construction or construction over reducing the size of the elementary classes, but I would like to say that a school construction initiative which is meaningful would send a message to the whole Nation and the whole public education system.

If we believe in a religion, then the first visible commitment of that religion is manifested in the kind of church they build or temple they have or synagogue they have. The physical facility is not at the heart of what the religion is all about, but the physical facility is a visible manifestation of a commitment.

If we abandon the public schools of this Nation, and we have a situation similar to the one we have now, where we are spending only 23 cents per child on physical infrastructure in the elementary and secondary schools, the Federal commitment, the Federal portion of the commitment to the physical infrastructure right now is about 23 cents per child. We have 53 million children in school. When we look at the amount of money the Federal Government is spending, it is about 23 cents per child.

I propose a bill, H.R. 1820, which I have already introduced and am seeking cosponsors, where we would spend $417 per year per child instead of 23 cents per year per child. For $417 per year per child, we could deal with the crumbling, dilapidated schools, schools that endanger the health of youngsters because they have coal-burning furnaces, lead pipes, some have serious problems in terms of the roof. No matter how many times you repair it, the water seeps into the walls at the top and it keeps coming down. Lead paint, lead is in the paint. There are all kinds of dangers.

Many buildings are just so old. We have a lot of buildings in New York City that are 75 years or older, many that are 50 years old. This is not unique to New York City. All of the big cities have the same problem. Many rural areas, of course, have even worse problems. They never had sound buildings. We need a construction effort.

I conclude by saying that investment in the public education system is one of many of the steps we need to take to end the oppression of working families and provide benefits, and have them share in the wealth, instead of being objects of our contempt.

Madam Speaker, I include for the RECORD the following information on World War II:

BIG STATE, BIG CITY CASUALTIES

State	Total casualties	Combat deaths	Three big cities
		World War I	
New York	35,100	7,307	New York, Buffalo, Albany
Pennsylvania	29,576	5,996	Philadelphia, Pittsburgh, Harrisburg
Illinois	15,984	3,016	Chicago, Springfield, Peoria
Ohio	14,487	3,073	Cleveland, Cincinnati, Dayton
Massachusetts	11,455	2,153	Boston, Amherst, Burlington
Michigan	9,702	2,213	Detroit, Ann Arbor, Lansing
New Jersey	8,766	1,761	Newark, Jersey City, Hoboken
California	6,153	1,352	San Francisco, Oakland, Los Angeles

BIG STATE, BIG CITY CASUALTIES—Continued

State	Total casualties	Combat deaths	Three big cities
		World War II	
New York	89,656	27,659	New York, Buffalo, Albany
Pennsylvania	81,917	24,302	Philadelphia, Pittsburgh, Harrisburg
Illinois	54,686	17,338	Chicago, Springfield, Peoria
Ohio	49,989	15,636	Cleveland, Cincinnati, Dayton
Massachusetts	31,910	9,991	Boston, Amherst, Burlington
New Jersey	31,544	9,742	Newark, Jersey City, Hoboken
California	47,073	17,048	San Francisco, Oakland, Los Angeles
		Korean Conflict	
New York	8,780	2,249	New York, Buffalo, Albany
Pennsylvania	8,251	2,327	Philadelphia, Pittsburgh, Harrisburg
Illinois	6,435	1,744	Chicago, Springfield, Peoria
Ohio	6,614	1,777	Cleveland, Cincinnati, Dayton
Michigan	5,181	1,447	Detroit, Ann Arbor, Lansing
		Vietnam	
New York	N/A	4,108	New York, Buffalo, Albany
Pennsylvania	N/A	3,133	Philadelphia, Pittsburgh, Harrisburg
Illinois	N/A	2,926	Chicago, Springfield, Peoria
Ohio	N/A	3,082	Cleveland, Cincinnati, Dayton
Massachusetts	N/A	1,317	Boston, Amherst, Burlington
Michigan	N/A	2,641	Detroit, Ann Arbor, Lansing
California	N/A	5,563	San Francisco, Oakland, Los Angeles

REPORT ON RESOLUTION PROVIDING FOR CONSIDERATION OF H.R. 1401, NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2000

Mrs. MYRICK (during the Special Order of Mr. WELDON of Pennsylvania), from the Committee on Rules, submitted a privileged report (Rept. No. 106–175) on the resolution (H. Res. 200) providing for consideration of the bill (H.R. 1401) to authorize appropriations for fiscal years 2000 and 2001 for military activities of the Department of Defense, to prescribe military personnel strengths for fiscal years 2000 and 2001, and for other purposes, which was referred to the House Calendar and ordered to be printed.

INFORMATION RELATIVE TO THE COX REPORT

The SPEAKER pro tempore (Mrs. BIGGERT). Under the Speaker's announced policy of January 6, 1999, the gentleman from Pennsylvania (Mr. WELDON) is recognized for 60 minutes.

Mr. WELDON of Pennsylvania. Madam Speaker, I rise tonight to continue to provide for our colleagues in the House and for the constituents that they represent across the country information relative to the Cox report and the way this report is being spun by this administration.

Madam Speaker, I had wanted to go into much of the information I am going to share tonight in more detail yesterday, but because I had to leave after 30 minutes, I could not go into detail last evening. I will do so tonight.

Madam Speaker, I want to start off this evening, as I did last night, by saying it is not my normal course to spend every evening over a given period of time on the floor of this House discussing the same issue. But like eight of my colleagues, I spent almost the last year of my life focusing on the investigation that we were asked to perform by the leadership in both parties in this body on potential security harm done to our country by our policies relative to China and other nations that might benefit from technology developed here in America.

We worked tirelessly behind closed doors, cooperating fully with the FBI and the CIA, and with the full support of George Tenet, who heads the CIA, in trying to determine whether or not there were damages done to our national security, and if so, what was the extent of that damage.

We deliberately made a decision when we began the process last summer that we would not go into the specifics of campaign finance activity or what other motives would have driven policymakers to lower the thresholds for exports, or perhaps the reasons why influence would be allowed by Chinese nationals and others, both at the White House and to other Federal agencies, to allow those key players to gain access to the key decisionmakers that would benefit them in acquiring technology.

□ 2145

The nine Members that were a part of the Cox committee represent a broad basis of views in this Congress, four Democrats and five Republicans, very serious Members; and our goal was and the result was a totally nonpartisan effort.

We looked at every aspect of technology that may in fact pose problems for us down the road: whether or not that technology had in fact been transferred; if so, to what extent, how it was transferred, and what the implications were for our long-term security.

The almost 1,000-page document that we completed is, I think, very detailed and certainly would be required reading for any American. The problem is, most American citizens, like most Members of Congress, do not have the time to sift through almost 1,000 pages of detailed explanations and stories relative to various technologies that had been transferred out of the U.S. over the past several decades.

Therefore, because much of this is contained within the thousand-or-so-page report, even though 30 percent of that remained classified because the administration would not declassify the entire document, the media, to a large extent, have chosen not to focus on the substance of what is in the Cox committee report.

Unfortunately, the bulk of the American media, and I say the bulk because there are a few exceptions, people like Jeff Girth with the New York Times, who has been doing tireless work in this area before our report was even issued; people like Carl Cameron at Fox News, who continues to do extensive work in this area; people like 60 Minutes, who are right now doing research in these areas, and other network affiliates, they are the exception. The bulk of the mainstream media have chosen to accept the spin that has been given by this White House to the work that we did.

What I am trying to do, Madam Speaker, is to present information to our colleagues, which they could, in turn, provide to their constituents, of a factual basis that compliments the work that was done by the Cox committee.

Now, the public at large can receive copies of the Cox committee report. It is available on the newsstand, or they can get it on the Web site that has been established by the Cox committee itself. Many libraries now have copies of the Cox committee three-volume series.

Last evening, I mentioned the fact that I have now established a Web site on the Cox report that goes beyond the information that is covered in the Cox report and provides the visual explanation of the overview of the problem that we dealt with in the Cox committee.

So our colleagues, Madam Speaker, and all of their constituents can now turn to the Internet where they can access the material I am going to show this evening, and they can download the actual charts that I am going to provide. In addition, smaller versions of these larger charts have been made available to every Member of this body. All they have to do is contact my office, send a staffer over; and be they Republican or Democrat, they can get the charts and all the related information that goes with the charts so they can share this information in a factual way with their constituents.

The Web site where our colleagues and the American people across this country can access this information is www.house.gov/curtweldon. Any American represented by any one of our colleagues can access this information through that Web site.

In fact, last evening, we had a number of contacts from throughout the country from people who want to get additional factual information in an investigational form, in a condensed form about what actually the Cox report focused on.

As I have said in a series of speeches that I have been giving both here and around the country, Madam Speaker, the focus of the Cox committee was not just on our laboratories. Now, if my colleagues listen to Bill Richardson, the Secretary of Energy and the point person that has been asked by the administration to provide the spin for the Cox committee report, my colleagues would think that our report only focused on our laboratories, Los Alamos, Sandia, and Lawrence Livermore in particular. Nothing could be further from the truth, Madam Speaker.

While it is true, the laboratory security was one part of what we looked at, it is only one small part of the bigger picture of the way that we loosened the controls over our technology for the past 7 years.

The American people need to understand that this effort was well beyond our laboratories. But as I did last night, I want to highlight four specific actions that rebut what Secretary Richardson has been saying around the country as the point person for this administration as he has tried to spin the Cox committee report as though it is only concerned with lab security.

Now, Madam Speaker, our colleagues know full well, because they have read the text of Mr. Richardson's speeches, that his focus has been something along the lines of this: This administration was the administration who uncovered the Chinese espionage in 1995 that happened in previous administrations that were run by Republicans, and we took aggressive action in this administration to correct those problems.

Secretary Richardson would have the American people believe and would have our colleagues believe that this administration had no responsibility whatsoever in technology being transferred to China and that the only thing they did was that they uncovered the fact that, in 1995, they learned that China had stolen the designs for our warhead capabilities, the W–88 and the W–87, that occurred in previous administrations. That has been the extent of Secretary Richardson's comments.

He has also gone on to say, now, look, we have taken steps to correct all of this, and today we have corrected the bulk of the problems.

Well, I am here to rebut that, Madam Speaker. I would like to do it in a forum where I could stand directly across from Secretary Richardson, or even the President, and have a chance to go at it verbally and exchange information, but it looks like that is not going to be possible.

The national media outlets will put Secretary Richardson on the Sunday morning talk shows to give the White House spin, but they have yet to give full consideration to the factual rebuttal to what Secretary Richardson has been saying. So I am going to attempt to do that here again on the public record tonight.

First of all, we must remind the American people that contrary to what Secretary Richardson has been saying, it was this administration, under the leadership of then-Energy Secretary Hazel O'Leary in 1993 that ended the policy of color coding laboratory security credentials at our laboratories. My understanding is that she thought having color coded badges was to some extent discriminatory and they were not necessary. So under her administration, acting on behalf of Bill Clinton, we did away with that process in 1993.

Now what did that mean? That meant, Madam Speaker, that all of those employees at our labs that we used to be able to tell by the color of the identifying ID system that they had on them no longer could be done, or no longer could be checked, because we did away with that color coding, making it much more difficult to determine where employees could or could not work or be in a particular classified laboratory setting.

So under Secretary Hazel O'Leary, this administration ended the practice of visually being able to identify what people at our labs could or could not have access to key areas. Now, obviously that made it much easier for unauthorized people to go into areas where they did not have appropriate clearance.

Now, if this policy were so acceptable and defensive, my question is, why did this administration 2 weeks ago reinstate the policy as it existed under President Reagan, President Bush, and even President Carter and before that? If this policy change, which Secretary O'Leary made on behalf of Bill Clinton in 1993 and 1994, was so critically important and logical, why 2 weeks ago did they go back to the policy as it was under Republican Presidents?

Was perhaps there some new revelation that this relaxation that occurred by the Clinton administration in 1993 and 1994 led to security problems in our laboratories? Bill Richardson has yet to answer that question.

Second point, Madam Speaker, we have not heard Bill Richardson talk about the fact that it was under Secretary Hazel O'Leary, acting on behalf of President Clinton, that FBI background checks of people who worked at our labs and visited our labs were put on hold.

Now, why do we have FBI background checks? They were there to discourage people who should not have access to our country's secrets to get into places where those secrets were kept. That was not done prior to 1993, Madam Speaker. That was done by this administration as a major change in policy that opened the floodgates for people to go to our labs, who in previous years would not have been allowed access to those facilities.

Bill Richardson has not dealt with that issue, because as he said, this administration only inherited problems and did everything to correct them.

Third point. There was an incident involving a retired employee from Lawrence Livermore Laboratory in the 1993 to 1995 time frame, where that employee, former employee, was accused by the Department of Energy of having released sensitive classified information to unauthorized people. The Department of Energy investigated that employee. The Oakland office of the Department of Energy saw fit, based on the factual evidence to remove that former employee's classified status so that he no longer, as a retiree, had access to classified information.

The employee appealed that decision to the Secretary of Energy's office. Hazel O'Leary herself overturned the decision of the Oakland Department of Energy office and allowed that retiree to retain his classified status. When that occurred, Madam Speaker, employees all across DOE involved in sensitive security areas got the feeling that this administration felt that giving away classified secrets was no big deal.

We lowered the threshold for the security clearance process. We stopped the FBI background checks. Then we even had an employee who was accused by the Department of Energy itself, and found guilty of giving classified information. The Secretary herself overturned the Department of Energy decision to take away his security clearance.

Now, those people that I have talked to in the Department of Energy who worked under Hazel O'Leary, way more than one or two people, have said that under her leadership, there were wholesale actions to declassify massive amounts of information, in some cases boxes and cartons of records that no one had gone through, simply declassified, made available for people to read in a spirit that I guess was considered openness, even though these were, in many cases, the most important technical secrets that this country had.

Let me give my colleagues one particular example, Madam Speaker. Secretary Richardson has gone around the country, and he has made the case that when this administration found the evidence in 1995 that China had stolen or received the design for our most capable nuclear warheads, the W–88 and the W–87, that this administration immediately corrected those problems so they would never occur again. Even though Janet Reno cannot properly explain why the Justice Department turned down requests for four wiretaps, for efforts by one of our employees at one of our labs that we thought was a spy, Secretary Richardson has said they took aggressive action.

Now, that is what he said publicly. I wish he would answer this question, because that same year, in 1995, U.S. News and World Report published a special report entitled ''Shockwave.'' ''Shockwave'' was printed on July the 31, 1995, distributed all across the country and around the world. I am sure a number of these copies were sold in China.

□ 2200

Because when I traveled to Beijing I saw copies of U.S. News and World Report on the shelves that people could buy. The same thing in Russia. These copies were available in North Korea, in Iran or Iraq. This edition of U.S. News and World Report's Special Supplement were sold wherever people would pay the price of whatever this document cost, $3.50. What was in this special report on the last page, which I showed last evening, was startling.

On July 31, 1995, this administration, not the Reagan administration, not the Bush administration, not the Carter administration, this administration leaked the design for our W–87 warhead to U.S. News and World Report. Not just the Chinese, the North Koreans, the Iraqis and Iranians, anyone who would buy U.S. News and World Report on July 31, 1995 got a documented diagram of the W–87, which up until that point in time was classified.

Here is the color version of what the Department of Energy released to U.S. News and World Report. This design shows in some detail the way our most capable nuclear warhead works. It shows and explains the process, it shows and locates the technology, the fuel, the process, the activity, the physics of the way America's most capable warhead would work. This was not secretly stolen by the Chinese, that this administration maintains they found in 1995. This diagram was given to U.S. News and World Report by this administration in 1995, and reproduced in U.S. News and World Report.

As I said last evening, Madam Speaker, I have been told, and I am tracking this down right now, that there was an internal investigation within the Department of Energy to find out who leaked this diagram, this sensitive diagram to U.S. News and World Report. Because I have been told, Madam Speaker, that that individual and group were told to stop the investigation. Why? Because the assumption was that this diagram came from Hazel O'Leary's office herself.

Why are we not hearing Secretary Richardson talk about this, Madam Speaker? Why is he not talking about in 1995, in July, when this diagram for the W–87 was reproduced and sold on newsstands all over the world to anyone who would pay the price? This was not some secret espionage capability of the Chinese. This was the Department of Energy, following Hazel O'Leary's desire to open up to the people of the world our most secret information about technologies important to our country.

There is one additional factor that needs to be investigated, Madam Speaker. There was an individual, or is an individual employed at the Department of Energy who has currently been placed on what I call political administrative leave. His name is Edward J. McCallum. He was the one who briefed Members of Congress and their staffs about problems with one of our nuclear facilities, Rocky Flats. When it was found out that he had done the outrageous thing of informing Congress about security concerns at one of our nuclear sites, what was the response of this administration? They put him on administrative leave. Secretary Richardson has announced that he is going to fire Mr. McCallum because he claims he gave out classified information.

Madam Speaker, I cannot believe this is happening in America, but there is some added irony here. Madam Speaker, I am providing for the CONGRESSIONAL RECORD, a document dated May 3, 1999, prepared by Mr. McCallum which outlines the problems at Rocky Flats and what steps he took to correct them.

STATEMENT OF EDWARD J. MCCALLUM

Mr. Chairman, thank you for the opportunity to speak with the committee today on the Department of Energy's Safeguards and Security Program. Over the past nine years, I have served as the Director of DOE's Office of Safeguards and Security. In this capacity, I have been responsible for the development and promulgation of policy that governs the protection of the national security assets entrusted to the department, to include those assets that are part of the nation's nuclear weapons program. I am also responsible for providing training and specialized technical advice and assistance to DOE field sites when requested. My office is also charged with conducting special inquiries into incidents of security concern to include, but not limited to, those incidents involving the unauthorized disclosure of classified information.

As you may know the Department of Energy has placed me on Administrative Leave since April 19, 1999. DOE officials allege that I committed a security infraction by claiming that I disclosed classified information during a conversation with a whistleblower from the Rocky Flats site. Based on the Department's own classification procedures and guidelines (CG–SS–3, Chap 10, Dispersal of Radioactive Material), I firmly believe that these allegations are completely unfounded. I have been an authorized classifier in the DOE and it's predecessor organizations for over 25 years and helped develop the first classification guide in this area in 1975. Further DOE also failed to follow its own procedures in investigating these issues before placing me on Administrative Leave. I believe this action to be an obvious act of retaliation against the individual and the office that has tried to bring an increasingly distressing message of lax security at the DOE Laboratories forward since 1995.

Prior to joining the Office of Safeguards and Security I held several high level positions within the department's safeguards and security program areas. From 1988–1989 I served as Director, Office of Security Evaluations. In 1978 I joined the DOE at the Chicago Operations Office and in 1979 became the Director of the Safeguards and Security Division. Prior to joining DOE I served as an officer in the U.S. Army. Active military service included a number of Military Intelligence and Special Forces assignments in Europe and Southeast Asia. I culminated my military duty after over thirty years of active and reserve service.

In fulfilling my responsibilities as the Director, Office of Safeguards and Security, I have attempted to provide senior DOE management with the most sound, professional judgment possible concerning the status of security within the department, along with recommendations as to how best to rectify shortcomings. As you are no doubt aware, much of what I have offered over recent years has not been altogether positive, nor well received. The steady decline in resources available to the DOE safeguards and security program as well as a lack of priority have allowed the department's protection posture to deteriorate to a point where a program that long operated in a defense in depth mode, where no single point failure permitted the system to fail, can no longer afford such a strategy.

The information presented in this statement is not new. It has been repeated consistently over the last decade in Departmental reports such as the Annual Reports to the Secretary in 1995, 1996 and 1997 by the Office of Safeguards and Security. External reviews such as the Report to the Secretary in 1991, by General James Freeze, and the Nuclear Command and Control Staff Report on Oversight in the DOE in 1998 cite similar concerns. There have also been a large number of General Accounting Office Reports on these areas. However, for numerous reasons the department has not been able to resolve these serious and longstanding problems.

COMPUTER SECURITY

One of the primary interests expressed by the Committee, and indeed widely covered by the media recently, is the loss of classified information from the computer systems at the National Laboratories. Indeed, we may be sitting at the center of the worst spy scandal in our Nation's history.

The DOE Computer Security Program suffers from a variety of problems. One of the primary concerns is the protection of unclassified sensitive information processed by the Department and the relationship of these systems to the classified architecture. Relatively little guidance has been issued on how to protect sensitive but unclassified information. System administrators are charged with the responsibility for designing their own protective measures. Unfortunately, many of them do not have the computer security background or knowledge required to implement a sound computer security program. Attempts to issue comprehensive guidance by my office and the Chief Information Officer as early as 1995 met with significant Laboratory resistance. Several Laboratories complained that providing protection such as firewalls and passwords were unnecessarily expensive and a hindrance to operations. Implementation of the proposed Computer Security Manual in 1996 would have prevented many of the problems being reported today.

Another area of great concern is the migration of classified information from systems approved for processing classified data to less secure unclassified processing systems. My office has noted a number of problems in this area to include: Failure to conduct classification reviews before placing information onto an unclassified processing system, intentionally creating unclassified data that is very close to classified data to ease processing, and using personal computers at home to process classified information.

A variety of computer security tools and techniques, such as encryption devices, firewalls, and disconnect features, are available and their use is required; however, these protective measures are not always used. In some cases, this is due to lack of knowledge by system administrators. In other cases, it is due to lack of funding or priority for the required equipment.

PROTECTIVE FORCES

While much of the attention of late has been directed toward the area of foreign visitors and the protection of classified information, equally serious cause for concern exists in other areas as well. For instance, since 1992, the number of protective forces at DOE sites nationwide has decreased by almost 40% (from 5,640 to the current number of approximately 3,500) while the inventory of nuclear material has increased by more than 30%. The number of Protective Force Officers has declined to the point where it is questionable at some facilities whether the DOE Protective Force could defeat an adversary. By 1996 several facilities were no longer capable of recapturing a nuclear asset or facility if it were lost to an adversary. Indeed, a number of sites stopped even training for this mission because resources had been reduced below the minimum level necessary to expect success. We have had some success in increasing these numbers of recent years so that at this time all sites report they can meet this minimum capability. Several sites are using performance tests to verify that their Protective Force can defeat the adversary; however, many of these tests are not realistic. For example, performance tests sometimes are not consistent in providing the adversary with the weaponry or explosive breaching devices used by terrorist groups. At times artificial ''safety constrains'' are imposed on exercise adversary teams that effectively neutralize their ability to operate. This results in ''winning'' the performance test, in a less than realistic scenario.

There have been several other consequences of the reduction in the number of Protective Force Officers. First is a relatively older Protective Force (the average Protective Force Officer is now in his/her early 40s). Second, DOE sites are relying on local law enforcement agencies to handle serious security threats. Their ability in nuclear terrorist situations is questionable. Third, sites have difficulty increasing the tempo of security operations during high threat periods. Fourth, Protective Force personnel are displaying lower morale due to reduced training and job stagnation. Finally, an average annual overtime rate in our nuclear weapons facilities of approximately 25% has detrimental effects on safety, training, and response capabilities.

EXERCISES

A centrally funded and well-integrated National-level security exercise program is critical to meet the safeguards and protection needs of DOE and the nation. Exercises that address site response and management of security crisis are required by regulation to be held annually at critical DOE facilities. However, participation by State and local law enforcement, regional offices of the Federal Bureau of Investigation (FBI) and other Federal agencies is inconsistent and varies considerably across the complex. Under Presidential Decision Directives 39 and 62, the Secretary of Energy is directed to conduct exercises to ensure the safety and security of its nuclear facilities from terrorism. DOE is also tasked to support the FBI in its lead as the Federal agency responsible for managing all domestic incidents involving terrorist threat or use of weapons of mass destruction (WMD). In addition, the recent creation of the Department of Justice National Domestic Preparedness Office, the FBI Critical Incident Response Group (CIRG), and other National crisis response assets, requires that DOE plan and practice a new and expanded role in supporting a security crisis response beyond the local site and internal Department level.

Currently, the present DOE organizational structure separates exercise responsibility between Program offices and Safeguards and Security; this hampers the integration of sequential training objectives that can be monitored and tracked and creates confusion at the site level. More importantly, the majority of the funding resides at the site level where expenditures must vie with other program needs each fiscal year, often to their detriment.

PHYSICAL SECURITY SYSTEMS

Another area of concern involves aging and deteriorating security systems throughout the DOE complex. Physical security systems are critical to ensure the adequate protection of Special Nuclear Material (SNM). Many facilities have systems ranging in age from 14 to 21 years, and are based on mid-70's to early-80's technology. Because of the obsolescence of these systems, replacement parts and services are increasingly expensive and hard to obtain. Expensive compensatory measures (i.e., protective force response) are required to ensure needed confidence levels of adequate protection. Older systems are also increasingly vulnerable to defeat by advanced technologies that are now readily and cheaply available to potential adversaries. Continual reductions, delays or cancellations in line-item construction funding increases the vulnerability risks to sites protection capability. Also, DOE is not realizing significant savings available through advancements in technology that have increased detection, assessment, and delay capabilities.

Some sites are using a variety of nonstandard security alarm and access control systems that have not been fully tested to determine if they contain vulnerabilities, or if they meet Departmental requirements without compensatory measures. Such systems may have back doors or viruses, that allow the insider adversary to cripple the entire site protection system, thus leaving the site vulnerable. Some sites do not have qualified personnel to conduct these vulnerability tests and are generally unwilling to conduct any type of attack on the system to determine if such vulnerabilities can be accomplished.

COUNTERTERRORISM MEASURES

PDD–39, The United States Policy on Counterterrorism, requires all governmental agencies to implement security measures to defend against Weapons of Mass Destruction, including chemical and biological weapons. The Office of Safeguards and Security has developed the necessary policies and requirements for implementing PDD–39. Field Elements, however, have been slow to purchase and install explosive detection systems, with only a limited number of sites having done so. Program Offices claim that there is no funding for such equipment.

PERSONNEL SECURITY

I fear that a recent decision by the department to have program offices fund the cost of clearances for field contractor personnel will have severe repercussions. Since implementing this new approach at the beginning of FY 1999, we have already begun to see a dramatic increase in the backlog of background investigations. As with other security areas, program offices must decide upon competing interests when determining those areas to be funded. Unfortunately, security activities are relegated to a lower tier in terms of importance by some program offices and selected field sites. This appears to be the case with the funding of security background investigations. As the first line of defense against the ''insider'' threat, the adequate funding and timely conduct of reinvestigations is critical to ensuring the department maintains a protection posture commensurate with the level of threat.

ROLES AND RESPONSIBILITIES

Operating beneath the surface of these major challenges are some fundamental issues that, if properly addressed, could provide the impetus to effect real progress. These challenges, for the most part, are not new, nor are their solutions.

Organizational Structure: In all of the reviews of the safeguards and security program conducted during the last decade, there is a recurring theme. Simply, the Department's organizational structure of the Safeguards and Security Program is such that programmatic authority and responsibility are not properly aligned. The Safeguards and Security Program in its current structure has one organization developing policy, training and providing technical field assistance (NN), another organization providing funding and ''implementing guidance'' (Headquarters Program Offices), a third organization (Field Site) is responsible for implementation of policy, while a fourth (EH) is responsible for oversight. A fundamental change in both the organizational structure and funding of the Safeguards and Security Program is absolutely necessary before the Department can begin to systematically address the major challenges previously addressed. These organizations must be consolidated with policy, guidance and implementation in one location, with an appropriate budget to participate in the Department decision making.

Safeguards and Security Program Funding: This is the central, driving issue. Budget cutbacks have adversely affected all of DOE. As previously alluded to, however, when Program Offices face funding shortfalls, there is a tendency to cut security programs on a pro rata basis without the benefit of assessing the impact these cuts would have on the department's protection posture. The implementation of virtually every security program, from the Information Security Program to the Protective Force Program, has suffered significantly as a result. I believe many of these cuts are shortsighted and ill advised as they eventually lead to security lapses. Nevertheless, my office has no authority to force the Program Offices to implement departmental security policies and requirements. Similarly, my office has no funds to provide to Program Offices or Field Elements to help pay for appropriate security measures. Without an adequate budget there is simply no authority.

Security Policy and Requirements Formulation. DOE security policies and requirements are based upon current threat data and requirements identified by outside intelligence organizations. DOE, the Department of Defense, the Nuclear Regulatory Commission, the Federal Bureau of Investigation, and the Central Intelligence Agency meet every two years to evaluate current threat data and formulate an agreed upon threat statement that governs security programs throughout the U.S. Government. In addition, the Department of Energy internally reviews this threat statement annually. In DOE parlance, the resulting document is known as the Design Basis Threat. Program Offices are required to use the Design Basis Threat as the baseline for planning security measures. Security requirements are also levied upon the Department by the Office of the President, Congress, and the General Services Administration. For example, Presidential Decision Directive 39 directed all Executive Branch agencies to protect against terrorist attacks. This resulted in an increased need for explosive detection equipment, more frequent security patrols, and hardening of structures. In some cases, Program Offices have directed their field elements not to implement departmental security requirements. This is due to 2 main reasons: The program offices can't afford the new directive, or they simply don't agree with it. In other cases, they have issued interpretive guidance that changes the security policy or undermines the effectiveness of that policy. Again, the Office of Safeguards and Security has no authority to demand compliance with departmental security policies and requirements.

ACCOMPLISHMENTS

I would be less than forthcoming if I failed to mention some positive aspects of the department's safeguards and security program. Let me start by saying that the program is staffed by hard working dedicated men and women throughout the country who are firmly committed to protecting the critical national security assets entrusted to their care. The responsibilities of these individuals are most demanding, even dangerous in some respects. Yet despite the dwindling resources made available to them, these individuals continue to perform in outstanding fashion. Where this department has failed is in providing these professionals the necessary resources to allow them to perform their responsibilities appropriately. The Department has also failed to provide protection so that individuals will bring forward problems and deficiencies without fearing retaliation.

Progress has been made in some of the areas I previously addressed. In the area of physical security, the Department is working to correct identified weaknesses. Specifically, the Department augmented security at some field sites by deploying new technologies to safeguard special nuclear materials and weapons; worked with other agencies to train departmental protective forces; identified and developed more sophisticated detection and deterrent systems; and hired additional security personnel. New explosive detection systems are being installed at selected nuclear facilities and some sites are upgrading access control systems.

In the area of information security, the Secretary recently directed the shut down of classified computer operations at three national laboratories until such time as he was assured that information processed on the systems is being done so securely. From a longer-term perspective, the department is requesting a dramatic increase in budget for information security. The additional funding will be used to help further secure the department's classified and unclassified computer networks. The improvements will help strengthen fire walls, develop better intrusion detection devices, and fund rapid response teams to work with the FBI to detect and track cyber intruders.

In the area of the control, measurement and accountability of special nuclear materials, the Department has established the Fissile Materials Assurance Working Group (FMAWG) to assess needed areas of improvement and make recommendations. In this regard, the FMAWG identified unmeasured materials and initiated actions to resolve discrepancies. They further identified issues regarding the safeguarding of irradiated material and are promulgating policy for implementation. The Department is developing new technologies for tamper indicating devices and proposing pilot projects for field implementation.

A PATH FORWARD

All of these positive steps are good, necessary actions to ensure the adequacy of our protection posture. More is needed, however. As previously addressed, organizational realignment of safeguards and security activities is sorely needed. I understand that this is now under review by the department. While addressing the problems inherent in the current organizational structure of the Department will not in itself solve all of the issues contained in this report, it will establish the necessary framework to allow resolution in a more effective and lasting manner. Simple organizational realignment, however, by itself, will not result in the fundamental change in approach that is required. The Department should work closely with Congress to establish a budget line item for safeguards and security. Doing so will enable a more accurate accounting and control of safeguards and security expenditures. It will also improve the likelihood that policy will be issued in conjunction with the necessary resources to implement that policy.

It should be apparent that attempts to have effective internal oversight of the DOE safeguards and security program have failed over a twenty-year period. While there have been high points and periods when oversight has been effective, organizational and budget pressures have played too central a theme for this function to remain within DOE. An organization like the Defense Nuclear Facilities Board should be established to independently review Security at DOE and the Laboratories. Further a direct reporting mechanism should be established to one or more of the Congressional Committees.

Perhaps the biggest challenge facing the department today as we strive to meet our protection responsibilities is the attitude throughout the complex toward security. There are some that believe that safeguards and security is an overhead expense. I disagree, strongly. Safeguards & security is a mission-critical element. Without it, why bother creating new national defense technologies, if present or future foes can have ready access to it? To treat it as a mission-critical element requires a greater sense of accountability than seen to date. Secretary Richardson has committed to establishing and maintaining a sound safeguards and security program. It will take the commitment not only of the Secretary, however, but of each and every program official throughout the department if this mission essential element is to be fulfilled. It is incumbent upon senior departmental management to make safeguards and security a priority. It is too important to be relegated to a secondary status where its operations are viewed as ancillary. Both Congress and the public rightfully expect our best effort in executing this vital program. We should demand no less from ourselves.

DEPARTMENT OF ENERGY,
Germantown, MD, January 27, 1997.

MEMORANDUM FOR DISTRIBUTION LIST

From: Edward J. McCallum, Director, Office of Safeguards and Security.
Subject: Status of Safeguards and Security.

This report provides a comprehensive review of Safeguards and Security activities throughout the Department of Energy complex during 1996 and provides a candid look at the future of the Program. The report is structured to present a Departmental perspective of the Safeguards and Security Program to senior management and all safeguards and security professionals. For the first time the report also contains a section which summarizes safeguards and security participation in National Nuclear Command and Control activities.

During the past year disturbing trends continued that resulted in additional budget reductions, further diminishing technical resources, reducing mission training and undermining our ability to protect nuclear weapons, special nuclear materials and other critical assets. This is occurring at a time of increased responsibilities resulting from the international transfer of nuclear materials and dismantling of U.S. nuclear weapons. Although traditional and time proven protection principles are still emphasized, it is becoming increasingly difficult to adequately protect our nation's nuclear stockpile in the face of inadequate resources, obsolescent systems, aging protection forces and funding uncertainties. This has increasingly resulted in a ''hollow-force'' that goes below the ''bottom line'' and makes it more difficult to fulfill National Security mandates. It is imperative that the Safeguards and Security downward resource spiral be immediately halted. Further, nuclear materials must be consolidated to reduce costs or additional resources must be found for protection. Adequate investment is essential to sustain a vital Safeguards and Security Program that continues to support the nation's security, the public health, safety and our environment.

I am confident that the report will be a valuable tool to stimulate open conversation, provide constructive feedback and assist in addressing the continued viability of the Department's Safeguards and Security Program. Collectively, we must continue to strive to maximize the use of our resources necessary to ensure requisite security for the

Nation's and the Department's most vital assets.

Attachment.

CENTRAL INTELLIGENCE AGENCY,
Washington, DC, March 16, 1999.

Dr. ERNEST MONIZ,
Acting Deputy Secretary, Department of Energy, Washington, DC

DEAR DR. MONIZ: As the Central Intelligence Agency's representative to the Department of Energy (DOE) Security Management Board, I would like to convey some important perspectives concerning on-going discussions to reorganize the Department's security element. Of concern is consideration that is being given to further decentralize DOE's security management apparatus and assignment of security expenses to indirect costs (i.e., overhead) at the individual sites and Laboratories. In my judgment, and based on our experience at CIA, DOE should undertake such reorganizational and budgetary alignments advisedly.

Using CIA's experience as an example, reorganization through division can be highly ineffective and inefficient. Shortcomings to CIA's 1994 decision to divide the Office of Security were quickly exposed, including: expensive duplication of security activities, deteriorated management focus over a tangential security program, elimination of a coherent security career service, and dilution of CIA's leadership role in the Community. Adding to the difficulties, security managers under this arrangement had limited control over their fiscal fate, having been placed alongside and beneath numerous budgetary layers.

Director Tenet recognized these inefficiencies immediately, and placed me in charge of consolidating CIA's program in 1997. In addition, he has provided security with a stronger voice in its fiscal future. The process to reconstitute our security apparatus has been challenging; but, its benefits have already become apparent through a stronger, more viable security program.

The lessons learned after CIA decentralized its security organization have also been experienced by other agencies, several of which have chosen to reconsolidate their activities. With such stark examples of the shortcomings of decentralization in security apparatuses, I urge you to give strong consideration to the implications of such reorganization of DOE.

Furthermore, in today's world of sophisticated technological threats, and given the developing review at one of the National Laboratories so widely publicized, I would further caution against leading the charge toward field autonomy, and anticipated the Department looking toward reinforcing centralized security expertise.

When appointed to the Security Management Board a year ago I expected that the Department wanted the input of the representatives from other Agencies in security issues of this nature. In fact, I believed that obtaining such outside counsel on issues of this nature was the purpose for which the Board was created. Unfortunately, my experience with the Board indicates that it is a feckless exercise with no accomplishments almost fifteen months after it was established. I would welcome the opportunity to further discuss my views with you at your convenience.

Sincerely,

RAYMOND A. MISLOCK, Jr.
Associate Deputy Director
For Administration for Security.

[From the Wall Street Journal, May 3, 1999]

CONGRESS BRINGS NEW INQUIRES INTO WEAPONS SECURITY FAILURES

(By John J. Fialka)

WASHINGTON.—House and Senate investigators are launching new inquires into the Energy Department's $800 million security program and how it failed to stop the apparent compromise of many of the nation's most valuable nuclear-weapons secrets.

Rep. John D. Dingell, the Michigan Democrat who led several of the House Commerce Committee's previous investigations in the 1980s and early 1990s, charged that the department runs a system of ''inverse reward and punishment.'' People who have identified lax security at the nation's defense labs have been punished and those who somehow finesse, ignore or abuse the program have been rewarded, he said.

The panel will hold hearings this week on the latest example of this seeming paradox: Edward McCallum, the Energy Department's top internal critic of security deficiencies, has been put on leave and is being investigated by the Federal Bureau of Investigations for allegedly leaking secret information. At the same time, Wen Ho Lee, the former Los Alamos nuclear-weapons scientists who allegedly transferred many of the nation's most sensitive nuclear-weapons codes to an unprotected computer between 1983 and 1995, is described by the FBI as being ''unprosecutable.''

There is no evidence that China obtained any of the codes, although Mr. Lee met with China's weapons experts on two occasions during the 1980s and Chinese scientists were among the most frequent visitors to the lab.

The Commerce Committee has threatened to subpoena 13 Energy Department officials who know about the investigation of Mr. McCallum, a 25-year department veteran who, among other things, has complained about difficulties in trying to protect the secret computer system at Los Alamos. The network of 2,000 computers is used to store digital models of nuclear tests that show, moment-to-moment, how nuclear weapons work.

Committee members have invited Mr. McCallum to testify along with another department veteran, Glenn Podonsky, who runs internal inspections for the agency. While Republicans are leading the charge in the various congressional investigations, the two witnesses and others are expected to tell of foul-ups and budget shortfalls that date to the Carter administration.

Energy Department reports show that Mr. Podonsky, as early as 1994, had identified the problem that researchers could transfer data from the secured computer system to the unprotected one.

Over the weekend, Department of Energy officials said that a classified report prepared by U.S. intelligence agencies in November showed that there had been numerous efforts to penetrate the weapons laboratories' unclassified computer system. The secret report also noted that China was among a number of nations the laboratories should regard as a threat. Still, investigators didn't examine Mr. Lee's computer until March and didn't close down the classified system until last month. The report's findings were first published in the New York Times.

Brooke Anderson, a spokeswoman for Energy Secretary Bill Richardson, said the secretary ''is extremely concerned that the hearing may bring potential disclosures of classified information and his priority is to protect the national security.'' Mr. Richardson, a former member of the Commerce Committee, irritated its leaders after a security hearing last week, accusing the panel of ''exhuming the past.''

David Tripp, Mr. McCallum's lawyer, said the information involved in the allegations against Mr. McCallum wasn't classified and that he is being punished for being ''a pain in the neck'' about exposing security problems. Rose Gottemoeller, the assistant energy secretary who removed Mr. McCallum from his job, denied that was the reason, calling Mr. McCallum ''a valued security professional'' who has made ''major improvements.''

Despite substantial spending on ''gates, guards and guns,'' one problem that had received relatively little scrutiny is the so-called insider threat. As the Cold War has faded, the threat has grown because many Americans now shun careers in engineering, physics and mathematics—skills in demand at the weapons labs. The shortage forced the labs to turn to foreign-born experts who had become naturalized U.S. citizens, such as Mr. Lee, Taiwanese whose skills included modeling nuclear-weapons explosions on supercomputers.

[From the TelePort of: Ed McCallum, May 7, 1999]

To: Al Santoli.

Memo: This is draft and has not been given to DOE except verbally. It clearly shows there was no classified unless DOE wants to change the published rules./Ed

DRAFT

HERNDON, VA, *May 6, 1999.*

Subject: Classification Analysis of Rocky Flats Transcripts

Mr. JOSEPH MAHALEY,
Director, Office of Security Affairs, U.S. Department of Energy, Washington, DC.

DEAR JOE: Since I have not been given the opportunity to present my technical analysis of the classification decisions that I made during the subject discussions with the DOE contractor whistleblower, Mr. Jeff Peters, I will do so now. The presentation being made in this letter should have been part of the first step of the inquiry process described in DOE Manual 471.2–1B, 7a.(1), and should have been completed before proceeding with any inquiry. If both sides of a technical discussion had been laid on the table before the Department's classification authority, I firmly believe a determination would have been made at that time that the tape conversation and subsequently released transcripts were unclassified.

To date, six authorized classifiers have assessed the transcripts. Two areas of the conversation have been identified for further review. First, reference is made to ''20 percentile'' and ''80 percentile'', but no further context is provided by either speaker. Even if the reader can speculate the discussion relates to protective force computer modeling, no specific scenario is developed, no specific facility (e.g. building or vault, as stated in Topic 610 of CG–SS–3) is identified, and no specific attack developed.

DOE Classification Guide, CG–SS–3, Chapter 6, ''Vulnerabilities'', D. states clearly that information must, ''meaningfully aid a terrorist or other malefactor in targeting DOE facilities or bypassing security measures . . .''.

Vulnerability is defined in Appendix A, Definitions of CG–SS–3, as ''an exploitable capability or an exploitable security weakness. . . . If the vulnerability were detected and exploited by an adversary, then it would reasonably be expected to result in a successful attack . . .''. Clearly, no exploitable vulnerability is discussed within the meaning and intent of this classification guide that has been used by DOE for over 25 years.

The second area of conversation identified for review is the statement ''Put some HE on top of it and boost it up—you don't need to take it in the middle of Denver, it's going in the middle of Denver anyway.'' This portion of the conversation refers to a radiological dispersal device. CG–SS–3, Chapter 3, ''Malevolent Dispersal of Radioactive Material'', provides detailed guidance for classification in this area:

Paragraph C, states that for information to be classified it must be,'' . . . detailed,

specific information that, if not controlled, would significantly enhance the probability of such a dispersal''. Further elements of the same paragraph require elements such as ''Details of specialized access procedures to areas or equipment . . .''. ''Detailed scenarios (combining details of radioactive source type, size and form; container design; dispersal mechanism design) . . .''

Topic 1101.1 states specifically ''Trivial or generally known methodology'' is *Unclassified*.

Topic 1030, ''Design of credible Radiation Dispersion Device (RDD), states a design is ''Unclassified for unsophisticated designs.''

Topic 1052 cites ''Generic description of methods that could be used to disperse radioactive material (e.g., fire, *explosives*)'' as Unclassified.

Special nuclear materials discussed in the conversations have been publicly associated with the nuclear weapons program and included in Section 51 of the Atomic Energy Act of 1954. They are defined as ''Pure Products'' and as ''High-Grade Materials'' in unclassified DOE Regulations and in CG–SS–3.

Further, information concerning radioactive source term and scenarios of worst case dispersal with consequence estimates are contained in great detail in Safety Analysis Reports for each site. These reports contain worst case scenarios for radiological releases. They are unclassified, published and available in DOE Public Reading Rooms and periodically on the internet.

I know of no other issues that have been reviewed or could be considered even close to classified information. Further, I was given a 30-minute briefing on Defense Programs weapons design program(s) in the past. Nothing I have seen or heard of these programs would void or invalidate the published guidance in CG–SS–3.

I firmly believe that I have not disclosed classified information and have not crossed any boundaries, real or imagined. In no case were details or specifics provided any reader. Speculation might cause a reader to draw conclusions that are completely external to these illegally recorded conversations. The transcripts have been reviewed by a number of authorized classifiers and all have reached the conclusion that the conversation does not contain classified information and in no way crossed any prohibited boundaries.

I believe I have seen a rush to judgment on this classification issue and subsequent actions that violate the procedures published in DOE classification guidance and DOE Manuals relative to the investigation of a potential compromise. If the basic elements of ''due process'' had been followed this would have only been a technical discussion with possible clarified technical guidance provided by one side or the other. In closing, if Defense Programs believes these elements are so sensitive, then why weren't adequate physical protections immediately put in place to allay their concerns?

Sincerely,

DEPARTMENT OF ENERGY,
Germantown, MD, February 3, 1999.

Memorandum for Joseph S. Mahaley, Director, Office of Security Affairs

From: Edward J. McCallum, Director, Office of Safeguards and Security

Subject: Hagengruber Study.

I have completed my initial review of the subject document and offer the following impressions. These thoughts are not intended to be all inclusive, nor do they address all of the facts that I find questionable. In this regard, I have directed the Office of Safeguards and Security (OSS) Program staff to conduct a thorough review of the entire report with respect to its factual accuracy. Upon completion of this review, detailed comments regarding factual inaccuracies will be forwarded. Beyond the factual accuracy of some of the items found in the report, however, it is evident that this study not only misses the mark of the task assigned, but if left unchallenged could serve to damage the Department's standing in the security and intelligence community at large.

In reading the report, I am struck by the elementary understanding it portrays of the Safeguards and Security (S&S) Program, specifically as it relates to the national level directives that provide much of the foundation for many of the areas called into question. There is no mention of the Presidential Decision Directives (PDD) or the requirements contained therein governing federal agencies and their policies toward counterterrorism, explosives detection, radiological sabotage, and chemical/biological weapons defense. In fact the assertions offered are in direct contradiction to President Clinton's policy on Counterterrorism promulgated in PDD–39. For a study that spent the better part of a year examining the Department's S&S Program, I find this glaring omission of national policies to be alarming. Furthermore, it conveys a lack of understanding of the environment in which the Department operates that consequently diminishes the value of any findings or recommendations.

Beyond the lack of depth of understanding of S&S Program requirements, however, I find the team failed to answer the only question that was posed to them. Specifically, whether current—DOE practices ensure that Special Nuclear Material (SNM) and Nuclear Weapons are adequately protected against Raidological Dispersal Device (RDD) and Improvised Nuclear Device (IND) threats. The short statements in the report that we need to change policies to require a higher standard of protection of SNM is gratuitous and provides no new information. The single graphic depicting greater quantities of explosives relative to SNM types was recognized long ago when the Atomic Energy Commission began this program, and again in 1988 when the graded safeguards table for SNM protection was established. I was disappointed to find that the validation of specific time lines of existing guidelines currently in the Secretary's office awaiting completion of this study were completely avoided.

Equally disappointing is the amount of effort and detail directed at the management and organizational issues that have been previously reported in numerous studies to include your Report to the Secretary of October 1997 and the OSS Annual Report to the Secretary of January 1997. That the fragmented and divisive S&S structure is difficult to manage is well acknowledged and has been addressed repeatedly by DOE through reorganization and restructuring (e.g., SAI 26). There is no new information here, and the recommendations offered are confusing and inconsistent with one another. The solution as I understand it would further decentralize authority and responsibility to field sites thereby recreating the exact same environment as existed in Counterintelligence prior to the issuance of PDD 61.

The report wades through a plethora of symptoms and offers the often repeated Laboratory rhetoric to limit Headquarters involvement and trust the contractor to carry out the government's mission. Trust is not the question, execution is. As you know, cost is an essential element of risk management. The House of Representatives, Committee on Commerce, Oversight and Investigations Subcommittee challenged the DOE on the oversight of its contractor's S&S programs throughout the 1980's and early 1990's. Senator Glenn asked the same questions in Senate, Government Affairs Committee hearings. These facts are either unknown or ignored by the report team. I have yet to hear an allegation that DOE provides too much oversight of our contractors except from the Labs. Consequently, the suggestion that S&S should be funded through a site's overhead budget is simply irresponsible. It is unclear to me how this would be the preferred method of funding. Such a move would further remove the Department's control over this critical area. It is precisely this approach to safeguards and security as an ''overhead'' function that has led to many of our difficulties. It further underscores the lack of understanding of the mission essential element of safeguards and security as it relates to the Department's overall mission. It is precisely this type of thinking that Admiral Crowe's January 1999 report on the embassy bombings in Nairobi and Dar Es Salaam warns against. In his cover letter to Secretary Albright he expresses concern about the ''. . . relative low priority accorded security concerns throughout the US government—by the Department, other agencies in general, and on the part of many employees both in Washington and in the field.'' Admiral Crowe goes on to advise that, ''Saving lives and adequately addressing our security vulnerabilities on a sustained basis must be given higher priority by all those involved if we are to prevent such tragedies in the future.''

Again, this lack of understanding leads to another distrubing assertion found in the report. Specifically that: ''Safeguards and security is not a mission of DOE. Rather, safeguards and security is the responsibility of the DOE and contractor management at individual sites.'' Such a statement is contrary to Department of Energy's Strategic Plan of September 1997. Under the Strategic Plan's National Security Strategic Goal is the objective to ''ensure the vitality of DOE's national security enterprise.'' In support of this objective is a strategy to ''ensure the protection of nuclear materials, sensitive information and facilities.'' The fact that safeguards and security is found in the Strategic Plan as well as in the Secretary's Performance Agreement with the President clearly raises its level of import to more than ''a requirement of operation.''

A final point worthy of note is the complete lack of understanding of the Department's Design Basis Threat (DBT) process. The FBI, CIA, DOE, and the military services as well as the Nuclear Command and Control Staff have developed the existing Design Basis Threat over a number of years. It has been extensively reviewed and supporting studies issued by the DIA. Sandia, as well as our other Labs, have been asked to comment and participate in the development process. To describe the process and approach as flawed further underscores the superficial nature and questionable analysis found in the report.

Perhaps most distressing is the lack of balance in its approach to the critical safeguards and security issues facing the Department. Rather, what is provided is a very parochial Defense Programs/Laboratory view that ignores not only the external drivers found in national level policies, but a total lack of understanding of specific procedures implementing these policies. Suffice to say, I am strongly opposed to the continued funding of Phases II and III of this effort. If Phase I is any indication of the quality of effort that might be expected, any further funding in this regard would be imprudent at best. Nonetheless, if the program is continued, I strongly suggest we manage the direction and quality of the next phase.

As stated in this and other studies, successful resolution of the issues facing this

Department relative to safeguards and security will require a concentrated effort on the part of all interested parties to include the Office of Defense Programs and the National Laboratories. What concerns me is that critical information concerning these issues is missing from this study. While such an omission may serve certain short term interests, it is not in the best interest of the Department or the nation. As an agency, we must endorse and implement two significant objectives concerning our protection strategy: (1) to protect our nation's critical assets from those who would cause our nation harm, and (2) to protect the forces that secure our facilities from unnecessary vulnerability. To do any less is to undermine our national security responsibility, which is without question, a core mission of this Department.

Mr. WELDON of Pennsylvania. Madam Speaker, Mr. McCallum has been punished and has been placed on administrative leave and may lose his job. Guess who now sits on the corporate board of directors, being paid, overseeing the operation of that same facility? You guessed it, Madam Speaker. Hazel O'Leary. Hazel O'Leary now sits on the board of directors of the company that oversees the Rocky Flats facility that Mr. McCallum attempted to bring to the attention of the Congress was being protected in a woefully inadequate way. What is the response of this administration? To make him the scapegoat.

It is a shame that he did not precede Notra Trulock, because as many of my colleagues know, it was Notra Trulock who began to blow the whistle on this administration for not paying attention in 1995 to security breaches that were occurring in the Department of Energy. But Notra Trulock lucked out. Because when the administration realized that what Notra Trulock was saying was true, they could not go after him. They gave Notra Trulock a $10,000 bonus and now Notra Trulock is on national media programs and talks about how the administration has gotten its act together.

It is a shame that Mr. McCallum did not precede Notra Trulock. Perhaps he would have gotten the $10,000 raise for being the whistle-blower. I can tell my colleagues, Madam Speaker, I am not going to sit by, and neither are a number of our colleagues, and see an innocent individual doing his job professionally be railroaded out of his position because this administration is embarrassed over the policies of their lack of control and decontrol in security measures involving our national laboratories, our Department of Energy facilities, our defense installations, and our military and other technology.

The American people, Madam Speaker, can now read the statement of Mr. McCallum for themselves in tomorrow's CONGRESSIONAL RECORD. The American people also now, Madam Speaker, can read information I provided last evening giving the big picture of the China connection. I want to review that again today in some more detail.

As a member of the Cox committee, I had the opportunity, over the 7 months that we worked aggressively on this project, to meet a number of senior and very capable intelligence officers and people within our intelligence establishment who are absolutely frustrated by what they see occurring in this administration on security issues. When we completed the Cox Commission report, I knew that the American people would not sit through and read, for the most part, a document that is almost a thousand pages in length. Very difficult to understand.

So working with this group of people, and I would add for the record, who are today currently employees of this administration, so I cannot name them because they will be given the same treatment as Mr. McCallum has been given, these people have given me the information that I am providing to our colleagues and to the American people.

This chart, Madam Speaker, for the first time, even though it looks like a hodgepodge of blocks, it can be pulled down on the Internet site, as I have said earlier, and this site is www.house.gov/curtweldon. This document gives the full pictorial representation of what we think China had planned to acquire western technology.

Now, should we fault China for establishing this network? Probably, yes. But as many have said, what country does not spy or look to acquire technology from other countries? I would say we are the fools if we are stupid enough to allow China to access information that we should be controlling. And that is why I think the bulk of the responsibility here, Madam Speaker, lies with our own government. It was our government that failed the American people.

This chart outlines the Central Military Commission of the People's Liberation Army of China. The red boxes on this chart, which are too difficult to read without having the chart directly in front of you, are the various military commands and entities that are a part of the Central Military Commission that we know have been involved in engaging and in acquiring technology for China. Now, some of that acquisition has been legal, and there is nothing wrong with that. If they can buy it, how can we fault China for buying things we are legally willing to sell them or other countries will sell them? Some of it was not legal. By and large, though, much of what they got, they got through legal manipulation that we allowed to occur.

The green boxes are those entities and banks and financial institutions here, in Hong Kong and Macao, as well as in Europe and Asia, that were designed to fund the acquisition of these technologies. Now, because they could not buy them directly, front companies were established, and they are the blue boxes. We estimate there were hundreds and hundreds of front companies established by the Chinese to acquire technologies, paid for by these entities, to go to the arms of the People's Liberation Army, because that is a desire they had for these specific technologies.

A very elaborate scheme, but very simple. The financing through the entities to buy it go back to those entities that wanted to improve their missile systems, their nuclear programs, their computing capabilities, the design of their fighter aircraft, whatever the need might be. Again, if we are stupid enough to sell sensitive technology, how can we just blame China for buying it in the open market? This was the network.

Now, we can see that what we did not look at in the Cox committee is what influenced these people to allow this technology to flow. Was it money, was it influence, was it a desire to increase economic activity for American companies? What was the motivation? We did not look at that in our China committee effort. We thought that should be a follow-on once we determined that there was security harm done to our country. That is why I prepared this document and the document I am going to follow up with.

There are some connections here, Madam Speaker, that the American people need to look at, because some of these green boxes have attached to them campaign donations. Ted Sioeng, $200,000 to $400,000 to the Democratic National Committee. Or John Huang and James Riady, and all of these people who contributed millions of dollars to the Democratic National Committee. Or the temple that gave, through Maria Hsia, $50,000 at a fundraiser at a temple of impoverished religious leaders. Those connections need to be pursued.

This information, Madam Speaker, has been investigated much more thoroughly by the FBI and the CIA than I have. Now, I have seen some of the classified versions of this, which are far more elaborate, which I obviously cannot show publicly. What I have shown here is an unclassified version of the connections between these agencies that have been publicly identified. And in response to a question by a Member of Congress at a public hearing, Louie Freeh, the director of the FBI, was asked: ''How much of the information that we are aware about in public form, like this, compares to what you know in the FBI and the CIA about what happened in this entire series of transactions?'' This was the response of FBI director Louie Freeh. ''The public knows about 1 percent.'' One percent of what went on that we have in the FBI and the CIA in terms of these connections. One percent, Madam Speaker, which means that 99 percent beyond this our intelligence and our law enforcement agencies know about but we do not.

□ 2215

Madam Speaker, the individual that Louis Freeh assigned to investigate this, Charles LaBella, when he got

through all of this evidence, well beyond what I have, wrote a memorandum to Louis Freeh that I have been told is almost 100 pages in length. That then resulted in Louis Freeh sending a memo to Janet Reno saying there is enough evidence here that you better impanel a special investigative effort, an independent counsel, because of what may be here. Janet Reno refused Louis Freeh and refused Mr. LaBella. That document has never been released to the Members of Congress nor the American public. In fact, I am not aware of any Member of Congress that has read that memo. But I can tell you, Madam Speaker, every Member of this body and every citizen in America should demand of this President one thing, and, that is, to release the LaBella memorandum. If this President and Vice President GORE have nothing to hide, if there are no connections, if there is no scandal, if there is no grand scheme, if there are no implicating factors, it can all go away very quickly by releasing the LaBella memorandum. That document has been subpoenaed by the Congress and it has been refused by Janet Reno to be turned over to us so that we have not had the opportunity to see what Charles LaBella said was there in that 99 percent of information that we do not know about. What I have given to the American people is the unclassified information that they can read, and it in itself is revealing. In fact, Madam Speaker, you will notice there are lines connecting many of these boxes. The solid lines indicate direct working relationships between the PLA entities, the financing entities, and the front companies. So they are directly linked. The dotted lines, which are fewer in number, are those where there is a loosely connected relationship but not a direct relationship. Now, the logical question is, ''Well, hold it, Congressman, you can't just draw lines. You've got to provide some documentation.'' Well, we did. Again working with existing employees of this government who have been frustrated by what they have seen occurring have helped me identify 26 documents that are available on the public record that are not classified, that include newspaper articles, research documents, business reports, company annual reports where you can connect the lines. Each of the numbers on this chart which corresponds with a line gives you a specific document that you can read which I have outlined and identified in the CONGRESSIONAL RECORD yesterday which you can get off of my web site which gives you the public information that supports the linkage between these various entities. It is public information. Now, that is not all. And the media when I brought this out last week said, ''Well, wait a minute, you haven't established a direct relationship.'' I cannot show classified information here. That is a violation of our Federal laws. I have given unclassified documentation which without a doubt shows the connections between the major players in the effort to allow China to acquire technology that they have been wanting to buy.

Now, the administration would have us believe that this is really all concocted by China and that we should make China the evil empire. I am not doing that, Madam Speaker. I cannot blame China if decisions made by this administration allowed technology to flow legally, and that is what occurred in most cases. The influence that was peddled by these financial people ended up lowering the controls over our regulation of technology being sold abroad. The influence exercised by these people and their money influenced key decisionmakers in this administration. In my opinion, that lies in terms of fault at the feet of this administration itself. And as much as we would like to totally blame China, I blame our own government.

Now, are there instances where China went too far? Absolutely. And I would say this again on the record. If we can document that there is direct espionage that took place at our labs or at other facilities, we should use the full force of our law to prosecute those people who in fact spied on America, much like we have done in the past. But we cannot blame a country if we willingly sold them the bulk of this technology because of influence they were able to get by putting some money around or by currying favor with certain people.

Let me go to the second chart, Madam Speaker. The second chart, which was also prepared with the help of existing employees that work for this government who are in sensitive positions, gives the time line, the time line of liberalized and decontrolled technologies to the People's Republic of China. But I want you to know, it was not just China that benefited from these policies. Many of these policy decisions benefited a number of countries who were able to legally buy our technology.

Now, I am not against our companies selling technology abroad. In fact, I am an advocate of our companies being able to sell and compete in the world marketplace. But, Madam Speaker, that is not what occurred here. What occurred here was the elimination in a wholesale way of a legitimate process that was in place under previous administrations to monitor technology and to do it with our allies. As I mentioned last night, the reason I started this chart in 1993 was not because that is when Bill Clinton took office, it was because in 1993 this President ended a process called COCOM. COCOM was an organized group of our allied nations and Japan that met on a regular basis to monitor sensitive technology that was produced in any one of the allied countries. There was an agreement that none of those COCOM nations would sell sensitive technology to countries that we thought might use it against us, so that none of our companies were hurt because all the countries that have this technology were working together so that no one could benefit.

It was this administration in 1993 that unilaterally decided to end COCOM, did away with it. Without even consulting with our allies, we said, ''We're doing away with this process.'' From 1993 on, the floodgates opened. Because now you had companies in Great Britain and France and Japan who said, ''Wait a minute, there's no more COCOM, we're not going to let the U.S. sell this technology abroad, we're going to sell competing technology.'' So now you had a mad scramble, you had American companies trying to keep up with German, French, Italian, British and Japanese firms who now saw American companies selling technologies that under COCOM they could not sell. So the European countries and Japan said, ''Wait a minute, we're going to sell that technology as well,'' and you had a mad scramble to sell technology in a totally uncontrolled fashion. That began in 1993 under this administration. The Commerce Department will tell you it was good for business. Some business leaders will tell you it was good for business. We on the Cox Committee will tell you it was bad for America. Other allied nations will tell you it was bad for international security. Proliferation has never been worse than it has been for the past 6 years. Iran, Iraq, Syria, Libya, North Korea, India, Pakistan, all have cutting-edge technologies that up until 1993 were tightly controlled by COCOM, all of that ended by this administration. That is the focus of the Cox report.

The chronology of this chart takes each technology separately: warhead design, machine tools, low observable technologies, telecommunications, propulsion systems, high-powered computers, encryption technology, space launch technology, and analyses when key decisions were made by this administration and gives you the month and the date that allowed technologies to flow that up until these dates were controlled. And you can see by the number of red dots here that during this time frame, the floodgates opened. We said, ''We'll sell anything and everything and we won't consult with our allies.'' So you have had a mad competition among companies in countries that up until 1993 worked together to make sure that no one could unfairly have a larger share of the market with sensitive technologies. After 1993, the demise of COCOM, the floodgates opened. Everything and anything was for sale. Our companies got their way, they got to sell whatever they wanted, foreign countries and companies the same thing, and China took advantage of it.

Now, there are some interesting other factors about this chart, Madam Speaker. You will notice a gray area in the center of this chart, starting in 1995, ending in 1997. Why did I make that gray? Because in 1995, we have been told by Bill Richardson that this

administration found out that China was acquiring our most sensitive technology. And if you listened to Secretary Richardson, this is what he said: ''Boy, when we found that out, we took aggressive action. We said, 'We're not going to let China steal our technology.'''

Well, that is what he said. The color in the blue, Madam Speaker, and all the red dots you see here, just under Space Launch alone, 15 separate actions after this administration knew that China had stolen our design technologies that they took in 3 years to give more technology to countries like China. And that is across the board, Madam Speaker. So the blue indicates where this administration knew that China was trying to acquire this technology and doing it illegally, opened the floodgates even further for more technology.

There is one more factor here, Madam Speaker. All of us in America know when the elections were held. It is kind of interesting when you look at this chart from a distance that the bulk of the clustering of these dots are in and around the time frame of 1996. I wonder what was happening in that year, Madam Speaker? Might that have been the year when the presidential elections were being held? Could there be some coincidence that many of these key decisions in terms of policy changes were being done because elections were being held and maybe people were interested and from the standpoint of corporate America in having policymakers make determinations to allow more products to be sold overseas, could that be a reason? That is what the LaBella memorandum referred to, Madam Speaker, that this country needs to see for itself, the reasons why these decisions were made. Why did we change our policy so much? Why did we allow access? Why did we totally decontrol technologies in a way that was not being aware and cognizant of our own security concerns?

But it goes beyond these issues, Madam Speaker. Let us move down to this next item here. PRC Nationals to U.S. High Tech Companies. It was in 1994, in fact it was in March, that Chinese nationals to our U.S. labs and our U.S. high tech companies was allowed. The COMEX review of foreign nationals was abandoned, by this administration. That was in 1994. I am sure that was done because the companies wanted less hassle of foreign nationals going into our high tech companies. And over here in 1997, we revised our deemed exports policy to allow foreign nationals to work at U.S. high tech companies. Now, that was in 1997. These were decisions made that allowed more Chinese nationals to work in our high tech companies in America. And how about the high tech furnace approval for weapons of mass destruction? That approval was given in 1998, Madam Speaker, a technology that gives China capability for the production of weapons of mass destruction. Even though this administration said when they found out about the theft of nuclear secrets, they took aggressive action to control it.

Let us go down further, Madam Speaker. During this same period of time, China and Russia were both violating international arms control agreements. The Missile Technology Control Regime, the control of exports. We caught them on a number of occasions. In fact, in last night's special order, and again the American people can read this through my web site or get a copy of it through the CONGRESSIONAL RECORD last evening—and I did not do the work, the Congressional Research did the work—we documented the arms control violations that we caught Russia and China involved in over 6-year time period. Here is that chronology as documented by the Congressional Research Service.

□ 2230

The dates, the type of transfer, who the transfer went to are all documented. This was not done by some partisan group; it was done by the Congressional Research Service, a part of the Library of Congress.

These violations of arms control agreements by China, were they sent technology? Where did they send the technology to? Let us look at the chart.

Well, they sent technology to Pakistan, Iran; Iran? North Korea. Syria. They sent solid propellant production technology to Libya, Iran, Egypt. They sent missile accelerometers and gyroscopes to Iran, Syria, Libya, Egypt and Pakistan. They sent antiship missiles to Iran. They sent more material to Pakistan; chemical weapons technology to Iran again.

All of these transfers done by China.

What was the response of this administration? Nothing.

On, yes, two times out of about 17 or 21, I forget which it is, they did impose temporary sanctions; but they eventually waived them.

So not only are we getting Chinese access in a way they never had access before, not only were we helping to expedite and grease the skids for the financing of the purchase of technologies, but we were ignoring violations of arms control agreements that China was required to abide by. We did not call them on these violations.

And at the bottom of the chart, Madam Speaker, even though I could not complete it, I was only able to do this up through 1996, I list a number of times that the major players in the Chinese financing scams visit at the White House, not visited Members of Congress, but were in private visits in the White House itself.

In the case of John Huang, in the one year of 1993 alone, we know of 12 times he was in the White House. In 1994, twice; in 1995, let us see, one, two, three times; or 1994, three times; 1995, three times. These are people that are involved in that elaborate scheme of organizations and financing entities that were given direct access to our White House, to our top policy maker to our commander in chief, to our key leaders who were then being pressured to relax our policies relative to technology being sold abroad.

Madam Speaker, these two charts represent the pictorial view of the Cox committee report. They represent what needs to be explored further.

I am not here as a partisan, Madam Speaker. Both times I ran for mayor of my hometown I was the nominee of the Republican Party and the Democrat Party both times I ran. I work with many Democrats in this body and frequently get up on the floor of this House and praise our Democrat colleagues for their leadership role on defense and security issues. I have joined with members of the Democrats on a number of key issues involving social policy, family medical leave, environmental policies, protection for our workers, and I have supported the President and the administration in some of those issues which my party has not been supportive of. But, Madam Speaker, when it comes to national security, we have a big problem here. This needs to be looked at beyond the Cox committee.

To me, I know why in my mind Janet Reno turned down the recommendation of Louis Freeh based on the memos sent by Charles LaBella to appoint an independent counsel. I am convinced, Madam Speaker, the evidence is there. I am convinced that 99 percent that we have been told we have not seen yet has far more than many people in this country want to become public.

I am also convinced, Madam Speaker, that we had better pay attention here. This is not some story about a dress, this is not some intern in the White House. This is not some story about a travel office. This is not even about Republicans or Democrats. Madam Speaker, this is about the very core of what our country is about. No one, no party official in either party, no elected leader, has the right to allow a wholesale technology faucet to open that we are going to have to pay the price for.

Now, if I am overreaching, Madam Speaker, I do not think I am because, a member of the Cox committee having sat through as many of those meetings as any one of my colleagues, with perhaps the exception of Chairman Cox himself, I know what evidence the FBI and the CIA has, and I have only seen a small fraction of what is not on this chart. I know there is much more.

If there is nothing there, Madam Speaker, the President can clear this entire issue up in a heartbeat. All he has to do is release the entire unabridged version of the Charles LaBella memo to Louis Freeh. If there is nothing to hide, if there is nothing to these connections, if there is no story, I will be happy.

I do not think that is the case, Madam Speaker. I think the reason

why Janet Reno did not accept Louis Freeh's recommendation, based on LaBella's memo, is because she knew what is there. That document that LaBella prepared, which I understand is quite voluminous, goes into extensive detail and actually points to individual people.

Madam Speaker, this country, this democracy, needs the American people and its elected officials to see the overview of the evidence that LaBella gave to Freeh that now remains closed and confidential. If there is nothing there, then there is no problem with the memo; if there is no evidence, if there is no story, if there is no substance, the whole thing will go away, and the China story will end, and we will make the necessary corrections to our own policies.

Madam Speaker, I would encourage every one of our colleagues and every constituent in every district of a Member of this body and the other body to demand that this administration do one thing: release the full text, the uncensored text, of the Charles LaBella memorandum to Louis Freeh. Let us see what evidence they thought may be there in terms of a greater scheme for the Chinese to acquire technology by facilitating and greasing the skids of certain key people and certain key agencies that ended up with America's security being harmed. That was the unanimous vote of all nine members of the Cox committee, that America's national security has been harmed by the actions that we investigated in the Cox committee work.

We cannot just stop with this document, and we cannot rely on the mainstream media because with the exception of a few people like those that I have mentioned and some others, the mainstream media is too stinking lazy to go through the investigative details necessary to uncover what is here. We need to have this administration come clean, give us the uncensored text of what Charles LaBella said to Louis Freeh which only went to Janet Reno. When that happens, we will then know the true extent of the China connection and its impact with this administration.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore (Mrs. BIGGERT). The Chair will remind Members to refrain from making personal references towards the President.

INTRODUCTION OF LEGISLATION TO DENY COMMUNIST CHINA NORMAL TRADE RELATIONS STATUS

The SPEAKER pro tempore. Under the Speaker's announced policy of January 6, 1999, the gentleman from California (Mr. ROHRABACHER) is recognized for 60 minutes.

Mr. ROHRABACHER. Madam Speaker, first of all, I would like to commend my colleague, the gentleman from Pennsylvania (Mr. WELDON). We have worked together over these last 10 years while I have been a Member of Congress on many, many occasions, and I find Congressman WELDON to be a patriot, a man of integrity, a man of courage, and I think when all of this is said and done, when we find out the jeopardy that our country has been put in and take the measures that are necessary to correct this situation and to make our country safe again, the gentleman from Pennsylvania (Mr. WELDON) will be on the list of real American heroes that came about to save the day, and I am just proud to serve with him.

Madam Speaker, tonight it is fortuitous that I will be speaking after the gentleman from Pennsylvania (Mr. WELDON) because my remarks are in parallel with what Mr. WELDON has been talking about. It goes into a slightly different subject. Tonight I will be talking about Most Favored Nation status and our economic, as well as military and diplomatic, relations with China. But of course everything that Mr. WELDON has said today amplifies the need that I will be demonstrating for us to reexamine American policy towards Communist China.

In fact, let me state right at the beginning that when it comes to Communist China, we have been treating a hostile power, the world's worst human rights abuser, as a strategic partner, that is what this administration has insisted on us calling Communist China, and I believe that Americans will pay a woeful price for this irrational, amoral and greed-driven policy if we do not change it, and that is what we need to do to change that policy that has been in place to some degree or another for 2 decades, but especially in these last 6 years.

Yesterday I introduced legislation to do just that, to change that policy. It is a bill of disapproval of extending so-called ''normal trade relations,'' which was previously known as Most Favored Nation status, with Communist China. So what my proposal is is that we deny Communist China normal trade relations status with the United States, formerly called Most Favored Nation status.

The time, Madam Speaker, is long since past when the United States should reexamine its fundamental policies toward the Communist dictatorship that now rules the mainland of China. Our commercial policies, as well as our diplomatic and military policies, for the past decade have worked against the interests of our own people and have not, as we had hoped, increased the level of freedom enjoyed by the Chinese people. In fact, some of the initial progress that we saw in China has now gone in the opposite direction, especially since the end of the Reagan administration and the tragic national reversal in China in 1989 at Tiananmen Square when they had the massacre at Tiananmen Square.

The gentleman from Texas (Mr. ARMEY), one of our Republican leaders here in the House, defines ''insanity'' as doing more of the same, but expecting the results to be different. Well, for 10 years the cause of freedom in China has been in decline. Things are getting worse. So much for the engagement theory, the strategy of engagement, and what we hear from those people advocating normal trade relations and to continuing our relations with China is doing more of the same, but expecting that China is going to be different, that there will be different results now.

Well, that makes no sense. It is the unreasonable and perhaps irrational optimism of some people to assume that continuing our fundamental policies toward China will bring about different results than the retrogression that we have seen in the past decade.

In the past 10 years, the genocide, for example, has continued in Tibet. The Chinese democracy movement has been wiped out, and there has been increasing belligerence by the clique that runs China. The Beijing regime is modernizing and expanding its military power while threatening the United States and bullying its neighbors, especially in Taiwan and the Philippines.

Big business falsely claims that China is a country that is liberalizing through commercial engagement. There is no evidence for that claim. So every time you hear it: Well, we have got to engage them, that is what will make them better; just be aware that there is every evidence to show just the opposite. In fact, the empirical evidence shows that China is going in the opposite direction, that engagement is not making things better, is not causing a freer China, but instead for the last 10 years has resulted in more repression, more militarization.

Furthermore, the trade relationship is working against the people of the United States. So here we are in an economic engagement that is not helping us bring about a freer China, thus, less belligerent, thus a China that will be more peaceful. It is not doing that, but it is also not even helping us economically.

□ 2245

The Chinese are using their $60 billion annual trade surplus with us to modernize their Armed Forces, including building nuclear missiles aimed at the United States, and they are continuing to proliferate weapons of mass destruction. For example, Communist China is reported to be the power behind North Korea's space program. Get into that.

North Korea has a space program. This is a country that has people who are starving by the thousands, that we are giving millions of dollars worth of food aid to, but they have a space program? You got it. Communist China is helping the North Korean regime with a so-called space program. In other words, they are helping them build