HEINONLINE

Citation: 4 Bernard D. Reams Jr. Law of E-SIGN A Legislative of the Electronic Signatures in Global and National Act Public Law No. 106-229 2000 iii 2002

Content downloaded/printed from HeinOnline (http://heinonline.org) Sun Apr 21 21:28:43 2013

-- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from uncorrected OCR text.

NATIONAL SECURITY AND DEFENSE ISSUES (House of Representatives - September 04, 1997)

[Page: H6909]

The SPEAKER pro tempore. Under the Speaker's announced policy of January 7, 1997, the gentleman from Pennsylvania [Mr. **Weldon]** is recognized for 60 minutes as the designee of the majority leader.

Mr. WELDON of Pennsylvania. Mr. Speaker, I rise this evening to discuss several defense issues, but before discussing those issues, I would like to follow up on the previous special order that we just heard, since many of our colleagues perhaps in their offices, and citizens around the country, have been listening to three of our colleagues discuss education.

Mr. Speaker, I want to, first of all, applaud the gentleman from Texas [Mr. **Green]** because I heard him use the word `bipartisanship' a number of times in reference to education success. I want to applaud him, because I want to distinguish my colleague from Texas as opposed to the other two Members from whom we heard nothing except the phrases `Democrats, Democrats, Democrats.'

Now, I do not know what amount of classroom teaching experience my colleagues that spoke have. I spent 7 years in the public schools of Pennsylvania, was active in my education association as a vice president, was a negotiator for a while, was involved in running a chapter 1 program in an impoverished area in my county. So my experience is based on real life. I am not one of the attorneys in this institution.

Mr. Speaker, Republicans have in the past, continue today, and will be in the future, in the forefront of working to improve our educational system in this country, and for some Member to stand up here for 50 minutes and talk about only one party has a market on what we need to do to improve our schools is an absolute outrage. It is really a shame, because I think it is a slap in the face to people like the gentleman from Pennsylvania [Mr. **Goodling]** who chairs our Committee on Education and the Workplace, who himself was a classroom teacher, a superintendent, and someone who was involved in education. Or the gentleman from Illinois [Mr. **Porter]**, who spent a significant amount of time working on education priorities.

The successes that we have had in this Congress have been bipartisan, and they have not been because of any one party. In fact, I would remind some of my colleagues who just spoke, and I again say with the exception of the gentleman from Texas [Mr. **Green]**, that it was the Democrat Party who for 50 years controlled this institution. In fact, the first 2 years of the Clinton administration the Democrats controlled the White House and both Houses of Congress.

Is not it amazing that those who would seek to be most partisan in this debate on education would now begin to take credit as a political aspect of the Democrats' agenda for what a Republican Congress has enacted in the last 3 years? It has, in fact, not been a Democrat win and it has not been a Republican win. It has been a bipartisan effort, as the gentleman from Texas alluded to, to bring Members of Congress together for the good of our children and the schools of this country.

Mr. Speaker, I take exception to some of the comments that were made, and as a classroom teacher who spent a number of years working to improve the quality of our children's educational

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [iii] 2002

opportunities, I am proud of what this party and this Congress has done, bringing Democrats in with us, to bring forth new initiatives and new ideas to help all of our schools across this great Nation.

Mr. Speaker, my real purpose tonight is to discuss several defense priorities that are going to be coming up and should be on the minds of our colleagues over the next several weeks. In fact, one issue is going to be coming before several of our committees. It already has, in fact, been an issue in the Committee on International Relations as well as the Committee on the Judiciary where a bill has passed and is now pending before the Committee on National Security, the House Permanent Select Committee on Intelligence, and the Committee on Commerce.

This bill, Mr. Speaker, is a very technical piece of legislation dealing with an issue that many of us have not focused on, and that is the whole issue of information.

One of our greatest challenges as we approach the 21st century is how to manage information and to make sure that we, in fact, can become smart cities, smart regions, and further utilize information technology to enhance the quality of the lives of our people.

Mr. Speaker, in that process, however, we face a dilemma. At a hearing that I chaired in March of this year as the chairman of the Subcommittee on Research and Development, I took testimony for 6 hours on the issue of information warfare, and I heard recommendations and reports provided to us that an adversary in the 21st century may not have to spend his or her dollars on sophisticated weapons systems or on bigger bullets or larger missiles or longer range technologies, but rather concentrate on using methods to compromise our information systems, to bring down our banking and financial systems, our mass transit systems.

Mr. Speaker, the recommendation coming out of that hearing from the Defense Science Board was that we should dramatically increase spending for information security and control by about $3 billion a year.

Mr. Speaker, we cannot afford to do that because that is just too much money. We made a modest increase in this year's defense bill and we are working to keep that modest increase in place to demonstrate new technologies to allow us to protect our systems in this country from the threat of an adversary taking them down.

But there is a piece of legislation that is being pushed on a fast track basis that would totally remove the export controls over encryption technology. Encryption, Mr. Speaker, as we all know, is the technology and the process used to code information so that when we have a conversation over the Internet, no one else can intercept that conversation.

There are very important principles in question here relative to the security of the people of this country having their ability to communicate and not having the Government or anyone else be able to have access to that.

Encryption provides that protection and, in fact, it is available in this country. However, the piece of legislation that is now under consideration, H.R. 695, which a number of our colleagues have cosponsored, would basically remove export controls and allow this technology in its most sophisticated form to be sent overseas.

Now, there are some in this country, and myself included, who have some concerns about the

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [iv] 2002

administration's current policy over encryption and want to see reforms that will allow our software industry to continue to be on the cutting edge of new technologies to encrypt information that, in fact, we will be using every day.

However, while I do not support the current policy of this administration, I cannot in good conscience support a total wiping out of any export control on technology that a cartel, a drug cartel, or an

adversary nation has been using and could be using to prevent our law enforcement, intelligence, and defense resources from protecting the American people from the threats of drug dealing, from the threats of intimidation, terrorist activities, or other activities of that type.

Mr. Speaker, I urge our colleagues to carefully review the impact that this legislation will have, first of all, on our national security and on our intelligence-gathering capabilities. In fact, everyone in fact in the administration concerned with defense intelligence has come out with grave reservations about this legislation.

Mr. Speaker, I have also received a letter from Secretary Cohen expressing his grave reservations about this legislation.

Mr. Speaker, on Tuesday, when the Committee on National Security marks up this piece of legislation, I will be offering an amendment that will enjoy the support of both the gentleman from South Carolina [Mr. **Spence**], chairman of the Committee on National Security, and the gentleman from California [Mr. **Dellums**], ranking Democrat on that committee, that hopefully will pass, that will deal with one-half of the issue and that is whether or not we should completely eliminate all export controls and export process to review encryption technology that would be sold overseas and marketed overseas.

I think it is a fair compromise. It does not, in fact, satisfy all of the industry groups who want to have no export controls, and it does not satisfy the administration, but it does give us an ability to have a process in place to continue to allow our Department of Defense to monitor the kinds of technologies that we allow to be sold to rogue nations. It is a very important amendment.

It also closes a loophole, Mr. Speaker, in H.R. 695 that, in effect, would allow supercomputers to be sold overseas if, in fact, they have encryption built in.

Now, this is kind of an ironic twist here, because many of the cosponsors of this bill voted for an amendment that criticized the administration for allowing Cray supercomputers to be sold to China and Russia. Yet, Mr. Speaker, in this very provision that some of them have unknowingly cosponsored, there is a loophole that would allow those same supercomputers, if encryption is contained in those supercomputers, to be sold overseas with no restrictions. I do not think that is the intent of most of our colleagues, and the amendment that I will be offering on Tuesday will correct that.

Now, I would also encourage our colleagues, Mr. Speaker, to try to get briefings from Louis Freeh, the Director of the FBI, who I had in my office today for 1 hour, or from the National Security Agency, on the domestic impact of a total elimination of controls over encryption.

Again, I am not happy with the administration nor am I happy with their proposal to establish what is called a key recovery system. But we do need to allow the law enforcement entities in this Nation, we

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [v] 2002

do need to allow the Justice Department, to go through the established system of our courts with court and judicial approval to gain access to gather data that can be used; for instance, in uncovering pedophiles who in fact have been using and continue to use our Internet to unknowingly get the attention and to communicate with young people through the Internet; or to get access to encrypted data that, in fact, has been used by drug cartels; or for instance, the group that was involved in the bombing of the World Trade Center in New York.

Our law enforcement community has to have some ability, through a very difficult and very well-thought-out process, to get the approval from our courts to get access to encrypted data for very specific purposes when the national security of this Nation and our people is at risk.

It is extremely important every law enforcement head in our Federal Government has, in fact, signed a letter to every Member of Congress stating their concern with this bill. I would also, Mr. Speaker, like to enter that letter into the Record.

Office of the Attorney General,
Washington, DC, July 18, 1997.

[Page: H6910]

Dear Member of Congress: Congress is considering a variety of legislative proposals concerning encryption. Some of these proposals would, in effect, make it impossible for the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Secret Service, Customs Service, Bureau of Alcohol, Tobacco and Firearms, and other federal, state, and local law enforcement agencies to lawfully gain access to criminal telephone conversations or electronically stored evidence possessed by terrorists, child pornographers, drug kingpins, spies and other criminals. Since the impact of these proposals would seriously jeopardize public safety and national security, we collectively urge you to support a different, balanced approach that strongly supports commercial and privacy interests but maintains our ability to investigate and prosecute serious crimes.

We fully recognize that encryption is critical to communications security and privacy, and that substantial commercial interests are at stake. Perhaps in recognition of these facts, all the bills being considered allow market forces to shape the development of encryption products. We, too, place substantial reliance on market forces to promote electronic security and privacy, but believe that we cannot rely solely on market forces to protect the public safety and national security. Obviously, the government cannot abdicate its solemn responsibility to protect public safety and national security.

Currently, of course, encryption is not widely used, and most data is stored, and transmitted, in the clear. As we move from a plaintext world to an encrypted one, we have a critical choice to make: we can either (1) choose robust, unbreakable encryption that protects commerce and privacy but gives criminals a powerful new weapon, or (2) choose robust, unbreakable encryption that protects commerce and privacy and gives law enforcement the ability to protect public safety. The choice should be obvious and it would be a mistake of historic proportions to do nothing about the dangers to public safety posed by encryption without adequate safeguards for law enforcement.

Let there be no doubt: without encryption safeguards, all Americans will be endangered. No one disputes this fact; not industry, not encryption users, no one. We need to take definitive actions to protect the safety of the public and security of the nation. That is why law enforcement at all levels of government--including the Justice Department, Treasury Department, the National Association of

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [vi] 2002

Attorneys General, International Association of Chiefs of Police, the Major City Chiefs, the National Sheriffs' Association, and the National District Attorneys Association--are so concerned about this issue.

We all agree that without adequate legislation, law enforcement in the United States will be severely limited in its ability to combat the worst criminals and terrorists. Further, law enforcement agrees that the widespread use of robust non-key recovery encryption ultimately will devastate our ability to fight crimes and prevent terrorism.

Simply stated, technology is rapidly developing to the point where powerful encryption will become commonplace both for routine telephone communications and for stored computer data. Without legislation that accommodates public safety and national security concerns, society's most dangerous criminals will be able to communicate safely and electronically store data without fear of discovery. Court orders to conduct electronic surveillance and court-authorized search warrants will be ineffectual, and the Fourth Amendment's carefully-struck balance between ensuring privacy and protecting public safety will be forever altered by technology. Technology should not dictate public policy, and it should promote, rather than defeat, public safety.

We are not suggesting the balance of the Fourth Amendment be tipped toward law enforcement either. To the contrary, we only seek the status quo, not the lessening of any legal standard or the expansion of any law enforcement authority. The Fourth Amendment protects the privacy and liberties of our citizens but permits law enforcement to use tightly controlled investigative techniques to obtain evidence of crimes. The result has been the freest country in the world with the strongest economy.

Law enforcement has already confronted encryption in high-profile espionage, terrorist, and criminal cases. For example:

An international terrorist was plotting to blow up 11 U.S.-owned commercial airliners in the Far East. His laptop computer, which was seized in Manila, contained encrypted files concerning this terrorist plot.

A subject in a child pornography case used encryption in transmitting obscene and pornographic images of children over the Internet.

A major international drug trafficking subject recently used a telephone encryption device to frustrate court-approved electronic surveillance.

And this is just the top of the iceberg. Convicted spy Aldrich Ames, for example, was told by the Russian Intelligence Service to encrypt computer file information that was to be passed to them.

Further, today's international drug trafficking organizations are the most powerful, ruthless and affluent criminal enterprises we have ever faced. We know from numerous past investigations that they have utilized their virtually unlimited wealth to purchase sophisticated electronic equipment to facilitate their illegal activities. This has included state of the art communication and encryption devices. They have used this equipment as part of their command and control process for their international criminal operations. We believe you share our concern that criminals will increasingly take advantage of developing technology to further insulate their violent and destructive activities.

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [vii] 2002

Requests for cryptographic support pertaining to electronic surveillance interceptions from FBI Field Offices and other law enforcement agencies have steadily risen over the past several years. There has been an increase in the number of instances where the FBI's and DEA's court-authorized electronic efforts were frustrated by the use of encryption that did not allow for law enforcement access.

There have also been numerous other cases where law enforcement, through the use of electronic surveillance, has not only solved and successfully prosecuted serious crimes but has also been able to prevent life-threatening criminal acts. For example, terrorists in New York were plotting to bomb the United Nations building, the Lincoln and Holland Tunnels, and 26 Federal Plaza as well as conduct assassinations of political figures. Court-authorized electronic surveillance enabled the FBI to disrupt the plot as explosives were being mixed. Ultimately, the evident obtained was used to convict the conspirators. In another example, electronic surveillance was used to stop and then convict two men who intended to kidnap, molest, and kill a child. In all of these cases, the use of encryption might have seriously jeopardized public safety and resulted in the loss of life.

To preserve law enforcement's abilities, and to preserve the balance so carefully established by the Constitution, we believe any encryption legislation must accomplish three goals in addition to promoting the widespread use of strong encryption. It must establish:

A viable key management infrastructure that promotes electronic commerce and enjoys the confidence of encryption users.

A key management infrastructure that supports a key recovery scheme that will allow encryption users access to their own data should the need arise, and that will permit law enforcement to obtain lawful access to the plain text of encrypted communications and data.

An enforcement mechanism that criminalizes both improper use of encryption key recovery information and the use of encryption for criminal purposes.

Only one bill. S. 909 (the McCain/Kerrey/Hollings bill), comes close to meeting these core public safety, law enforcement, and national security needs. The other bills being considered by Congress, as currently written, risk great harm to our ability to enforce the laws and protect our citizens. We look forward to working to improve the McCain/Kerrey/Hollings bill.

In sum, while encryption is certainly a commercial interest of great importance to this Nation, it is not solely a commercial or business issue. Those of us charged with the protection of public safety and national security, believe that the misuse of encryption technology will become matter of life and death in many instances. That is why we urge you to adopt a balanced approach that accomplishes the goals mentioned above. Only this approach will allow police departments, attorneys general, district attorneys, sheriffs, and federal authorities to continue to use their most effective investigative techniques, with court approval, to fight crime and espionage and prevent terrorism.

Sincerely yours,

JANET RENO,
Attorney General.

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [viii] 2002

LOUIS FREEH,
Director, Federal Bureau of Investigation.

BARRY MCCAFFREY,
Director, Office of National Drug Control Policy.

THOMAS A. CONSTANTINE,
Director, Drug Enforcement Administration.

LEWIS C. MERLETTI,
Director, U.S. Secret Service.

RAYMOND W. KELLY,
Undersecretary for Enforcement, U.S. Department of Treasury.

GEORGE J. WEISE,
Commissioner, U.S. Customs Service.

JOHN W. MAGAW,
Director, Bureau of Alcohol, Tobacco and Firearms.

--

--

Mr. WELDON of Pennsylvania. And finally, Mr. Speaker, I would like to ask our colleagues to please listen to the law enforcement community. For the last year, Members of Congress, especially those who have cosponsored this legislation, have heard from the software industry, the Microsofts and those companies that see dollar signs in terms of export sales that could grow astronomically. And I want to see them succeed, too. That is part of my ultimate goal. But we also need to listen to law enforcement.

Mr. Speaker, I would ask to include a letter signed by four of the major law enforcement groups in this country, including the District Attorney's Association, the Chiefs of Police, and others, expressing their strong reservations about a total elimination of our ability to deal with encryption as it relates to law enforcement.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE,
Alexandria, VA, July 21, 1997.

Dear Member of Congress: Enclosed is a letter sent to you by the Attorney General, the Director of National Drug Control Policy and all the federal law enforcement heads concerning encryption legislation being considered by congress. Collectively we, the undersigned, represent over 17,000 police departments including every major city police department, over 3,000 sheriffs departments, nearly every district attorney in the United States and all of the state Attorneys General. We fully endorse the position taken by our federal counterparts in the enclosed letter. As we have stated many times, Congress must adopt a balanced approach to encryption that fully addresses public safety concerns or the ability of state and local law enforcement to fight crime and drugs will be severely

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [ix] 2002

damaged.

Any encryption legislation that does not ensure that law enforcement can gain timely access to the plaintext of encrypted conversations and information by established legal procedures will cause grave harm to public safety. The risk cannot be left to the uncertainty of market forces or commercial interests as the current legislative proposals would require. Without adequate safeguards, the unbridled use of powerful encryption soon will deprive law enforcement of two of its most effective tools, court authorized electronic surveillance and the search and seizure of information stored in computers. This will substantially tip the balance in the fight against crime towards society's most dangerous criminals as the information age develops.

We are in unanimous agreement that congress must adopt encryption legislation that requires the development, manufacture, distribution and sale of only key recovery products and we are opposed to the bills that do not do so. Only the key recovery approach will ensure that law enforcement can continue to gain timely access to the plaintext of encrypted conversations and other evidence of crimes when authorized by a court to do so. If we lose this ability--and the bills you are considering will have this result--it will be a substantial setback for law enforcement at the direct expense of public safety.

Sincerely yours,

DARRELL L. SANDERS,
President, International Association of Chiefs of Police.

[Page: H6912]

FRED SCORALIE,
President, National Sheriffs' Association.

JAMES E. DOYLE,
President, National Association of Attorneys General.

WILLIAM L. MURPHY,
President, National District Attorneys Association.

Mr. WELDON of Pennsylvania. Mr. Speaker, again I am not saying that the administration's policy is a correct one nor is their policy of key recovery one that I can support. What I am saying is that this bill should not be rushed through. Members need to look at this very complicated subject in detail.

Yes, we need to protect the civil liberties of our citizens to be able to communicate in a confidential and protected manner. But we also need to look out for the national security implications of this legislation, the intelligence implications of this legislation, and for the ability for our law enforcement community, our State Police, the FBI, the Justice Department, when necessary through an established legal process to be able to get access to deal with those rogue entities that are using encryption to hide the activities they are involved in which are illegal. So I would ask our colleagues to closely monitor this legislation as it moves through the process.

Mr. Speaker, the second issue I would like to discuss is also a national security and defense issue, and I want to bring this up because it is going to be a major issue this weekend in the national media. It

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [x] 2002

deals with a concern that I have relative to the former Soviet Union, especially now with one of the former Soviet States, Russia, the largest one.

Mr. Speaker, as many of our colleagues know, I spend a great deal of time working in a positive way with Russia and its leadership on energy issues and environmental issues. This year I focused on establishing a middle-income housing program for the Russian people. I have established a new Russian Duma American Congress study group, which I cochair with the gentleman from Maryland [Mr. **Hoyer**] and which is chaired on the Russian side by Deputy Speaker Shokhin.

So I spend a lot of time trying proactively to improve our relationships, but I have a great deal of concern with what I think, and with my impression of the administration not being aggressive enough in pursuing concerns that many of us have relative to Russia's ability to control its nuclear material, its strategic weapons, and the state of the military in Russia.

Mr. Speaker, the problem is compounded by the fact that the administration, especially the Commander in Chief, has repeatedly used the bully pulpit to convey a message to America that we no longer have to worry about a threat coming from Russia. Again, I do not want to recreate a scenario where we depict Russia as some `Evil Empire,' because it is not. And I trust Boris Yeltsin for what he is trying to do, and applaud him for his efforts, as well as his key leadership, Chernomyrdin, Nemtsov, Chubays, and all of his people involved in leading his country.

[TIME: 2315]

But facts are facts. And there are major problems that we cannot sweep under the rug or put our head in the sand and ignore. And to that extent, Mr. Speaker, I want to talk about my most recent trip to Russia in May of this year and I have been there twice.

The most recent trip was a part of an interparliamentary exchange where we met with senior members of their Duma and discussed common issues. And we found many areas where we can work together.

Along with that, Mr. Speaker, I wanted to focus on some security concerns that I have with Russia and the need for Russia to be more transparent in terms of what their objectives and intents are relative to national security issues.

In the course of these meetings, I had the occasion to meet, along with the entire delegation, for 2 hours with Gen. Alexander Lebed. As we know General Lebed was a major candidate for the office of President when Boris Yeltsin ran for that office and won successfully last year against Mr. Zuganov, the candidate of the Communist Party.

Many speculate that the reason why Yeltsin was so successful was because he was able to get Lebed out of the race, partly by offering him a position as senior defense advisor to President Yeltsin on defense issues as a very respected retired Russian general. So the credibility of General Lebed is not something that I can vouch for but rather, based upon what President Yeltsin did in moving General Lebed into this position on his confidence in General Lebed as a senior defense advisor.

In our meeting with General Lebed he talked to us without the press being present and this is now in the public record and our trip report about the status of the stability of the Russian military. He raised some very serious concerns to us, Mr. Speaker, that we have to deal with and understand and that this administration has got to be more aggressive in pursuing as to whether or not they are facts or fiction.

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [xi] 2002

One of our questions to General Lebed was whether or not there was a possibility of armed revolution inside of Russia by its own military. General Lebed said he thought that was not possible primarily because, as General Lebed said, former Defense Minister Pavel Grachev had removed all the professionals from the army. General Lebed went on to say that the trained professional soldiers and leaders are gone and are now working with the criminal elements inside of Russia. And many of these generals and admirals have had access in the past to very sophisticated weapons and technologies that in fact could be sold on the black market.

And, in fact, we are seeing some evidence of proliferation of both weapons, strategic materials and in some cases even the seeking of nuclear materials. In fact, General Lebed went on to say that the army and the military does not have sufficient control over nuclear weapons.

In fact, he said to us that of 132 nuclear submarines being decommissioned by Russia, only 25 have had their reactors dismantled. In fact, two submarines nearly sank. Some reactors, he said, are in emergency condition. We have an aggressive program through our Navy to work with Russia to help them deal with their nuclear technology. I have been supportive of that.

But the problem is a very real one. Russia has severe problems with control of their nuclear material. He went on to say something that is even more provocative and something that is going to be the subject of a `60 Minutes' speech on Sunday evening this week, which I urge our colleagues to tune into. It is also going to be the subject of a Washington Post story and an AP story and also is going to be highlighted in a book that is going to be released next week by two authors. That book, by the way, is the basis, part of the basis for the Steven Speilberg movie that will be released this month entitled `Peacemaker,' which is a fictional depiction of the possible transfer of a Russian SS-18 missile out of Russia to a rogue nation.

General Lebed, in our meeting with six Members of Congress, said that when he had been Boris Yeltsin's chief defense advisor, he was given the responsibility to account for the location of 132 suitcase-sized nuclear devices, these are nuclear bombs, each with a capacity of 1 kiloton. One kiloton is not as great as the bomb at Hiroshima because that was approximately 15 kilotons. But 1 kiloton would cause a significant amount of damage wherever it was used.

Now, General Lebed said to us in a session with the bipartisan delegation, he was given the responsibility to account for the location of 132 suitcase-sized nuclear devices that Russia had manufactured. During his time in the capacity of advising Boris Yeltsin, he could only find 48. When we asked him where the rest of these devices were, he shrugged his shoulders and could not answer us. That is troubling. That is troubling because here was a man who Boris Yeltsin put into a key position advising him on defense matters who, according to him, was given the responsibility to account for these suitcase-sized nuclear weapons. And yet he told us, in a meeting in Moscow, that he could not in fact account for them. And I believe on `60 Minutes' this Sunday night you will see General Lebed again repeat that in his own words on that program.

I have asked the administration, both through our intelligence agencies as well as in a briefing that I gave to the current Secretary of Energy, to try to get an accounting from the Russians as to the validity of this statement.

Mr. Speaker, this is the kind of issue that we cannot sweep under the rug. I have the same ultimate objective that Strobe Talbott and President Clinton have in terms of a stabilized relationship with

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [xii] 2002

Russia. But that does not mean that we ignore problems that exist, whether it is suitcase-sized nuclear devices that may be out there available on the black market or whether it is the transfer of accelerometers and gyroscopes that had Russian markings, that were intercepted by the Jordanians on their way to Iraq, which is a violation of the missile technology regime, or whether it is the response by Russia to a Norwegian rocket weather launch that they had been given prior notice of and that Russia is in such a paranoid state that it put its entire strategic offensive force on alert because of Norway's launch of a weather rocket which meant that Russia was within 60 seconds of an all-out attack in response to a Norwegian weather rocket which they had been previously notified of.

Now the President of Russia has acknowledged publicly that his chegets, the devices that control the nuclear trigger, were in fact activated as a response to that Norwegian rocket launch.

Mr. Speaker, these are real issues, just as is the concern that many of us have over whether or not Russia just detonated another underground explosion, which is not in sync with the test ban treaty the administration has been pursuing. It is the same issue that I have over Yamantau Mountain, a major multibillion-dollar complex that has been under construction in the Ural Mountains for 18 years that is the size of the city of Washington, DC, where the Russians have built a city

of 65,000 people, a closed city, continuing to work on this project when Russian military officers do not have decent housing, when Russian retired officers have not been given back pay.

The question is, what is this huge complex being built for?

The reason why I raised these points, Mr. Speaker, is that we need the administration to be more aggressive in pursuing transparency and candor with Russia on these issues. I am not raising these issues for the first time, because it is not my intent to try to put a monkey wrench in the relationship between the United States and Russia. In fact, I have raised the issue of Yamantau Mountain on at least 10 occasions in written form and verbally with senior Russian leaders, my counterparts in the Russia Duma, and most recently a three-page letter that I wrote in Russian to Boris Yeltsin asking for transparency in terms of what is happening at Yamantau Mountain.

For us to have a stable relationship and if we follow the logic of this administration, a relationship with Russia based on bilateral treaties, then we must make sure that not just the United States but also Russia is abiding by those treaties, whether it is ABM, MTCR, the chemical weapons treaty, the nuclear test ban treaty or whatever that treaty happens to be. My feeling is that we have not done that, and I could take time to go through and cite specific examples at least seven times where the administration has not imposed sanctions on violations of the missile technology control regime that we know took place.

So I hope that what is going to unfold over the next several days, this weekend on `60 Minutes,' and into next week, as this new publication is released, will alert our colleagues that we must begin to focus on the problems of instability in Russia, not to create hostility between our two nations but, rather, to say we must be candid, we must be transparent, and we must work together to resolve the instability that currently exists and in the control of Russia's nuclear and conventional and strategic arsenal. It is of the highest importance for both nations and an issue that I am going to continue to pursue throughout the rest of this session of Congress.

Mr. Speaker, my final point tonight is one that is a personal item that I would like to spend a few moments discussing. It also has security implications but it also is a very emotional human interest

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [xiii] 2002

story that I would like to relate to my colleagues and pay appropriate thanks.

Mr. Speaker, as you know, we are always looking for new technology in the defense arena that can assist us in civilian applications. Shortly, this fall, we are going to be announcing the use of cold war technology that was used to at one point in time to detect rocket launchers around the world that we have been working on for the last year that is now going to be used to tell us when a wild land or forest fire first begins, instant imaging to give us that information so that we can have our emergency responders be there on the scene quickly to prevent the kind of conflagrations we have seen in the West, the Midwest, and the Northwest over the past decades. So it is using cold war technology for a very valuable function to assist us.

I saw evidence of a similar technology, Mr. Speaker, that we have now developed for commercial use called side scan sonar. I want to talk about the individual case because it involves a constituent family from Pennsylvania.

Back in February of this year, a young 19-year-old from Chester County, a neighboring county to my home county, the eldest of six children and the only son of the Swymer family was doing a co-op program at Penn State up at the Finger Lakes in New York.

During the course of his stay, right adjacent to Lake Owasco on a Saturday afternoon, where the temperature rose to the mid-60s, he ventured out into this very deep lake in a rowboat. A storm came up very quickly. And the individual evidently, for one reason or the other, because of the winds and the extreme nature of the storm, was tossed out of the boat.

The boat was found 2 days later on the opposite side of the lake, which is about a mile wide, along with the oar and the life preserver and no sign of this young 19-year-old, 6-foot tall, strapping, very successful student and solid athlete.

The State police in New York did a very commendable job in trying to locate the young man's body. They searched the entire lake perimeter. They tried to do dives and they just could not find this individual.

The family, through State representative Bob Flick, called my office in March and asked if I could provide any kind of technical assistance. Using the resources that we have developed primarily for the military and for ocean research as well as for disaster recovery, I called my friends in the oceangraphic community and my friends in the emergency response community. We were able to get the same technology that was developed for the military called side scanning sonar that was used to help us recover the remains of the TWA 800 crash off of Long Island in New York.

We were able to get that technology through the generosity of the New York Police Commissioner, Howard Safir, to have it sent up to the lake to look to see whether or not we could in fact locate this boy's body. A couple of suspected sightings were made, but we could not complete a dive to determine whether or not it was a positive find. They came back and were unsuccessful.

In June, I followed up with the Woods Hole Laboratory in Massachusetts and asked them to assist, and we identified perhaps the top national experts on deep dives relative to drownings.

We assembled a team that in the last week of August was able to travel to Auburn, NY, to put together on the water a team consisting of four boats, all volunteers during their time, to try to locate

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [xiv] 2002

this young man's body.

[Page: H6914]

[TIME: 2330]

The head technologist for this whole operation was Butch Hendrick, the president of Lifeguard Systems, Inc. of Hurley, NY, who is an expert in locating people in these kinds of situations and dealing with drownings. We also had an expert in terms of reading side scan sonar, Brett Phaneuf, from Marine Sonic Technology who also donated his time.

I spent the first 3 of the 5 days on the lake with this team, along with the very courageous volunteer firefighters from the Owasco Fire Department. Five of them spent the entire week away from their jobs volunteering the entire day each day to help us go back and forth across the 1,000-by-2,000 foot area of this lake and the lake was 1 mile wide and 14 miles long, trying to use this technology to determine whether or not we could find this young 19-year-old. I had to leave New York on Wednesday. On Thursday, three specific sightings were made, the markers were identified, and on Friday we brought in a dive team from Buffalo, NY, the Buffalo Industrial Diving Co. headed up by Mark Judd, four divers prepared to go down 150 feet. We had a decompression chamber on standby, a helicopter to take the divers if they should have problems. On the first dive, they recovered the body of 19-year-old Nathan Swymer and brought him back up and were able to reunite him so that his family could have a proper, decent burial.

Mr. Speaker, this story would not have been a success were it not for the cooperation of a number of very unselfish people, people who volunteered their time and their expertise to see if we could use a military technology to assist us in a very emotional situation involving the loss of someone's loved one.

The importance here, Mr. Speaker, is not that we just were able to locate Nathan Swymer 7 months after he fell off that row boat in Lake Owasco, but the technology that can be used across this country, in lakes, in rivers to assist us in similar types of operations and to avoid, where possible, the exposure to losing additional lives to send down to recover people who in fact have been drowned.

In fact, Mr. Speaker, over the past several years, it is my understanding that we have begun to lose more and more people in the rescue efforts to bring people who have drowned back than we should, and that is partly because we have not used appropriate technology to assist us in that process.

It will be my hope over the next several months to put together a congressional hearing where we can showcase this technology, where we can make the case that these kinds of technologies should be made available and that we should assist in that technology transfer process to departments across this Nation who have similar situations with deep lakes and with rivers so that we do not have to jeopardize additional lives in going down to recover our loved ones.

I particularly want to thank the gentleman from New York [Mr. **Walsh**] whose district Auburn and Lake Owasco is in. He has been very cooperative throughout this entire process and he was very supportive of our effort the last week of August.

I also want to thank Bill Andahazy, who is a consultant from Woods Hole who donated his time, Capt. Don Swain from the New York State Police and his team and all of those other individuals, the volunteer firefighters, the divers, the technologists who assisted us in closing this very difficult

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [xv] 2002

chapter in the lives of the Swymer family from Chester County, PA.

I want to encourage our colleagues, Mr. Speaker, to work with me, to see where we can find not just this kind of technology to use for commercial purposes but to see where we can take similar initiatives and assist us in solving day-to-day problems that face the people of this great Nation.

For the record, Mr. Speaker, I include the list of the Owasco Lake search team and thank them for their tireless efforts in this operation. A number of companies and individuals in the Philadelphia area donated over $10,000 along with the Chester County Chamber of Commerce to help us defray the costs of transporting the equipment to that lake. All of the individuals that were there donated their time. The money that we raised was used to defray the costs of the transportation of that equipment to the site to allow us to complete the rescue mission.

Mr. Speaker, I thank all of the staff who stayed this late hour for this special order.

Owasco Lake Search Team

Rep. Curt Weldon, Member, US House of Representatives

Rep. Robert J. Flick, Pennsylvania House of Representatives

W.J. (Bill) Andahazy, Independent Consultant

Capt. Donald Swain, Zone 2 HQ, New York State Police

Trooper David Hartz, Troop E, NY State Police

Trooper Karl Bloom, Troop E, NY State Police

Walter (Butch) Hendrick, President, Lifeguard Systems Inc., Hurley, NY

Andrea Zaferes, Lifeguard Systems

Craig Nelson, Lifeguard Systems

Lt. David Holland, Inst. of Environmental Medicine, Canadian Navy

Brett Phaneuf, Marine Sonic Technology, White Marsh, VA

Mark C. Judd, Buffalo Industrial Diving Company, Buffalo, NY

Andy Anderson, Buffalo Industrial Diving

Brad McCullum, Buffalo Industrial Diving

Brad Knight, Buffalo Industrial Diving

Tom Burns, Chief, Owasco Vol. Fire Co.

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [xvi] 2002

Joe Head, Assist. Chief, Owasco Vol. Fire Dept.

Tom Morgan, Assist. Chief, Owasco Vol. Fire Dept.

Tim Burns, Owasco Vol. Fire Dept.

Angelo Massina, Owasco Vol. Fire Dept.

Peter Pinckney, Sheriff, Cayuga County

Jim Tabor, Under Sheriff, Cayuga County

Gene Stiver, Dep. Chief of Navigation, Office of the Sheriff, Cayuga County

Chris Petrus, Navigation Deputy, Office of Sheriff, Cayuga County

Rev. and Mrs. (Dick and Pat) Streeter, Clergy and friends of Mr. and Mrs. Swymer.

Members of the Chester County Chamber Business and Industry Council.

Note that many other individuals also helped and offered services such as Alice Hamill of Mayflower Movers, King of Prussia, PA (although their services were not needed). The Holiday Inn Hotel, Auburn, NY staff worked with us on local arrangements as well as the Lake residents who let us use phones, water, etc. This operation was a community coming together that generated a successful conclusion to this tragedy.

END

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [xvii] 2002

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [xviii] 2002

Document No. 57

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [xix] 2002

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [xx] 2002