only the political and military resources of the West, but our economic and technological strength as well.

Today there is enormous confusion and uncertainty over the future of Soviet military forces and policy. In the words of the Secretary of Defense, "The former USSR remains a nuclear superpower in the midst of a revolution -- a situation without parallel in history. The continuing existence of enormous military capabilities in a state which is in the throes of a revolution -- and the accompanying potential for violence and chaos -- present a new kind of security challenge for the United States and its allies." As with the military threat that may be posed by the successor to the central government, in like manner we are unable to define with precision the intelligence threat that might emerge from the power that is heir to those Soviet institutions.

Will the Russian Republic inherit a KGB that picks up where the Soviet KGB left off? or will changes in relations and the absence of communist party control fundamentally transform the nature of that threat? We don't know. But given that even a relatively more benign nation, if armed with 30,000 nuclear weapons, still has to be of concern to us, likewise any nation that inherits the Soviet KGB must be accorded serious attention.

And I would note that to date, we have seen no diminution of KGB or GRU activity.

Whatever happens in the former Soviet Union, the knowledge and experience represented by the KGB, and those who have learned from the KGB, are realities. The Communist regimes still ruling China, Cuba, North Korea and others remain as threatening as ever. The increasing sophistication, availability and proliferation of espionage technology (SIGINT, IMINT, ELINT, and so forth) is also a reality. So we must take into account the possibility that organized, sophisticated and aggressive hostile intelligence threats will remain with us for some time to come.

In addition to these more or less traditional threats, there are a growing number of non-traditional threats. For example, it is possible that KGB intelligence officers may even now be circulating their resumes, looking for new work outside the former USSR. There may no longer be much demand for their ideological services, but many of these officers do have finely honed skills in the collection of technological and economic information. Possible targets would not be limited to the U.S. government, but could well include other nations and the U.S. commercial sector as well. Theoretically many unemployed intelligence officers, lacking work, could reason that their future is in high tech, and attempt to sell their talents in that market.

In today's world, there is a perceived premium for high technology, particularly weapons technology, that can turn a small nation into a threat to its region, its neighbors, or indeed to the U.S. itself and the Western world.

Proliferation of the technologies for weapons of mass destruction and their delivery systems is an increasing problem for the United States. Much of this technology that has already leaked has been obtained through theft and illegal diversion. Moreover, non-proliferation regimes which seek to control formal transfer of these technologies, while necessary to slowing down proliferation, may in fact generate intensified espionage efforts in the face of legal barriers.

Finally, we are in an age where national security allies have become economic competitors -- with their own special interests in America's technology and wealth. And while the efforts of non-Communist countries and firms to access U.S. research and technology are largely legal, open and direct, they are not exclusively so.

As a consequence, when it comes to commercially valuable financial and technical information, private American firms may find themselves competing not just with other companies but against foreign governments as well. President Bush has stated, "Historically, foreign governments -- and to some extent foreign businesses -- have tried to obtain our secrets and technologies." What many may not realize is that other nations frequently share

this data with their private businesses both formally and informally -- the competitors of U.S. commerce and industry -- to give them national economic advantage.

INTELLIGENCE AND THE PRIVATE SECTOR

When we see foreign government and foreign competition spying on U.S. business and industry, it is not surprising that some are asking why can't the U.S. use our intelligence assets to support our private sector. This appeals to our sense of fairness, on one level, but there are some very difficult questions associated with such an undertaking.

When the President's nominee for Director of Central Intelligence, Robert Gates, was asked about this issue at his confirmation hearings, he confessed that

One of the problems that we've wrestled with for at least a dozen years is how to take some of this information that we gather, that in essence practically falls into our hands, and make it useful to people. And the honest answer... is that we can't find a way. We've tried for 10 years or more to find a way to get it into the hands of U.S. business and we can't find a way to do that so it does not somehow get all tangled up in the law, in advantaging one company over another.

Why is this so difficult? Apart from the obvious concerns over the protection of intelligence sources and methods, there are many serious legal questions as well, especially of the Equal Protection variety. For example, given the complex nature of the international marketplace of multinational corporations, and transnational holding companies and investors, and foreign subsidiaries, how would we define what constitutes an American company? Such a distinction would be crucial not only in identifying eligible beneficiaries of intelligence sharing, but also in defining the targets for collection. How would priorities be set among competing private sector requirements for limited intelligence resources? How would those requirements be developed and tasked fairly?

Not only do these concerns present serious legal difficulties, but they also call into question the practical benefits of any intelligence sharing regime. And on a political level, any U.S. policy to collect commercial intelligence would have adverse consequences for our intelligence and other relations with key allies.

Finally, is the collection, analysis and dissemination of intelligence to support commercial ventures a proper role for the U.S. government from an ethical point of view? If what we mean by that question is, should the U.S. be in the business of industrial espionage, the answer is clearly no. Any such undertaking would require a radical restructuring of the way our

intelligence agencies do business, new legal regimes, and a new public mandate that would be a sharp departure from the national security assignments of the past.

Frankly I am concerned that talk of a fanciful new industrial espionage mission for the CIA has simply led to more misunderstanding and confusion, and diverted attention away from what should be the central question: what is the proper role for the U.S. government in the protection of private sector vital information and technology?

TENSION BETWEEN SECRECY AND VALUES

Over the past ten years, the United States has come of age in recognizing the strategic importance of the security of our information, our technology, and the communications and computer systems which enable us to use them productively. The next ten years will challenge us to act on that knowledge. And I believe our success will be measured by how well the Government and the private sector work together to secure our nation's vital strategic information against an increasingly sophisticated, aggressive and diverse threat.

The work ongoing on the new National Industrial Security Program, under development as a joint Government-Industry initiative, is an important example of this necessary partnership so far as government contractors are concerned. And we do understand the role of the government in the protection of government information and technology. While we may not have come as far as we need to in terms of resources or energy or thinking in carrying out that role, basically we understand what needs to be done to protect U.S. government information.

But for the most part, the nature of government and private sector interaction in protecting strategic information raises important and largely unanswered questions.

In the first place, there is an inherent tension between the need for secrecy and the fundamental values of a free and open society. This distinction between the free flow of ideas and the protection of national security and proprietary information -- in the government, among contractors and the private sector -- is a difficult one. Rapid strides in scientific and technological endeavors are severely hindered by limiting the free exchange of ideas and technology. Yet such information can be used by adversaries, both military and economic, to their advantage. And of course, we're not just talking about R&D, but tremendous volumes of financial and business information and other proprietary data as well.

So how does a society, based on openness, decide that certain things must nevertheless be protected? I don't know where the balance should be drawn, but I believe that it should be possible to find a balance that respects and supports our

basic values. Within the United States we believe in the free flow of information, but we don't believe in insider trading. We rigorously protect free speech but respect in both law and values the confidentiality of privileged communications. We support robust competition but honor patents and copyrights that protect intellectual property.

In short, we do recognize important constraints on the free flow of information. Based on the rule of private property, we need to find a way to extend that kind of basic fairness to the international situation.

To do this, I believe we must start with a coherent technology and information security policy that sets forth what information we must protect and why we should do so, in a way that supports our values and especially our deeply held belief in and respect for the free exchange of ideas. Indeed, unless we address the need for secrecy and the protection of information and technology as part of an integrated, rational, and even-handed policy, our protection programs are likely to result in unfairness and inefficiency, they will not command support, and they won't work.

This is true because the elements of counterintelligence, countermeasures and security which we single out as "information security" -- just as with the security of military secrets -- do not exist in a policy vacuum with an intrinsic value apart from their ultimate purpose. Practically, they do not stand by themselves. Both intelligence and security are contingent activities. The axiom that intelligence is useful only if it leads to or helps to execute policy is likewise true of security. What the government and the private sector do in counterintelligence, countermeasures and security must be driven by our policy objectives.

To date there is no generally accepted general theory of how the elements of strategic economic and technological information should be identified, integrated and protected. They include such diverse concerns as non-proliferation of weaponry, dual-use technology transfer and export controls, and the identification of technologies critical to the nation's future security and economic well-being. Moreover the explosion of technologies to store, process and transmit information makes protecting select pieces of information extremely difficult.

Developing a comprehensive national policy for information protection will not be an easy task. It's one thing for the government to identify technologies and information critical to foreign relations, military operations, or intelligence activities, but what about those things in the private sector that are also vital to the United States, such as financial and trade secrets, commercial properties, and industrial R&D? Given that the government does not own or control this strategic information and technology, how are we to arrive at a workable national policy to protect it?

I don't know the answer to that question, so I would pose it to you. Is there a way in which the private sector could offer its views, understanding, and ideas on how the U.S. public and private sectors together can arrive at such a policy? It seems to me this will require a serious public policy debate in the private sector -- not just narrowly focused "interest group" politics -- about the place of an information and technology security policy in American society, and the proper roles of government and commercial firms in supporting it.

GOVERNMENT-INDUSTRY PARTNERSHIP

Let me be clear. Under no circumstances would I advocate any kind of regulatory government activity in protecting private sector information, and I suspect I would get rather solid agreement on that point. But I do see the potential for a sort of shared Operations Security or OPSEC responsibility in a government-industry partnership, in which the government would provide threat and vulnerability data. It would be up to the private sector to determine their level of risk -- because they know the value of their strategic information, and they know their business -- and to apply the security and countermeasures required.

That may seem pretty straightforward, but I do not want to gloss over how difficult it can be in practice to assess what is strategic information and what is not, especially when it comes to information outside the bounds of what is traditionally defined as national security information. The government is currently struggling with these concepts, in such areas as export controls and critical technologies studies.

What is the right mechanism to identify the most vital information and technology assets of the private sector? It seems to me that defining which information is strategically vital in the commercial world is a duty and business function of the private sector. The analysis would vary from company to company, and would be up to each company to do or obtain for itself. So in the identification of what is truly valuable -- the first step in the OPSEC methodology -- the Government would have little role to play.

Now many business people might say, I think I know which of our corporate information is vital or sensitive; what I don't know is how vulnerable that information is, or what the nature of the threat is. Do we need to encrypt fax machines? Do we need to train executives in counterespionage techniques when they go abroad? Is the SIGINT threat serious in Des Moines? Are international telephone calls being intercepted?

When it comes to both general and specific threat and vulnerability information about foreign government collection

activities aimed as U.S. businesses, the government has a near monopoly. It seems to me that we should be exploring ways that general threat data might be made available to the private sector, as part of the government's role in this OPSEC partnership. However, while the government knows a great deal generally about the activities of foreign governments and their intelligence services, there has been too little emphasis to date on collecting against threats to the commercial sector. As some of you may be aware, the FBI is just beginning to look into the foreign counterintelligence requirements of protecting critical technologies and strategic proprietary information, in the development of its National Security Threat List. And across the board I think what we may be seeing here is an emerging new intelligence mission, as the protection of American private sector strategic information and technology is increasingly viewed as an element of the nation's security.

Providing specific threat data -- that is particular threats targeted against individual companies -- would present more of a problem. I believe the government could arguably provide such data without raising any philosophical or ethical concerns. But in practice this would raise some of the same legal and fairness issues, as well as some of the same practical difficulties, that I mentioned earlier in connection with proposals to share positive intelligence with business and industry. Each of these questions would have to be addressed.

General vulnerability data, like general threat data, would also fall within the government's responsibility in an OPSEC framework. The government understands a great deal about private sector vulnerabilities, which are often similar to the government's, because of its knowledge of the capabilities of our adversaries. Today this information is dispersed in different places within the government. In order to provide vulnerability data to the private sector, among other things we would need a way to collect, collate and analyze vulnerability data, with due regard for sources and methods, before the government could make it available. Some of this, of course, is already being done -- for example, the FBI's DECA briefings, and the State Department's Overseas Security Advisory Council's work. However, I do not believe this government support reaches the level that today's business and industry really needs. Although just how much threat and vulnerability data would be of use is an open question, which you in the private sector would need to answer.

Once strategic information has been identified, and threats and vulnerabilities are known, the next step in the OPSEC process is doing something about it. Here the government clearly has some responsibility, in particular in defeating foreign intelligence services operating in U.S.

But it seems to me that the commercial sector, armed with threat and vulnerability data, should be capable of providing its own security and countermeasures. There is an established and growing industry for providing sophisticated OPSEC, which is

represented liberally throughout this audience. While you may well need the government to tell you what your vulnerabilities are, you don't need an Army major showing up at your plant to show you how to protect your proprietary information and technology. The decisions on whether or not protection is warranted, and how to do so, rest with each firm, as they should.

How to spend your money is probably not an area where you really need more government advice.

CONCLUSION

If it seems I have raised more questions than provided answers, that's an indication that you graciously have been listening; and I thank you for that. But I would be even more grateful if, over the course of the next two days, you would give some thought to the answers. Because I believe that unless Americans in business and industry think seriously about these issues, and come forward with thoughtful and high-minded policy proposals, the government really will be able to do very little to help.

In closing, I have the honor of extending to you warm greetings from President Bush, and best wishes for a very successful security symposium.

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
02. Remarks	The Use of Intelligence in Support of US Competitiveness (5 pp.)	9/29/90	(b)(1)	

Collection:

Record Group: Bush Presidential Records
Office: Science and Technology Policy, Office of (OSTP)
Series: O'Neil, John F., Files
Subseries: Reports and Publications Files
WHORM Cat.:
File Location: Remarks by Michelle van Cleave

Date Closed: 6/1/2010	OA/ID Number: 62101-002
FOIA/SYS Case #: 2005-0336-F	Appeal Case #:
Re-review Case #:	Appeal Disposition:
P-2/P-5 Review Case #:	Disposition Date:
AR Case #:	MR Case #:
AR Disposition:	MR Disposition:
AR Disposition Date:	MR Disposition Date:

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P-1 National Security Classified Information [(a)(1) of the PRA]
P-2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P-3 Release would violate a Federal statute [(a)(3) of the PRA]
P-4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P-5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
P-6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Removed as a personal record misfile.

Freedom of Information Act - [5 U.S.C. 552(b)]

(b)(1) National security classified information [(b)(1) of the FOIA]
(b)(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
(b)(3) Release would violate a Federal statute [(b)(3) of the FOIA]
(b)(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
(b)(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
(b)(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
(b)(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
(b)(9) Release would disclose geological or geophysical information

MICHELLE VAN CLEAVE
REMARKS PREPARED FOR DELIVERY
ASPEN INSTITUTE BERLIN
SHEPARD STONE STUDY GROUP ON EAST-WEST RELATIONS
NOVEMBER 13, 1989

Last month I was in New York, and from the big picture windows of the downtown Athletic Club I could see New York Harbor and the Statue of Liberty. People from every nation represented in this room have been greeted by that Statue as they found a new home in America -- including some of my ancestors. I have been reminded of that sight as I watched the daily reports of newly arriving refugees from the East. And it strikes me that the words inscribed on the Statue of Liberty might be an equally fitting banner for Berlin today.

Who can fail to be touched by the tears and laughter of newly rejoined families and friends? Those of us who have known the blessings of liberty all of our lives are reminded anew of what a precious possession it is. And to those who are experiencing freedom for the first time, we say a heartfelt welcome.

But progress won't be measured simply by how many refugees make it to freedom. Progress will be measured by how many countries make it to freedom.

This is an extraordinary moment to be in Berlin. We in the West are watching with awe and with anticipation the sweeping developments throughout Eastern Europe. As I see it, there is a growing popular call for freedom of speech, to worship freely, to travel, to emigrate, coupled with a widespread resentment of the state. These appear to be the deeply held feelings of the average person, not just radicals or extremists. The obvious intense desire for change is breathtaking; and the new confidence and hope for the future inspiring.

And so this is an extraordinary moment to be at an international conference on the subject of East-West relations. I want to express my thanks to our host, the Aspen Institute of Berlin, for sponsoring this gathering. It does not take a crystal ball to see that the participants in the Shepard Stone Study Group have a fascinating two years ahead.

I have been asked to speak about East-West technology prospects. And in keeping with the spirit of this conference, what I have to say will reflect my own views, not necessarily the views of my government.

The United States has bilateral science and technology agreements with 86 nations, involving more than 20 federal agencies. We have supported and encouraged international

cooperation as an integral aspect of our broad S&T policy, to strengthen our scientific and technological enterprises, to enhance our commercial relationships, to protect our national security, and to promote our foreign policy goals.

If there is one thing the past forty years have taught us, it is that the path to technological development lies not through government control of economic activity but through freeing the creative energies of individuals. The newly industrialized countries have made remarkable economic strides, for the simple reason that their market-based policies have met the standards of international competition. They are especially skilled at finding imaginative commercial applications for new ideas, and then finding the markets for their trade.

By contrast, the economies of the East are suffering, for the simple reason that economic initiative and innovation cannot survive where the government controls the economy. What is needed is both free markets and free people. As Paul Johnson has noted, "market Communism" is a contradiction in terms: it is impossible to separate economic freedom from political freedom.

What does this mean for East-West technology prospects? It means that so long as the countries of the East Bloc cling to collectivist political systems, their economies will continue to fall behind. They will continue to be poor risk prospects for investment. And they will continue to have little to interest the West in terms of commerce or trade. These are the inherited liabilities Poland and Hungary are struggling to overcome.

When Soviet spokesmen complain about the "technological division of Europe" they are really complaining about the inherent liabilities of the political systems they have imposed on the East, secured by the presence of 400,000 troops. The Berlin Wall is not a high-tech barrier; it is a brute force barrier.

(Now it is a brute force barrier with beautiful big holes.)

The U.S. Secretary of Commerce Robert Mosbacher has outlined five principles within which the economic relationship between East and West can grow:

First, and most importantly, the national security needs of the West remain paramount. Export controls will remain in place. They are determined by the West's security requirements, not economics. Our objective is to prevent the transfer of militarily sensitive technology, not to shut down trade. And to that end, we will ensure that only essential technologies are controlled.

Second, there should be no large, careless lending or subsidized credit wars to encourage artificial growth of East-West trade that is inconsistent with economic realities. Trade must be on a sound commercial basis.

Third, investment must be based on commercial criteria. The countries of East need to make changes in their legal infrastructures to attract western investments.

Fourth, progress in human rights remains a prerequisite to fundamental improvements in East-West commerce.

And fifth, there must be increased openness in East Bloc economies. That means that Eastern governments must provide more information about their business and industries and societies. Markets cannot develop unless buyers and sellers have accurate data about each other and about their economies.

On the basis of these principles, the United States has joined with other Western countries to support the reforms underway in Hungary and Poland by opening our markets and providing foreign aid. And we are waiting to see whether internal liberalization will follow East Germany's historic decision to open its borders. Our approach has been to help create the conditions under which the people of Eastern Europe might have the opportunity to succeed -- or fail -- on their own terms. And if they do not succeed, to have the opportunity to try again.

In the Soviet Union, perestroika -- the restructuring of the Soviet economy -- so far has yielded little in the way of tangible results. Real GNP growth last year may actually have declined for the second year in a row, when inflation is taken into account. And from what we can see Mr. Gorbachev is coming under increasing internal pressure to make his reforms visible in the domestic Soviet economy.

Yet the very economy that engenders long lines for the opportunity to buy a toaster or a pair of shoes still poses a formidable military challenge to the Western alliance.

Although perestroika would seem to offer hope of better Soviet relations with the West, the Soviet military is interested in using it to obtain some of the new technologies they require to meet the rapid pace of weapons-related technological advances. As a Soviet general officer wrote in Red Star, "the most important elements in scientific-technical progress...are also the catalysts of military-technical progress."

I think there is a strong temptation in the West to look at the striking developments we have seen in recent months and conclude that past concerns over technology transfer are outdated. I wish that were true. But not only would such a conclusion be wrong, it would also tend to impede, rather than enhance, the process of positive change in Eastern Europe.

In the first place, the goods and materials Eastern economies need most are not hi-tech, dual use technologies. Hard currency expended in these areas would be hard currency unavailable for other, more pressing needs.

In the second place, many of the products the Soviets are seeking to support their modernization efforts -- especially in the areas of information processing, computers and microelectronics -- also have critical military applications. And there is no way to ensure that strategic goods made available to other East bloc nations won't be put to the wider service of the Warsaw Pact.

That is why I believe that COCOM -- the Coordinating Committee on Multilateral Export Controls -- is entering perhaps the most important era in its 40 year history. Since the founding of NATO, the Alliance has counted on superior economic productivity and technological innovation to offset Soviet military and political pressures. But as East-West relations have improved, nearly every Western democracy has chosen to cut back on defense research and development -- the very endeavor that historically has ensured the West's qualitative edge. If we are to offset Warsaw Pact quantitative strengths, we will need to be vigilant and united in enforcing rigorous controls on technologies that have military uses.

And this is perhaps the most important era for the NATO alliance as well. The events of this past weekend are a tribute to the success of the NATO alliance. Now, in the midst of so much change and so many questions about the future, it is the strength and unity of the West that inspire the greatest hope for all people who love freedom and would live freedom.

During our lifetimes, we have seen extraordinary scientific and technological accomplishments. Space travel. Superconducting materials. Computer capacity that once filled a warehouse reduced to a microchip. The discovery of DNA, and now the prospect of mapping the human genome.

But as monumental as these and other achievements may be, they would be eclipsed by one unparalleled event in modern history: the realization of freedom in the East.

The United States welcomes the East's movement toward the values that our own nation was founded on: individual rights, human dignity, economic liberty, and freedom of choice. These are the foundations not only of scientific and technological progress and prosperity, but of a real and lasting peace.

And today, joyously, West Berlin exemplifies all of these values, and draws Easterners like a magnet across the once impassable wall to share a taste of what it means to be free. As an American, I am deeply touched to have been here, to join in this celebration of freedom.

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
03. Remarks	Information Security Threat Forecast (9 pp.)	3/28/90	(b)(1)	

Collection:

Record Group: Bush Presidential Records
Office: Science and Technology Policy, Office of (OSTP)
Series: O'Neil, John F., Files
Subseries: Reports and Publications Files
WHORM Cat.:
File Location: Remarks by Michelle van Cleave

Date Closed:	6/1/2010	OA/ID Number:	62101-002
FOIA/SYS Case #:	2005-0336-F	Appeal Case #:	
Re-review Case #:		Appeal Disposition:	
P-2/P-5 Review Case #:		Disposition Date:	
AR Case #:		MR Case #:	
AR Disposition:		MR Disposition:	
AR Disposition Date:		MR Disposition Date:	

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P-1 National Security Classified Information [(a)(1) of the PRA]
P-2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P-3 Release would violate a Federal statute [(a)(3) of the PRA]
P-4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P-5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
P-6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Removed as a personal record misfile.

Freedom of Information Act - [5 U.S.C. 552(b)]

(b)(1) National security classified information [(b)(1) of the FOIA]
(b)(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
(b)(3) Release would violate a Federal statute [(b)(3) of the FOIA]
(b)(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
(b)(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
(b)(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
(b)(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
(b)(9) Release would disclose geological or geophysical information

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
04. Remarks	Intelligence Support to Economic Competitiveness (10 pp.)	11/29/90	(b)(1)	

Collection:

Record Group: Bush Presidential Records
Office: Science and Technology Policy, Office of (OSTP)
Series: O'Neil, John F., Files
Subseries: Reports and Publications Files
WHORM Cat.:
File Location: Remarks by Michelle van Cleave

Date Closed: 6/1/2010	OA/ID Number: 62101-002
FOIA/SYS Case #: 2005-0336-F	Appeal Case #:
Re-review Case #:	Appeal Disposition:
P-2/P-5 Review Case #:	Disposition Date:
AR Case #:	MR Case #:
AR Disposition:	MR Disposition:
AR Disposition Date:	MR Disposition Date:

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P-1 National Security Classified Information [(a)(1) of the PRA]
P-2 Relating to the appointment to Federal office [(a)(2) of the PRA]
P-3 Release would violate a Federal statute [(a)(3) of the PRA]
P-4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
P-5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
P-6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Removed as a personal record misfile.

Freedom of Information Act - [5 U.S.C. 552(b)]

(b)(1) National security classified information [(b)(1) of the FOIA]
(b)(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
(b)(3) Release would violate a Federal statute [(b)(3) of the FOIA]
(b)(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
(b)(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
(b)(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
(b)(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
(b)(9) Release would disclose geological or geophysical information

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
05. Remarks	Strategic Economic Information (10 pp.)	3/12/91	(b)(1)	

Collection:

Record Group: Bush Presidential Records
Office: Science and Technology Policy, Office of (OSTP)
Series: O'Neil, John F., Files
Subseries: Reports and Publications Files
WHORM Cat.:
File Location: Remarks by Michelle van Cleave

Date Closed:	6/1/2010	OA/ID Number:	62101-002
FOIA/SYS Case #:	2005-0336-F	Appeal Case #:	
Re-review Case #:		Appeal Disposition:	
P-2/P-5 Review Case #:		Disposition Date:	
AR Case #:		MR Case #:	
AR Disposition:		MR Disposition:	
AR Disposition Date:		MR Disposition Date:	

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P-1 National Security Classified Information [(a)(1) of the PRA]
 P-2 Relating to the appointment to Federal office [(a)(2) of the PRA]
 P-3 Release would violate a Federal statute [(a)(3) of the PRA]
 P-4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
 P-5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
 P-6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Removed as a personal record misfile.

Freedom of Information Act - [5 U.S.C. 552(b)]

(b)(1) National security classified information [(b)(1) of the FOIA]
 (b)(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
 (b)(3) Release would violate a Federal statute [(b)(3) of the FOIA]
 (b)(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
 (b)(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
 (b)(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
 (b)(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
 (b)(9) Release would disclose geological or geophysical information

Danger of spies increases

By Bill Gertz
THE WASHINGTON TIMES

Economic espionage against the United States has been a problem for years but is only one of the growing threats posed by foreign intelligence services, a senior White House official said yesterday.

"It would be seriously misleading and very dangerous in practical terms to focus on one area of the foreign intelligence threat to the exclusion of others," said Michelle Van Cleave, a national security specialist with the White House Office of Science and Technology Policy.

Miss Van Cleave, in a speech to a conference of security managers, said it is "ill-advised" for the U.S. intelligence community to shift its resources and priorities toward economic intelligence collection and analysis.

U.S. security and intelligence agencies should avoid any "subtle politicization" resulting in focusing more attention on international economic problems than on an array of serious threats to security posed by foreign intelligence services," she said.

Spies, particularly the Soviet KGB, continue to target U.S. technology — both hardware and software — and classified information on plans and capabilities, Miss Van Cleave said.

Intelligence services have caused serious damage to national security over the past 15 years by penetrating many U.S. political, military and intelligence agencies, and by stealing technology and defense-related secrets and information, she said.

"In the decade ahead, I believe the United States will face an increasingly diverse, aggressive and sophisticated intelligence threat to all of our strategic secrets and values," Miss Van Cleave told the conference sponsored by the National Security Institute.

Foes, friends, and would-be friends "all spy on us" — on U.S. military and diplomatic secrets, and private businesses, she said.

As the threat of foreign spying grows, so does the vulnerability of automated information systems — computers and telephone links — to foreign and corporate spies, Miss Van Cleave said.

"Both government and private-sector dependence on information systems is increasing, and our national security ... increasingly depends on them," Miss Van Cleave said. "So at a time when we are most dependent, we are also most exposed."

Regarding the Soviet Union, the success of U.S. high-technology weapons in the Persian Gulf war will increase pressure on the Red Army to improve its military forces, she said. As a result, the KGB can be expected to target Strategic Defense Initiative technology in particular.

"Strategic defense capabilities are likely to present a new target and a new incentive for technology theft," Miss Van Cleave said.

She also said the Bush administration has seen no fundamental changes in the KGB.

- Computer Programmer!
- Computer Operator!
- Computerized Business Systems!

**CALL TODAY FOR INFORMATION
ABOUT CLASSES**

703-971-0500

COMPUTER LEARNING CENTER

SEARS

UP TO \$250 TRADE-IN

**for your old doors when
replaced with SEARS new
cabinet doors and finishings**

Now you can enjoy a beautiful kitchen with stylish new replacement doors by SEARS. Installed on your present wood or metal cabinets, our skilled craftsmen will transform your kitchen into a showplace. Call today and see for yourself how easy and affordable your beautiful kitchen can be with replacement cabinet doors by SEARS. Optional modifications

include added cabinets, drawers, sinks, faucets and countertops.



\$49 PER MONTH*

On Sears Charge Home Improvement Credit Plan

*Based on a \$2200 purchase of replacement cabinet doors. Your actual payment can vary depending on your account balance.

**Call (202) 269-5344
THE EASY AFFORDABLE WAY
TO A BEAUTIFUL KITCHEN**

15-22 Doors \$150⁰⁰ Allowance, 23-32 Doors \$200⁰⁰ Allowance, 33+ Doors \$250⁰⁰ Allowance. Does Not Apply with Other Discounts or Previous Sales. Offer Ends 3/31/91. Sold, furnished and installed by KITCHEN CRAFT INC., a Sears Authorized Installer. M.H.I.C. 321 and 22446.

SEARS
Your money's worth
and a whole lot more.

**For HOME DELIVERY of
The Washington Times
(202) 636-3333**

Withdrawal/Redaction Sheet

(George Bush Library)

Document No. and Type	Subject/Title of Document	Date	Restriction	Class.
06. Remarks	Strategic Economic Information (12 pp.)	4/17/91	(b)(1)	

Collection:

Record Group: Bush Presidential Records
Office: Science and Technology Policy, Office of (OSTP)
Series: O'Neil, John F., Files
Subseries: Reports and Publications Files
WHORM Cat.:
File Location: Remarks by Michelle van Cleave

Date Closed:	6/1/2010	OA/ID Number:	62101-002
FOIA/SYS Case #:	2005-0336-F	Appeal Case #:	
Re-review Case #:		Appeal Disposition:	
P-2/P-5 Review Case #:		Disposition Date:	
AR Case #:		MR Case #:	
AR Disposition:		MR Disposition:	
AR Disposition Date:		MR Disposition Date:	

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

P-1 National Security Classified Information [(a)(1) of the PRA]
 P-2 Relating to the appointment to Federal office [(a)(2) of the PRA]
 P-3 Release would violate a Federal statute [(a)(3) of the PRA]
 P-4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
 P-5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
 P-6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Removed as a personal record misfile.

Freedom of Information Act - [5 U.S.C. 552(b)]

(b)(1) National security classified information [(b)(1) of the FOIA]
 (b)(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
 (b)(3) Release would violate a Federal statute [(b)(3) of the FOIA]
 (b)(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
 (b)(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
 (b)(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
 (b)(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
 (b)(9) Release would disclose geological or geophysical information