88

MINISTERIE VAN ALGEMENE ZAKEN
kabinet van de minister-president

[redacted]
Datum: 13 november 1998
Kenmerk: 98G000188
Rubr. ambt.: [redacted]
Einddatum rubr.: aanw. 18

Aan de leden van het CVIN:
Hr. S.J. van Hulst/Hoofd BVD
Drs. K.M. Meulmeester/AZ
Cdre. H.J. Vandeweijer/Hoofd MID
[redacted]/BuZa
[redacted]/Ju
[redacted]. (plv SG/EZ)
[redacted] (HDTP/V&W)
[redacted] APL a.i. d.t.v. [redacted]
[redacted]

Betreft: Nieuwe richtlijnen VS inzake export sterke cryptografische producten
(agendapunt 2b van de CVIN-vergadering van 20 november 1998)

Ten behoeve van de behandeling van agendapunt 2b zend ik u de volgende documenten ter kennisname:
a. Press briefing bij the vice-president etc. d.d. 16 september 1998
b. Statement by the press secretary d.d. 16 september 1998
c. mr. Leahy: vragen over Ädministrations's updated encryption policy"d.d. 17 september 1998
d. Interim rule Department of commerce d.d. 22 september 1998
e. Memo van de Werkgroep operationele cryptoproblematiek (WOC) d.d. 10 november 1998..

De memo van de WOC is besproken tijdens een vergadering van de Stuurgroep van 5 november jl. De stuurgroep stelde vast dat de gevolgen van de nieuwe VS-richtlijnen nader onderzocht dienen te worden en is van mening dat de aanbevelingen in de WOC-memo navolging verdienen.

Bij de behandeling van dit agendapunt is de Algemeen Projectleider a.i, de [redacted] aanwezig. Ik stel voor dat het CVIN aan de APL de opdracht geeft om een analyse te doen opstellen die een volledig inzicht verschaft in gevolgen van het VS-beleid voor de opsporing van strafbare feiten, voor het werk van de I&V-diensten en voor het beveiligingsniveau van producten in de telecommunicatiesector. Een dergelijke analyse, voorzien van conclusies en aanbevelingen kan ter behandeling in de vergadering van maart 1999 aan het CVIN te worden voorgelegd.

De coördinator van de inlichtingen- en
veiligheidsdiensten,
voor deze,

[redacted]

26.a 83

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release September 16, 1998

PRESS BRIEFING BY
THE VICE PRESIDENT,
DEPUTY CHIEF OF STAFF JOHN PODESTA,
PRINCIPAL ASSOCIATE DEPUTY ATTORNEY GENERAL ROBERT LITT,
ASSISTANT DIRECTOR OF THE FBI CAROLYN MORRIS,
UNDER SECRETARY OF COMMERCE WILLIAM REINSCH,
DEPUTY SECRETARY OF DEFENSE JOHN HAMRE,
AND DEPUTY NATIONAL SECURITY ADVISOR JIM STEINBERG

The Briefing Room

11:57 A.M. EDT

THE VICE PRESIDENT: Good morning. While my colleagues are coming in here, let me acknowledge them. John Podesta is going to take over the podium after I complete my statement, and he is joined by Bob Litt of the Justice Department, Bill Reinsch of the Commerce Department -- Under Secretary for the Export Administration -- and John Hamre, Deputy Secretary of Defense.

I also want to acknowledge Carolyn Morris of the FBI; Barbara McNamara of the National Security Agency; John Gordon, Deputy Director of the CIA. And you all should know that this process, the results of -- the interim results of which I'm announcing here, is a process that has been run principally by John Podesta and Jim Steinberg, Deputy at the National Security Council. And I also want to thank Sally Katzen at the NEC and David Beier on my staff for the work that they and many others have done on this.

Some of you who have followed this issue know that it is probably one of the single, most difficult and complex issues that you can possibly imagine. But we've made progress, and we're here this morning to announce an important new action that will protect our national security and our safety, and advance our economic interests and safeguard our basic rights and values in this new Information Age.

The Information Age has brought us the Internet, an inter-connected global economy and the promise of connecting us all to the same vast world of knowledge. But with that exciting promise comes new challenges. We must make sure that in the Information Age you get information about the rest of the world and not the other way around. We must ensure that new technology does not mean new and sophisticated criminal and terrorist activity which leaves law enforcement outmatched

-- we can't allow that to happen. And we must ensure that the sensitive financial and business transactions that now cruise along the information superhighway are 100 percent safe in cyberspace.

Balancing these needs is no simple task, to say the least. That is why, in taking the next step toward meeting these complex goals, we worked very closely with members of Congress from both parties, House and Senate; with industry; with our law enforcement community and with our national security community. And as we move forward we want to keep working closely with all who share a stake in this issue -- especially law enforcement -- to constantly assess and reassess the effectiveness of our actions in this fast changing medium.

Today I'm pleased to announce a new federal policy for the encryption and protection of electronic communication, a policy that dramatically increases privacy and security for families and businesses without endangering out national security.

Beginning today, American companies will be able to use encryption programs of unlimited strength when communicating between most countries. Health, medical, and insurance companies will be able to use far stronger electronic protection for personal records and information. Law enforcement will still have access to criminally-related information under strict and appropriate legal procedures. And we will maintain our full ability to fight terrorism and monitor terrorist activity that poses a grave danger to American citizens.

With this new announcement, we will protect the privacy of average Americans, because privacy is a basic value in the Information Age, indeed in any age. We will give industry the full protection that it needs to enable electronic commerce to grow and to thrive. And we will give law enforcement the ability to fight 21st century crimes with 21st century technology, so our families and businesses are safe, but on-line outlaws are not safe.

In just a moment you will hear more of the details of this new policy, but I want to conclude by saying that this policy does reflect one of the greatest challenges of these new times. And to state it broadly, it's a challenge of how we can harness powerful new technology while protecting our oldest and most cherished values, such as privacy and safety.

I'm grateful to those who have worked so hard to reach this balance. And with today's announcement I believe that all families and businesses have reason to feel safer, more secure and more confident as we approach the 21st century.

And now I'd like to turn things over to White House Deputy Chief of Staff John Podesta.

Q Mr. Vice President, before you go, can you tell us what you say to Democratic lawmakers who say the President ought to resign?

THE VICE PRESIDENT: I disagree.

Q How about the release of that tape? What do you think --

THE VICE PRESIDENT: The President is going to have a press conference shortly and I'm sure that you will not miss the opportunity at this national security press conference with the leader of a foreign country to raise all these questions.

Q What about the videotape, should it be released?

Q It was staged by the White House -- you know that, don't you?

MR. PODESTA: Guess what? I'm here to talk about encryption. Okay. I can see the front row leaving here. (Laughter.) As the Vice President noted, Jim Steinberg and I have co-chaired our process in this matter. I volunteered for that duty because of my well-known fascination with The X Files, which most of you know about.

As you know, this is an important and challenging issue that affects many of our interests in our society. And over the past year we've promoted a balanced approach to the issue, working with all segments of our government and working with industry to find a policy that promotes electronic commerce, preserves privacy, protects national security and law enforcement interests, and permits U.S. industry to secure global markets.

Recognizing the importance of moving this issue forward, last March the Vice President asked us to intensify our dialogue with U.S. industry, to bring industry's technical expertise to bear on this issue with the hope of finding more innovative ways that we might assist law enforcement. We appreciate the efforts of Congress, the law enforcement community and particularly the industry groups.

I would note the Computer Systems Policy Project and the Americans for Computer Privacy, who have been in an intensive dialogue with us over the past many months to foster an environment that has allowed us to come up with a policy which we believe has balanced the elements that are necessary in this regard.

I think all the stakeholders in this process, on our side, as well as on private industry's side, now have a greater appreciation of the issues and intend to continue the dialogue, which I think we're most pleased by. Again, I think some of the people here from industry will be available at the stakeout later to take some comment.

Based on the ideas discussed among the various stakeholders, today we're proposing an update to our policies that we've announced in the past. I'm going to serve kind of as M.C. We're going to start off with Bob Litt from the Justice Department and Carol Morris, who I asked to join us, from the FBI, to talk about the law enforcement-FBI concerns. Then we're going to turn to Bill Reinsch from the Commerce Department to talk about export control and electronic commerce. And finally you'll hear from Dr. Hamre from the Defense Department. I might ask Jim also to join us up here.

Before I give up the floor to Bob and Carol, though, I want to stress that encryption policy is an ongoing process. It's one of adaptation; it's an evolutionary process. We intend to continue the dialogue, and over the course of the next year, determine what further updates are necessary as we work with industry to try to, again, come up with a policy that balances national security, law enforcement, and the real needs for privacy and security in electronic commerce.

Thank you. Let me turn it over to Bob.

MR. LITT: Thank you, John. Good afternoon. The Justice Department and the FBI and law enforcement in general is supportive, very supportive of today's announcement on the updating of our export controls on encryption products, particularly with respect to those products that allow law enforcement to obtain lawful access to the plain text of encrypted information.

We have been very encouraged over the last few months by industry's efforts to work with us to develop and market strong encryption products that provide law-abiding citizens with the ability to protect the privacy of their communications and their electronically-stored data, while at the same time maintaining law enforcement's ability to ensure public safety when these products, when they become commercially available, are used in furtherance of serious criminal activity.

Our goal is through whatever means to ensure that when we have the lawful authority to take steps to protect public safety, we have the ability to do so. And we have been working cooperatively with industry for many months to develop approaches that will deal with that.

Carolyn Morris will now talk a little bit about the technical support center that is being proposed.

MS. MORRIS: Thank you very much, Bob.

Good afternoon, ladies and gentlemen. We in federal, state, and local law enforcement, are pleased with the administration's support to establish a technical support center. This center will provide federal, state, and local law enforcement with the resources and the technical capabilities we need to fulfill our investigative responsibilities.

In light of strong, commercially available encryption products that are being proliferated within the United States, and when such products are used in the furtherance of serious criminal activity, this center becomes very, very critical to solving the encryption issues that we need to make cases. As a matter of fact, the FBI has already begun planning activities of this critical technical support center in anticipation of the availability of funds.

The United States federal, local and state law enforcement community looks forward to a cooperative partnership with American industry, the Congress and the administration to ensure that this technical support center becomes a reality in the near future. With this center the American people can be assured that federal, state, and local law enforcement has the necessary resources and tools we need to fulfill our public safety mission.

Thank you very much.

UNDER SECRETARY REINSCH: With respect to export controls, the administration is updating its policy in three areas: Our existing policy and some revisions there, an expansion with respect to certain sectors, and an expansion with respect to so-called recoverable products. And let me address each of these separately. In keeping with the administration's reinvention initiatives, I'm going to try to do it in plain language -- or plain English, So that those of you that speak the vocabulary of encryption may find it to elementary, but we can go back and do it again in another language, if you want, later on in questions.

With respect to our existing policy, we have for two years ending this December, permitted the export of 56-bit products after an initial one-time review without further review by the government. What we're announcing today is the maintenance of that window permanently. And so 56-bit products will be freed from export controls after a one-time review, in perpetuity, not ending at the end of this year. We are, however, removing the requirement for key recovery plans or key recovery commitments to be provided in return for that change, which was the initial condition that we extracted.

In addition, we are continuing to permit the export of key recovery products -- products that contain those features -- without restraint worldwide. We are, however, going to simplify significantly our regulations that relate to those exports. In particular, we're going to eliminate the need for six-month progress reports for the plans that have been submitted, and we're going to eliminate the requirement for any prior reporting of key recovery agent information. For those of you that follow the regulations in detail, that means we're going to eliminate Supplement Five of our regulations on these matters.

Now, with respect to sectors, we're making some new innovations in four areas. Some of you may be familiar with the fact that some time ago we announced expanded treatment of encryption products for export to banks and financial institutions. And what we did at that time, briefly, was to permit the export of encryption products of any length, any bit length, with or without key recovery features to banks and financial institutions in a list of 45 countries.

What we are announcing today is, first, that we are adding insurance companies to the definition of financial institutions, so insurance companies will be treated the same way under this policy as banks and other financial institutions are now. In addition, we are providing the same kind of treatment for exports of these encryption products to the health and medical sector operating in the same set of countries. We are excluding from that biochemical and pharmaceutical producers. But the rest of the health and medical sector will be the beneficiary of the same kind of treatment.

In addition, we are providing also this expanded treatment for that country group to on-line merchants that are operating in those countries. That means that for products that are like client-server applications, like SSL, will be able to be exported to those destinations.

All these things will take place under what we call license exception, which means after initial one-time review to determine whether or not your product is, in fact, what you say it is, they can then go without any further review or intervention by the government to those locations. In addition, there is always the option in the export control system of coming in with an application to export these kinds of products to other destinations beyond the ones that I'm talking about right now, and those will be reviewed one by one on their merits.

Finally, with respect to what we have come to refer to as a class of so-called recovery capable or recoverable products, and these are the products that, among others, include what has become known as the doorbell products, which are products that, among other things, will deal with the development of local area or wide area networks and the transmission of e-mail and other data over networks -- we are going to permit the export of those products under a presumption of approval and an export licensing arrangement to a list of 42 countries. And within those countries we are going to permit that export to commercial firms only within those countries. And both in that case and in the case of the on-line merchants that I referred to a few minutes ago, we are going to exclude manufacturers or distributors of munitions items, I think for obvious reasons.

We can go into further details later, if you would like. I think for those of you that are interested in the nitty-gritty of all this stuff, BXA intends to post all the details, including the country lists, on its website and we should have that up later today.

Thank you.

DEPUTY SECRETARY HAMRE: Good morning. I'm here to speak on behalf of the national security community. I'm joined today by my enormously capable counterparts and colleagues, Deputy Director Barbara McNamara for the National Security Agency; and Deputy Director John Gordon from the Central Intelligence Agency.

The national security establishment strongly supports this step forward. We think this is a very important advance in a crucial area for our security in the future.

We in DOD had four goals when we entered these discussions. First was to strengthen our ability to do electronic commerce. We're the largest company in the world. Every month we write about 10 million paychecks. We write about 800,000 travel vouchers. One of our finance centers disburses $45 million an hour. We are a major, major force in business. And for that reason, we can't be efficient unless we can become fully electronic, and electronic commerce is essential for us. And this is an enormous step forward.

Second, we must have strong encryption and a security structure for that in order to protect ourselves in cyberspace. Many of you know that we have experienced a number of cyber attacks during the last year. This will undoubtedly increase in the future. We need to have strong encryption because we're operating over public networks; 95 percent of all of our communications now go over public infrastructure -- public telephone lines, telephone switches, computer systems, et cetera. To protect ourselves in that public environment, we must have encryption and we must have a key recovery system for ourselves.

The third goal that we had was to help protect America's infrastructure. One of the emerging national security challenges of the next decade is to protect this country, the homeland defense of this country, against attack. We must have strong encryption in order to do that, because most of this infrastructure now is being managed through distributed computer-based management systems, and this is an important step forward.

Finally, it is very important that the Department of Defense and our colleagues in the national security establishment have the ability to prosecute our national security interests overseas. Terrorists and rogue nations are increasingly using these tools to communicate with each other and to lay their plans. We must have the ability to deal with that. And so this policy, it's a balanced and structured approach to be able to deal with all four of those problems.

UNDER SECRETARY REINSCH: I apologize -- in listing my changes, I neglected one very important item that I want to go back to, and that is, in the sector area we are also announcing today the ability to export strong encryption of any bit length, with or without key recovery features, to subsidiaries of U.S. companies to all destinations in the world with the exception of the seven terrorist nations.

MR. PODESTA: Okay, I think we're happy to take your questions now. If you could identify whom you're addressing, because there is a variety of expertise. And I would like to introduce one other person, Charlotte Knepper from the NSC staff, who has been instrumental in pulling this all together.

Q John, this is a question for you. In October '96 and other White House statements on encryption, there has usually been a line also addressing the domestic side, saying that all Americans remain free to use any strength encryption. I didn't notice anything like that in today's announcement. Are there any conditions under which the White House would back domestic restrictions on encryption?

MR. PODESTA: We haven't changed our policy, and the previous statements are certainly intact. We have made a number of policy statements in the past, since this administration came into office, and I think that you should view this as a step forward, building on the policies that we have put before the American public in the past.

Q John, could I ask you one question about an un-encrypted matter?

MR. PODESTA: Maybe. (Laughter.)

Q Democrats on the Hill are now saying, and John Kerry is saying that the President's actions absolutely call for some sort of punishment. What are Democrats telling you about what they feel must be done at this point?

MR. PODESTA: Well, I think I'm not going to stand here and take a lot of questions, but I'm going to give special dispensation, as a Catholic, today -- which is I'm going to return your phone calls later. But in deference to the people up here I think we'll handle it that way.

But in specific response, I'll take one, which is that I think that we had a number of productive meetings with Democrats on both sides of the Hill yesterday. They view the President as a person who has led on the issues that are important to them, and I think what they want to do is get back to having him speak out and be a leader on the issues of education and the health care bill of rights, on saving Social Security. And I think they pointed at that and wanted to work with us on that.

I think with regard to the question that you posed with regard to Senator Kerry, I think that's a matter that they are debating amongst themselves more than they are debating with the White House. I think it's probably presumptuous for us at this point to offer them assistance or guidance. I mean, the President has said that what he has done was wrong; he's apologized for it; he's asked for forgiveness. He is moving forward. And I think that this debate is going on, on Capitol Hill, but it's largely going on amongst members themselves.

Q We haven't heard many of them say they want to get back to the work at hand.

MR. STEINBERG: You heard John, and I'm going to leave it there.

Let me just add a word in response, in connection with the domestic controls issue. I think one of the lessons that we've learned from this exercise is that -- actually, two lessons -- one, that trying to balance the various interests and equities in this is much less of a zero sum gain than I think some began to look at the question. That is, you heard from Dr. Hamre and others that many of the interests involved have common interests in making sure that we have secure and effective means of dealing with communications and stored data.

And so we found, by looking in a very pragmatic way, that there were ways to solve these problems without very, kind of, broad-based solutions. In particular, I think the idea that there's no one-size-fits-all answer to the problems of meeting the various needs informs the decisions that we reached -- that there are a variety of different techniques that respond to the different aspects of the industry, the different aspects of the technology. I think that's what made the progress possible today, is that industry, agencies and Congress sat down together, pulled the problem apart, began to look at its different components and began to fashion very pragmatic solutions.

And so I think we came to this discussion with a spirit of not looking for a kind of single or simple solution to the problem but, rather, how do you tackle and meet the various needs. And I think that's what led to this resolve.

Q Could you talk a little more about the on-line merchants part of it? I mean, what do you have to do to qualify as an on-line merchant? Do you have to register or can anybody sort of set themselves up in business?

UNDER SECRETARY REINSCH: I think the simplest way to respond to that right now is we'll have a definition in the reg that will be very clear as to what the criteria are for qualification. And those definitions have already been dealt with and agreed to, so we should have them up on the web site this afternoon.

Q A question for Bill Reinsch. How do you handle, then, 128-bit, to which the Department has given export -- or has allowed to be exported after going through this review? Will 128 or things above 56-bit, will they require a license or will they still have to go through plans --

UNDER SECRETARY REINSCH: Well, with respect to the subsidiaries, the health sector, the banks, the financial institutions, the insurance companies, the on-line merchants, and the recoverable products as in the universe defined -- no. In the case of all but the recoverable products, they will all go on license exception, which means one-time review and then out the door. With respect to recoverable products, they will come in and go out pursuant to an export licensing arrangement, where we'll have to do a little tailoring depending upon the nature of the product. But there is a presumption of approval for the 42 countries that I indicated.

And that's without reference to bit length -- 128 or more is all covered by that. Now, if you want to export an 128-bit product that is beyond any of those universes, then you would have to come in for an individual license application.

Q A question for Mr. Litt. With regard to the technical support center, when do you expect that to be in operation?

MR. LITT: I don't think we have a specific timetable yet. Obviously, it would be helpful for us to have it up and operational as soon as possible, but there are planning and budgetary issues that have to be dealt with.

Q This is probably a question for Under Secretary Reinsch. The export exceptions now are essentially going to U.S. subsidiaries -- foreign subsidiaries of U.S. companies. I was wondering, could you be a little more specific -- what size company, what kind of company will be allowed to export powerful crypto to its foreign subsidiaries?

UNDER SECRETARY REINSCH: That doesn't make any difference. The universe is determined by the end user, not by the nature of the American company. But it is not -- while part of this relates to subsidiaries of U.S. companies, that is correct, we also intend, on a case-by-case basis, to provide for favorable treatment for export of the same kind of thing to strategic partners of U.S. companies -- those foreign companies that are engaged in a closer, say, joint venture, that kind of relationship.

Well, I think that's it.

Q What about foreign companies that have U.S. subsidiaries, like Seaman's or -- or Chrysler -- can they get this encryption?

UNDER SECRETARY REINSCH: Well, keep in mind, there are multiple universes here. If you're talking about the financial institutions, the banks and the insurance companies, those aren't necessarily American financial institutions. That's for export to any financial institution, and for their use in any of their branches, aside from the terrorist countries. This is true for the health sector; this is true for on-line merchants as well. Those are not restricted to U.S. companies.

Obviously, if we're going to have a requirement for U.S. subs, it relates to U.S. subs, and wouldn't affect the examples you've described. Now, with respect to recoverable products, which actually is one of the areas where the companies you mentioned would probably be looking because they'd be looking to build a network among their various offices, affiliates of subsidiaries, dealers if necessary, worldwide, the recoverable provisions that I described could be exported to those companies within the territorial universe I described -- the 42 countries.

Thank you very much.

END 12:25 P.M. EDT

2.6.6.

50

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release
September 16, 1998

STATEMENT BY THE PRESS SECRETARY

Administration Updates Encryption Policy

The Clinton Administration today announced a series of steps to update its encryption policy in a way that meets the full range of national interests: promotes electronic commerce, supports law enforcement and national security and protects privacy. These steps are a result of several months of intensive dialogue between the government and U.S. industry, the law enforcement community and privacy groups that was called for by the Vice President and supported by members of Congress.

As the Vice President stated in a letter to Senator Daschle, the Administration remains committed to assuring that the nation's law enforcement community will be able to access, under strictly defined legal procedures, the plain text of criminally related communications and stored information. The Administration intends to support FBI's establishment of a technical support center to help build the technical capacity of law enforcement - Federal, State, and local - to stay abreast of advancing communications technology.

The Administration will also strengthen its support for electronic commerce by permitting the export of strong encryption when used to protect sensitive financial, health, medical, and business proprietary information in electronic form. The updated export policy will allow U.S. companies new opportunities to sell encryption products to almost 70 percent of the world's economy, including the European Union, the Caribbean and some Asian and South American countries. These changes in export policy were based on input from industry groups while being protective of national security and law enforcement interests.

The new export guidelines will permit exports to other industries beyond financial institutions, and further streamline exports of key recovery products and other recoverable encryption products. Exports to those end users and destination countries not addressed by today's announcement will continue to be reviewed on a case-by-case basis.

Very strong encryption with any key length (with or without key recovery) will now be permitted for export, under license exception, to several industry sectors. For example, U.S. companies will be able to export very strong encryption for use between their headquarters and their foreign subsidiaries worldwide except the seven terrorist countries (Iran, Iraq, Libya, Syria, Sudan, North Korea and Cuba) to protect their sensitive company proprietary information.

On-line merchants in 45 countries will be able to use robust U.S. encryption products to protect their on-line electronic commerce transactions with their customers over the Internet.

Insurance companies as well as the health and medical sectors in those same 46 countries will be able to purchase and use robust U.S. encryption products to secure health and insurance data among legitimate users such as hospitals, health care professionals, patients, insurers and their customers.

The new guidelines also allow encryption hardware and software products with encryption strength up to 56-bit DES or equivalent to be exported without a license, after a one time technical review, to all users outside the seven terrorist countries. Currently, streamlined exports of DES products are permitted for those companies that have filed key recovery business plans. However, with the new guidelines, key recovery business plans will no longer be required.

The Administration will continue to promote the development of key recovery products by easing regulatory requirements. For the more than 60 companies which have submitted plans to develop and market key recovery encryption products, the six month progress reviews will no longer be required. Once the products are ready for market, they can be exported, with any bit length -- without a license -- world-wide (except to terrorist nations) after a one-time review. Furthermore, exporters will no longer need to name or submit additional information on a key recovery agent prior to export. These requirements will be removed from the regulations.

Finally, industry has identified other so-called "recoverable" products and techniques that allow for the recovery of plaintext by a system or network administrator and that can also assist law enforcement access, subject to strict procedures. The Administration will permit their export for use within most foreign commercial firms, and their wholly-owned subsidiaries, in large markets, including Western Europe, Japan and Australia, to protect their internal business proprietary communications.

The Administration welcomes a continued dialogue with U.S. industry and intends to review its policy in one year to determine if additional updates may be necessary to continue a balanced approach that protects the public safety and national security, ensures privacy, enables continued technology leadership by U.S. industry and promotes electronic commerce.

###

For Immediate Release
September 16, 1998

FACT SHEET

Administration Updates Encryption Policy

Exports of 56-bit DES and equivalent products (hardware and software) will be streamlined (under license exception). Requirements for key recovery plans are eliminated.

Exports of unlimited strength encryption products (with or without key recovery) will be streamlined (under license exception) to certain industries. The sectors are:

Subsidiaries of U.S. Firms, worldwide (except seven terrorist nations).

Insurance companies to the same 45 countries recently approved for exports to banks and financial institution exports.

Health and medical organizations (including civilian government health agencies) in the same 45 countries. Does not include biochemical/pharmaceutical manufacturers.

On-line merchants for client-server applications, in the same 45 countries, with the purpose of securing electronic transactions between merchants and their customers. Does not include manufacturers and distributors of items controlled on the U.S. munitions list.

Key Recovery products will continue to be exportable under license exception worldwide (except seven terrorist nations). Review of foreign key recovery agents is eliminated.

Exports of "recoverable" products will be approved to most commercial firms, and their wholly-owned subsidiaries, in a broad range of countries under encryption licensing arrangements. This group of countries covers most major commercial markets including Western Europe, Japan, and Australia. The policy does not include service providers and manufacturers and distributors of items controlled on the U.S. munitions list.

Exports to end users or destinations outside this policy are possible on a case-by-case basis.

Prior to export, products are subject to a one-time product technical review.

###

26.2 92

[Congressional Record: September 17, 1998 (Senate)]
[Page S10515]
From the Congressional Record Online via GPO Access [wais.access.gpo.gov]
[DOCID:cr17se98-135]

ADMINISTRATION'S UPDATED ENCRYPTION POLICY

Mr. LEAHY. Mr. President, when the Administration first announced the encryption policy that has been in effect for the past two years, I warned on October 1, 1996, that:

> The general outline of the Administration's plan smacks of the government trying to control the marketplace for high-tech products. Only those companies that agree to turn over their business plans to the government and show that they are developing key recovery systems, will be rewarded with permission to sell abroad products with DES encryption, which is the global encryption standard.

The Administration announced yesterday that it is finally fixing this aspect of its encryption policy. New Administration guidelines will permit the export of 56-bit DES encryption without a license, after a one time technical review, to all users outside the seven terrorist countries. No longer will the Administration require businesses to turn over business plans and make promises to build key recoverable products for the freedom to export 56-bit DES.

In 1996, I also raised serious questions about the Administration's proposal to pull the plug on 56-bit DES exports in two years. I warned at the time that this ``sunset" provision ``does not promote our high-tech industries overseas." I specifically asked,

> Does this mean that U.S. companies selling sophisticated computer systems with DES encryption overseas must warn their customers that the supply may end in two years? Customers both here and abroad want stable suppliers, not those jerked around by their government.

I am pleased that the Administration has also changed this aspect of its policy and adopted an export policy with no ``sunset." Instead, the Administration will conduct a review of its policy in one year to determine how well it is working.

Indeed, while 56-bit encryption may still serve as the global standard, this will not be the situation for much longer. 128-bit encryption is now the preferred encryption strength.

In fact, to access online account information from the Thrift Savings Plan for Federal Employees, Members and congressional staff must use 128-bit encryption. If you use weaker encryption, a screen pops up to say ``you cannot have access to your account information because your Web browser does not have Secure Socket Layer (SSL) and 128-bit encryption (the strong U.S./Canada-only version)."

Likewise, the Department of Education has set up a Web site that allows prospective students to apply for student financial aid online. Significantly, the Education Department states that ``[t]o achieve maximum protection we recommend you use 128-bit encryption."

These are just a couple examples of government agencies or associated organizations directing or urging Americans to use 128-bit encryption. We should assume that people in other countries are getting the same directions and recommendations. Unfortunately, while American companies can fill the demand for this strong encryption here, they will still not be permitted to sell this strength encryption abroad for use by people in other countries.

Nevertheless, the Administration's new encryption policy announced today moves in the right direction to bolster the competitive edge of our Nation's high-tech companies, allow American companies to protect their confidential and trade secret information and intellectual property in communications with subsidiaries abroad, and promote global electronic commerce. These are objectives I have sought to achieve in encryption legislation that I have introduced and cosponsored with bipartisan support in this and the last Congress.

I remain concerned, however, that privacy safeguards and standards for law enforcement access to decryption assistance are ignored in the Administration's new policy. These are critical issues that continue to require our attention.

20.193

22 September 1998
Source: http://www.access.gpo.gov/su_docs/aces/aaces002.html

[Federal Register: September 22, 1998 (Volume 63, Number 183)]
[Rules and Regulations]
[Page 50516-50527]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr22se98-21]

DEPARTMENT OF COMMERCE

Bureau of Export Administration

15 CFR Parts 732, 734, 740, 742, 743, 748, 750, 752, 770, 772, and 774

[Docket No. 980911233-8233-01]
RIN 0694-AB80

Encryption Items

AGENCY: Bureau of Export Administration, Commerce.

ACTION: Interim rule.

SUMMARY: This interim rule amends the Export Administration Regulations (EAR) by clarifying controls on the export and reexport of encryption items (EI) controlled for ``EI" reasons on the Commerce Control List. This rule incorporates public comments on an interim rule published in the Federal Register on December 30, 1996, and implements new licensing policies for general purpose non-recoverable non-voice encryption commodities or software of any key length for distribution to banks and financial institutions in specified countries.

DATES: Effective Date: This rule is effective September 22, 1998. Comments: Comments on this rule must be received on or before November 6, 1998.

ADDRESSES: Written comments on this rule should be sent to Nancy Crowe, Regulatory Policy Division, Bureau of Export Administration, Department of Commerce, P.O. Box 273, Washington, DC 20044.

FOR FURTHER INFORMATION CONTACT: James Lewis, Office of Strategic Trade and Foreign Policy Controls, Bureau of Export Administration, Telephone: (202) 482-0092.

SUPPLEMENTARY INFORMATION:

Background

On December 30, 1996, the Bureau of Export Administration (BXA) published in the Federal Register (61 FR 68572) an interim rule that exercises jurisdiction over, and imposes new combined national security and foreign policy controls on, certain encryption items that were on the United States Munitions List, consistent with Executive Order (E.O.) 13026 and pursuant to the Presidential Memorandum of that date, both issued by President Clinton on November 15, 1996.

BXA received comments from 45 commenters, and the comments fall into three broad categories: general concerns and objections to the policy embodied in the regulations; recommendations for specific changes or clarifications to the regulations that are consistent with the broad encryption policy implemented in the December 30 rule; and recommendations for additional changes to encryption policy.

Suggestions for Changes to Clarify Existing Policy

A number of commenters provided specific suggestions for changes or clarifications which are consistent with the intent of the policy and which would streamline or improve the regulations. Many of these suggestions are implemented in this rule, such as clarifying that the tools of trade provisions of License Exception TMP and License Exception BAG apply globally and clarifying that anti-virus software does not require a license for export.

Several commenters asked the Department of Commerce to adopt exemptions to license requirements which were available for encryption exporters under Sec. 123.16(b)(2) and (b)(9) of the International Traffic and Arms Regulations (ITAR), such as those which allowed the export of components to a U.S. subsidiary or which allowed the export of spare parts and components without a license for an already approved sale. This rule adds these new provisions under License Exception TMP, making them applicable to encryption controlled items as well as other items eligible for TMP treatment.

Two commenters asked that the regulations clarify that the ITAR licensing policy for equipment specially made for and limited to the encryption of interbanking transactions had not changed with the transfer of jurisdiction of encryption products to the Department of Commerce. This interim rule clarifies that this equipment is not subject to EI controls.

Several commenters recommended a number of changes to the Key Escrow Product and Agent criteria found in Supplement Nos. 4 and 5 part to 742 of the EAR. These recommendations were to simplify the criteria, and to modify some of the specific prescriptions to allow for greater flexibility and variation on the part of exporters. Many commenters found the criteria too bureaucratic and legalistic to help advance U.S. encryption policy goals, while others noted that the criteria were still overly focused on key escrow and not consistent with the broader approach to key recovery found elsewhere in the regulation. Several commenters also encouraged the administration to make clear that it had moved beyond key escrow to key recovery in its policy. One commenter

[[Page 50517]]

focused on weaknesses and omissions found in the key escrow product and agent criteria found in Supplement Nos. 4 and 5 to part 742 of the EAR, and provided suggested additions to the criteria to make them more consistent with emerging business practices. The criteria specified in Supplement Nos. 4 and 5 were discussed extensively with industry prior to publication of the December 30 interim rule, and the rule reflects these discussions. However, BXA continues to look for ways to streamline the criteria, and will address revisions in a future regulation.

Several commenters expressed concerns over the longer processing time required for licenses at the Department of Commerce. Some commenters noted that the involvement of Departments of Energy and State, the Arms Control and Disarmament Agency and other agencies which did not review license applications for encryption products submitted to the Department of State added unnecessary levels of review and caused unwarranted delays. BXA is continuing to work with other reviewing Departments and Agencies to ensure expeditious review of encryption license applications. Many commenters noted that the requirements for a Department of Commerce license were substantially greater than what was required at the Department of State. The Department of Commerce, for example, requires an end-use certificate to be obtained for some destinations before approving an export; the Department of State did not and exporters question the need for this change. Other commenters noted that the Department of State licensing system was more flexible and faster for approvals of distribution and manufacturing arrangements. The Department of Commerce has no equivalent licenses, but is reviewing the possibility of such licenses. Many oral comments received since the close of the comment period note that unlike the Department of State, the Department of Commerce does not allow licenses to be amended, so that if an exporter has, for example, a license which allows him to ship to thirty countries and wishes to add one more, the Department of Commerce requires submission of an entire new license while the Department of State was content with a simple letter noting the requested change. This rule will now allow the addition of countries to an Encryption Licensing Arrangement by letter. BXA understands industry concerns about the license process under the EAR, and continues to look for ways to streamline the process.

Additional Recommendations for Changes to Encryption Policy

A number of commenters asked that the Administration revisit a number of decisions made in the course of the development of the encryption policy as reflected in the December 30 interim rule. Several asked that we reconsider and liberalize the treatment of Cryptographic Application Program Interface. Others questioned the addition of ``defense services" controls similar to that contained in the ITAR (which prohibits U.S. persons from assisting foreign entities from developing their own indigenous encryption products). Several commenters objected to the structure of License Exception KMI for non-recoverable 56 bit products, with its requirement for a review every six months. Other commenters also called for a reversal of the decision to exempt transferred encryption items from normal Department of Commerce regulatory practices. Finally, several commenters recommended that the licensing criteria and License Exceptions applicable to other dual-use items be fully applicable to encryption products, such as considerations of foreign availability, the de minimis content exclusion, public domain treatment and the use of License Exceptions. This rule focuses on clarifications to existing encryption policy.

Based on public comments to the December 30 interim rule, this interim rule specifically makes the following changes:

--In Secs. 732.2(d) and 732.3(e)(2), makes editorial corrections to clarify that encryption items controlled for ``EI" reasons under ECCNs 5A002, 5D002 and 5E002 are not eligible for De Minimis treatment.
--In Sec. 734.2, clarifies that downloading or causing the downloading of encryption source code and object code in Canada is not controlled and does not require a license.
--In Sec. 740.6, clarifies that letters of assurance required for exports under License Exception TSR may be accepted in the form of a

letter or any other written communication from the importer, including communications via facsimile.

--Sec. 740.8 is also amended by adding a new paragraph to authorize, after a one-time technical review, exports and reexports under License Exception KMI of non-recoverable financial-specific encryption software (which is not eligible under the provisions of License Exception TSU for mass market software, such as SET or similar protocols) and commodities of any key length that are restricted by design (e.g., highly field-formatted with validation procedures, and not easily diverted to other end-uses) for financial applications to secure financial transactions, for end-uses such as financial transfers or electronic commerce. No business and marketing plan to develop, produce, or market encryption items with recoverable features is required. Such exports and reexports are eligible to all destinations except Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria. Conforming changes are also made in Sec. 742.15.

--Sec. 740.8 is also amended to authorize, after a one time review, exports and reexports under License Exception KMI of general purpose non-recoverable non-voice encryption commodities or software of any key length for distribution to banks and financial institutions (as defined in part 772 of the EAR) in destinations listed in new Supplement No. 3 to part 740, provided the end-use is limited to secure business financial communications or transactions or financial communications/ transactions between the bank or financial institution and its customers. No customer to customer communications or transactions are permitted. Software and commodities that have already received a one-time technical review through a classification request or have been licensed for export under an Encryption Licensing Arrangement or a license are eligible for export to banks and financial institutions under License Exception KMI without an additional one-time technical review. Note that no business or marketing plan is required. Conforming changes are also made in Sec. 742.15. Software and commodities that have already been approved under an Encryption Licensing Arrangement to banks in specified countries may now be exported or reexported to other banks and financial institutions in those countries under the same Encryption Licensing Arrangement.

--In Sec. 740.9, removes the reference to Country Group D:1. With this change, commodities and software are eligible for export under the tools of trade provisions of License Exception TMP to all destinations except countries listed in country group E:2 or Sudan. This also clarifies that encryption software controlled for EI reasons under ECCN 5D002 may be pre-loaded on a laptop and temporarily exported under the tools of trade provisions of License Exception TMP

[[Page 50518]]

to most countries, including those listed i. Country Group D:1.

--Also in Sec. 740.9, adds a new paragraph (a)(2)(ix) to authorize under License Exception TMP the export of components, parts, tools or test equipment exported by a U.S. person to its subsidiary, affiliate or facility in a country in Country Group B that is owned or controlled by the U.S. person, if the components, part, tool or test equipment is to be used for manufacture, assembly, testing, production or modification, provided that no components, parts, tools or test equipment or the direct product of such components, parts, tools or test equipment are transferred or reexported to a country other than the United States from such subsidiary, affiliate or facility without a license or other authorization from BXA.

--In Sec. 740.11, excludes items controlled for EI reasons from eligibility under the International Safeguards provisions of License

Exception GOV.
--In Sec. 740.14, clarifies existing provisions of License Exception BAG to distinguish temporary from permanent exports and imposes a restriction on the use of BAG for exports or reexports of EI-controlled items to terrorist supporting destinations or by persons other than U.S. citizens and permanent residents.
--New Supplement No. 3 to part 740 is added to list the countries eligible to receive under License Exception KMI general purpose non-recoverable non-voice encryption commodities or software of any key length for distribution to banks and financial institutions.
--In Sec. 742.15, adds 40-bit DES as being eligible for consideration under the 15-day review, for mass-market eligibility, subject to the additional criteria listed in Supplement No. 6 to part 742.
--In Sec. 742.15(b)(1), clarifies that subsequent bundling, updates or releases may be exported and reexported under applicable provisions of the EAR without a separate one-time technical review so long as the functional encryption capacity of the originally reviewed mass-market encryption software has not been modified or enhanced.
--New paragraph (b)(4) is added to Sec. 742.15 to authorize exports and reexports under an Encryption Licensing Arrangement of general purpose non recoverable, non-voice encryption commodities and software of any key length for use by banks/financial institutions as defined in part 772 of the EAR in all destinations except Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan. No business or marketing plan is required. Exports and reexports for the end-uses to secure business financial communications or between the bank and/or financial institution and its customers will receive favorable consideration. No customer to customer communications or transactions are eligible under the Encryption Licensing Arrangement.
--In Supplement No. 4 to part 742, paragraph (3), revises ``reasonable frequency'' to ``at least once every three hours'' to resolve the ambiguity on how often the output must identify the key recovery agent and material/information required to decrypt the ciphertext.
--In Supplement No. 4 to part 742, paragraph (6)(i), clarifies that the U.S. government must be able to obtain the key(s) or other material/ information needed to decrypt all data, without restricting the means by which the key recoverable products allow this.
--In Supplement No. 6 to part 742 for 7-day mass-market classification requests, clarifies that a copy of the encryption subsystem source code may be used instead of a test vector to determine eligibility for License Exception TSU for mass market software.
--In Sec. 743.1, requires reporting under the Wassenaar Arrangement for items controlled under ECCNs 5A002 and 5D002 when exported under specific provisions of License Exception KMI. This is not a new reporting requirement, but replaces and narrows the scope of the reporting requirement under the Encryption License Arrangement for financial-specific commodities and software and general purpose non-recoverable non-voice encryption commodities and software of any key length for distribution to banks and financial institutions that are eligible for License Exception KMI.
--In Secs. 748.9 and 748.10, clarifies a long-standing policy that no support documentation is required for exports of technology or software, and it removes the requirement for such support documentation for exports of technology or software to Bulgaria, Czech Republic, Hungary, Poland, Romania, or Slovakia. This rule also exempts from support documentation requirements all encryption items controlled under ECCNs 5A002, 5B002, 5D002 and 5E002. This conforms with the practice under the ITAR prior to December 30, 1996.
--In Sec. 750.7, allows requests to add countries of destination to Encryption Licensing Arrangements by letter.

--In Sec. 752.3, excludes encryption items controlled for EI reasons from eligibility for a Special Comprehensive License.
--In Sec. 770.2, adds a new interpretation to clarify that encryption software controlled for EI reasons under ECCN 5D002 may be pre-loaded on a laptop and exported under the tools of trade provision of License Exception TMP or the personal use exemption under License Exception BAG, subject to the terms and conditions of such License Exceptions.
--In part 772, adds new definitions for ``bank", ``effective control", ``encryption licensing arrangement", and ``financial institution".
--In Supplement No. 1 to part 774, Category 5--Telecommunications and Information Security is amended by revising ECCN 5A002 to authorize exports of components and spare parts under License Exception LVS, provided the value of each order does not exceed $500 and the components and spare parts are destined for items previously authorized for export, and to clarify that equipment for the encryption of interbanking transactions is not controlled under that entry.
--Revises the phrase ``up to 56-bit key length DES" where it appears to read ``56-bit DES or equivalent", and makes other editorial changes.

Note that this rule does not affect exports or reexports authorized under licenses issued prior to the effective date of this rule.

Several commenters also noted that the exemptions found under Sec. 125.4(b) of the ITAR should be implemented in the EAR. Most of the exemptions found in Sec. 125.4(b) of the ITAR are already available under existing provisions of the EAR. For example, Sec. 125.4(b)(4) of the ITAR authorizes exports without a license of copies of technical data previously authorized for export. The EAR has no restrictions on the number of copies sent to a consignee authorized to receive technology under license or a License Exception. Section 125.4(b)(5) authorizes exports without a license of technical data in the form of basic operations, maintenance, and training information relating to a defense article lawfully exported or authorized for export provided the technical data is for use by the same recipient. Further, Section 125.4(2) authorizes exports of technical data in furtherance of a manufacturing license or technical assistance agreement. License Exception

[[Page 50519]]

TSU for operation technology and software (see Sec. 740.13 of the EAR) authorizes the export and reexport of the minimum technology necessary for the installation, operation, maintenance and repair of those products (including software) that are lawfully exported or reexported under a license, a License Exception, or non license required (NLR). Section 125.4(b)(7) of the ITAR allows the return of technical data to the original source of import. License Exception TMP similarly authorizes the return of any foreign-origin item, including technology, to the country from which it was imported if the characteristics have not been enhanced while in the United States (see Sec. 740.9(b)(3) of the EAR).

BXA has also received many inquiries on Shipper's Export Declaration (SED) requirements for Canada. Note that the EAR do not require exporters to file an SED for exports of any item to Canada for consumption in Canada, unless a license is required. Further note that a license is not required for exports of encryption items for consumption in Canada, including certain exports over the Internet. Finally, BXA has received many requests for clarification on SED requirements for electronic transfers. Neither the EAR nor the FTSR provide for the filing of SEDs for electronic transfers of items controlled by the Department of Commerce under the EAR .

As further clarifications and changes to the encryption provisions of the EAR are intended, in particular regarding Supplement Nos. 4 and 5 to part 742 of the EAR, BXA will publish additional interim rules in the Federal Register.

Rulemaking Requirements

1. This interim rule has been determined to be significant for purposes of E. O. 12866.

2. Notwithstanding any other provision of law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with a collection of information, subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid Office of Management and Budget Control Number. This rule contains collections of information subject to the Paperwork Reduction Act of 1980 (44 U.S.C. 3501 et seq.). These collections have been approved by the Office of Management and Budget under control numbers 0694-0088, ``Multi-Purpose Application," which carries a burden hour estimate of 52.5 minutes per submission; and 0694-0104, ``Commercial Encryption Items Transferred from the Department of State to the Department of Commerce," which carries the following burden hours: marketing plans (40 hours each); semiannual progress reports (8 hours each); safeguard procedures (4 hours); recordkeeping (2 hours); annual reports (4 hours); and Encryption Licensing Arrangement letters (15 minutes).

3. This rule does not contain policies with Federalism implications sufficient to warrant preparation of a Federalism assessment under E.O. 12612.

4. The provisions of the Administrative Procedure Act (5 U.S.C. 553) requiring notice of proposed rulemaking, the opportunity for public participation, and a delay in effective date, are inapplicable because this regulation involves a military and foreign affairs function of the United States (Sec. 5 U.S.C. 553(a)(1)). Further, no other law requires that a notice of proposed rulemaking and an opportunity for public comment be given for this interim final rule. Because a notice of proposed rulemaking and an opportunity for public comment are not required to be given for this rule under 5 U.S.C. or by any other law, the requirements of the Regulatory Flexibility Act (5 U.S.C. 601 et seq.) are not applicable.

However, because of the importance of the issues raised by these regulations, this rule is issued in interim form and comments will be considered in the development of final regulations. Accordingly, the Department of Commerce encourages interested persons who wish to comment to do so at the earliest possible time to permit the fullest consideration of their views.

The period for submission of comments will close November 6, 1998. The Department of Commerce will consider all comments received before the close of the comment period in developing final regulations. Comments received after the end of the comment period will be considered if possible, but their consideration cannot be assured. The Department will not accept public comments accompanied by a request that a part or all of the material be treated confidentially because of its business proprietary nature or for any other reason. The Department of Commerce will return such comments and materials to the person submitting the comments and will not consider them in the development of final regulations. All public comments on these regulations will be a matter of public record and will be available for public inspection and copying. In the interest of accuracy and completeness, the

Department of Commerce requires comments in written form.

Oral comments must be followed by written memoranda, which will also be a matter of public record and will be available for public review and copying. Communications from agencies of the United States Government or foreign governments will not be made available for public inspection.

The public record concerning these regulations will be maintained in the Bureau of Export Administration Freedom of Information Records Inspection Facility, Room 4525, Department of Commerce, 14th Street and Pennsylvania Avenue, NW, Washington, DC 20230. Records in this facility, including written public comments and memoranda summarizing the substance of oral communications, may be inspected and copied in accordance with regulations published in Part 4 of Title 15 of the Code of Federal Regulations (CFR). Information about the inspection and copying of records at the facility may be obtained from Margaret Cornejo, Bureau of Export Administration Freedom of Information Officer, at the above address or by calling (202) 482-5653.

List of Subjects

15 CFR Parts 732, 740, 743, 748, 750, and 752

Administrative practice and procedure, Exports, Foreign trade, Reporting and recordkeeping requirements.

15 CFR Part 734

Administrative practice and procedure, Exports, Foreign trade.

15 CFR Parts 742, 770, 772 and 774

Exports, foreign trade.

Accordingly, 15 CFR chapter VII, subchapter C, is amended as follows:

1. The authority citation for 15 CFR parts 732, 740, 748, 752 and 772 continues to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

2. The authority citation for 15 CFR part 734 continues to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

3. The authority citation for 15 CFR part 742 continues to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; 18 U.S.C. 2510 et seq.;

[[Page 50520]]

22 U.S.C. 3201 et seq.; 42 U.S.C. 2139a; E.O. 12058, 43 FR 20947, 3 CFR, 1978 Comp., p. 179; E.O. 12851, 58 FR 33181, 3 CFR, 1993 Comp., p. 608; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

4. The authority citation for 15 CFR part 743 continues to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

5. The authority citation for 15 CFR part 750 continues to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; Notice of August 15, 1995 (60 FR 42767, August 17, 1995); E.O. 12981, 60 FR 62981; Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

6. The authority citation for 15 CFR part 770 continues to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

7. The authority citation for 15 CFR part 774 continues to read as follows:

Authority: 50 U.S.C. app. 2401 et seq.; 50 U.S.C. 1701 et seq.; 10 U.S.C. 7420; 10 U.S.C. 7430(e); 18 U.S.C. 2510 et seq.; 22 U.S.C. 287c; 22 U.S.C. 3201 et seq.; 22 U.S.C. 6004; Sec. 201, Pub. L. 104-58, 109 Stat. 557 (30 U.S.C. 185(s)); 30 U.S.C. 185(u); 42 U.S.C. 2139a; 42 U.S.C. 6212; 43 U.S.C. 1354; 46 U.S.C. app. 466c; 50 U.S.C. app. 5; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

PART 732--[AMENDED]

Sec. 732.2 [Amended]

8. Section 732.2(d) amended by revising the phrase ``ECCN 5A002 or ECCN 5D002" to read ``ECCNs 5A002, 5D002 or 5E002".

Sec. 732.3 [Amended]

9. Section 732.3(e)(2) is amended by revising the phrase ``ECCN 5A002 or ECCN 5D002" to read ``ECCNs 5A002, 5D002 or 5E002".

PART 734--[AMENDED]

10. Section 734.2 is amended by revising paragraph (b)(9)(ii) to read as follows:

Sec. 734.2 Important EAR terms and principles.

(a) * * *
(b) * * *
(9) * * *

(ii) The export of encryption source code and object code software controlled for EI reasons under ECCN 5D002 on the Commerce Control List (see Supplement No. 1 to part 774 of the EAR) includes downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S. (except Canada), or making such software available for transfer outside the United States (except Canada), over wire, cable, radio, electromagnetic, photo optical, photoelectric or other comparable communications facilities accessible to persons outside the United States (except Canada), including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States or Canada. Such precautions shall include ensuring that the facility from which the software is available controls the access to and transfers of such software through such measures as:

(A) The access control system, either through automated means or human intervention, checks the address of every system requesting or receiving a transfer and verifies that such systems are located within the United States or Canada;

(B) The access control system provides every requesting or receiving party with notice that the transfer includes or would include cryptographic software subject to export controls under the Export Administration Regulations, and that anyone receiving such a transfer cannot export the software without a license; and

(C) Every party requesting or receiving a transfer of such software must acknowledge affirmatively that he or she understands that the cryptographic software is subject to export controls under the Export Administration Regulations and that anyone receiving the transfer cannot export the software without a license. BXA will consider acknowledgments in electronic form provided that they are adequate to assure legal undertakings similar to written acknowledgments.

* * * * *

Sec. 734.4 [Amended]

11. Section 734.4 is amended by revising the phrase ``ECCN, 5A002, ECCN 5D002, and 5E002" in paragraph (b)(2) to read ``ECCNs 5A002, 5D002, and 5E002".

PART 740--[AMENDED]

12. Section 740.3 is amended by adding a new paragraph (d)(5) to read as follows:

Sec. 740.3 Shipments of limited value (LVS).

* * * * *

(d) * * *

(5) Exports of encryption items. For components or spare parts controlled for ``EI" reasons under ECCN 5A002, exports under this License Exception must be destined to support an item previously authorized for export.

* * * * *

13. Section 740.6 is amended by revising the first sentence in paragraph (a)(3) to read as follows:

Sec. 740.6 Technology and software under restriction (TSR).

(a) * * *
(3) Form of written assurance. The required assurance may be made in the form of a letter or any other written communication from the importer, including communications via facsimile, or the assurance may be incorporated into a licensing agreement that specifically includes the assurances. * * *
* * * * *

14. Section 740.8 is amended:
(a) By revising paragraph (b)(2);
(b) By revising the phrase ``recovery encryption software and equipment'' in paragraph (d)(1) to read ``recoverable encryption items'';
(c) By revising the phrase ``March 1 and no later than September 1'' in paragraph (e)(2) to read ``February 1 and no later than August 1'', as follows:

Sec. 740.8 Key management infrastructure.

* * * * *

(b) * * *
(2)(i) Non-recoverable encryption commodities and software. Eligible items are non-recoverable 56-bit DES or equivalent strength commodities and software controlled under ECCNs 5A002 and 5D002 that are made eligible as a result of a one-time BXA review. You may initiate this review by submitting a classification request for your product in accordance with paragraph (d)(2) of this section.
(ii) Non-recoverable financial-specific encryption commodities and software of any key length. (A)(1) After a one-time technical review through a classification request (see Sec. 748.3 of the EAR), non-recoverable, financial-specific encryption software (which is not eligible under the provisions of License Exception TSU for mass market software such as SET or similar protocols); and commodities of any key length that are

[[Page 50521]]

restricted by design (e.g., highly field-formatted with validation procedures, and not easily diverted to other end-uses) for financial applications to secure financial communications/transactions for end-uses such as financial transfers, or electronic commerce will be permitted under License Exception KMI for export and reexport to all destinations except Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.
(2) For such classification requests, indicate ``License Exception KMI'' in block #9 on Form BXA748P. Submit the original request to BXA in accordance with Sec. 748.3 of the EAR and send a copy of the request to: Attn: Financial Specific Encryption Request Coordinator, P.O. Box 246, Annapolis Junction, MD 20701-0246.
(B) Upon approval of your classification request for a non-recoverable financial-specific encryption commodities or software, you will become eligible to use License Exception KMI. This approval allows the export or reexport of encryption commodities and software specifically designed and limited for use in the processing of electronic financial (commerce) transactions, which implements cryptography in specifically delineated fields such as merchant's identification, the customer's identification and address, the merchandise purchased, and the payment mechanism. It does not allow for

encryption of data, text or other media except as directly related to these elements of the electronic transaction to support financial communications/transactions. For exports and reexports under the provisions of this paragraph (b)(2)(ii), no business and marketing plan is required, and the reporting requirements of paragraph (e) of this section and the criteria described in Supplement Nos. 4 and 5 to part 742 of the EAR are not applicable. However, you are subject to the reporting requirements of the Wassenaar Arrangement (see Sec. 743.1 of the EAR)

(iii) General purpose non-recoverable encryption commodities or software of any key length for use by banks/financial institutions. (A)(1) After a one-time technical review through a classification request (see Sec. 748.3 of the EAR), exports and reexports of general purpose non-recoverable non-voice encryption commodities or software of any key length will be permitted under License Exception KMI for distribution to banks and financial institutions as defined in part 772 of the EAR in all destinations listed in Supplement No. 3 to part 740 of the EAR, and to branches of such banks and financial institutions wherever located. The end-use is limited to secure business financial communications or transactions and financial communications/ transactions between the bank and/or financial institution and its customers. No customer to customer communications/transactions are permitted.

(2) For such classificiation requests, indicate ``License Exception KMI'' in block #9 on Form BXA748P. Submit the original request to BXA in accordance with Sec. 748.3 of the EAR and send a copy of the request to: Attn: Financial Specific Encryption Request Coordinator, P.O. Box 246, Annapolis Junction, MD 20701-0246.

(3) Upon approval of your classification request for a non-recoverable financial-specific encryption commodities or software, you will become eligible to use License Exception KMI.

(B) Software and commodities that have already received a one-time technical review through a classification request or have been licensed for export under an Encryption Licensing Arrangement or a license are eligible for export under the provisions of this paragraph (b)(2)(iii) without an additional one-time technical review.

(C) Software and commodities that have already been approved under an Encryption Licensing Arrangement to banks and financial institutions in specified countries may now be exported or reexported to other banks and financial institutions in those countries under the same Encryption Licensing Arrangement.

(D) For exports and reexports under the provisions of this paragraph (b)(2)(iii), no business and marketing plan is required and the reporting requirements of paragraph (e) of this section are not applicable. However, you are subject to the reporting requirements of the Wassenaar Arrangement (see Sec. 743.1 of the EAR).

* * * * *

15. Section 740.9 is amended:

a. By revising paragraph (a)(2)(i);

b. By revising the reference to ``Sec. 740.9(a)'' in paragraph (a)(2)(ii)(C) to read ``Sec. 740.10(a)'';

c. By revising the reference to ``under Sec. 740.8(b)(1)'' in the introductory text of paragraph (b)(1)(iii) to read ``under this paragraph (b)(1)''; and

d. By adding a new paragraph (a)(2)(ix) to read as follows:

Sec. 740.9 Temporary imports, exports, and reexports (TMP).

* * * * *

(a) * * *

(2) * * *

(i) Tools of trade. Usual and reasonable kinds and quantities of tools of trade (commodities and software) for use by the exporter or employees of the exporter in a lawful enterprise or undertaking of the exporter. Eligible tools of trade may include, but are not limited to, such equipment and software as is necessary to commission or service goods, provided that the equipment or software is appropriate for this purpose and that all goods to be commissioned or serviced are of foreign origin, or if subject to the EAR, have been legally exported or reexported. The tools of trade must remain under the effective control of the exporter or the exporter's employee (see part 772 of the EAR for a definition of ``effective control"). The shipment of tools of trade may accompany the individual departing from the United States or may be shipped unaccompanied within one month before the individual's departure from the United States, or at any time after departure. No tools of the trade may be taken to Country Group E:2 (see Supplement No. 1 to part 740) or Sudan. For exports under this License Exception of laptop computers loaded with encryption software, refer to item interpretation 13 in Sec. 770.2 of the EAR.

* * * * *

(ix) Temporary exports to a U.S. subsidiary, affiliate or facility in Country Group B. (A) Components, parts, tools or test equipment exported by a U.S. person to its subsidiary, affiliate or facility in a country listed in Country Group B (see Supplement No. 1 to this part) that is owned or controlled by the U.S. person, if the components, part, tool or test equipment is to be used for manufacture, assembly, testing, production or modification, provided that no components, parts, tools or test equipment or the direct product of such components, parts, tools or test equipment are transferred or reexported to a country other than the United States from such subsidiary, affiliate or facility without prior authorization by BXA.

(B) For purposes of this paragraph (a)(2)(ix), U.S. person is defined as follows: an individual who is a citizen of the United States, an individual who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(2) or an individual who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). U.S. person also means any juridical person organized under the laws of the United States, or any jurisdiction within the United States (e.g., corporation, business association, partnership, society, trust, or any other entity, organization or group that is

[[Page 50522]]

incorporated to do business in the United States).

* * * * *

Sec. 740.10 [Amended]

16. Section 740.10 is amended by revising the reference to ``Sec. 740.8(a)(2)(ii)" in paragraph (a)(2)(i) to read ``Sec. 740.9(a)(2)(ii)".

17. Section 740.11 is amended by adding new paragraph (a)(3) to read as follows:

Sec. 740.11 Governments and international organizations (GOV).

* * * * *

(a) International safeguards. * * *

(3) No encryption items controlled for EI reasons under ECCNs 5A002, 5D002, or 5E002 may be exported under the provisions of this

paragraph (a).

* * * * *

18. Section 740.14 is amended by revising paragraphs (a), (b), and (c); by adding a sentence to the end of paragraph (d); and by adding paragraph (f) to read as follows:

Sec. 740.14 Baggage (BAG).

(a) Scope. This License Exception authorizes individuals leaving the United States either temporarily (i.e., traveling) or longer-term (i.e., moving) and crew members of exporting or reexporting carriers to take to any destination, as personal baggage, the classes of commodities and software described in this section.

(b) Eligibility. Individuals leaving the United States may export or reexport any of the following commodities or software for personal use of the individuals or members of their immediate families traveling with them to any destination or series of destinations. Individuals leaving the United States temporarily (i.e., traveling) must bring back items exported and reexported under this License Exception unless they consume the items abroad or are otherwise authorized to dispose of them under the EAR. Crew members may export or reexport only commodities and software described in paragraphs (b)(1) and (b)(2) of this section to any destination.

(1) Personal effects. Usual and reasonable kinds and quantities for personal use of wearing apparel, articles of personal adornment, toilet articles, medicinal supplies, food, souvenirs, games, and similar personal effects, and their containers.

(2) Household effects. Usual and reasonable kinds and quantities for personal use of furniture, household effects, household furnishings, and their containers.

(3) Vehicles. Usual and reasonable kinds and quantities of vehicles, such as passenger cars, station wagons, trucks, trailers, motorcycles, bicycles, tricycles, perambulators, and their containers.

(4) Tools of trade. Usual and reasonable kinds and quantities of tools, instruments, or equipment and their containers for use in the trade, occupation, employment, vocation, or hobby of the traveler or members of the household being moved. For special provisions regarding encryption items subject to EI controls, see paragraph (f) of this section.

(c) Limits on eligibility. The export of any commodity or software is limited or prohibited, if the kind or quantity is in excess of the limits described in this section. In addition, the commodities or software must be:

(1) Owned by the individuals (or by members of their immediate families) or by crew members of exporting carriers on the dates they depart from the United States;

(2) Intended for and necessary and appropriate for the use of the individuals or members of their immediate families traveling with them, or by the crew members of exporting carriers;

(3) Not intended for sale or other disposal; and

(4) Not exported under a bill of lading as cargo if exported by crew members.

(d) * * * No items controlled for EI reasons may be exported or reexported as unaccompanied baggage.

* * * * *

(f) Special provisions: encryption software subject to EI controls.

(1) Only a U.S. citizen or permanent resident as defined by 8 U.S.C. 1101(a)(20) may permanently export or reexport encryption items controlled for EI reasons under this License Exception.

(2) The U.S. citizen or permanent resident must maintain effective

control of the encryption items controlled for EI reasons.

(3) The encryption items controlled for EI reasons may not be exported or reexported to Country Group E:2, Iran, Iraq, Sudan, or Syria.

19. New Supplement No. 3 is added to read as follows:

Supplement No. 3 To Part 740--Countries Eligible To Receive General Purpose Encryption Commodities and Software for Banks and Financial Institutions

Anguilla
Antigua
Argentina
Aruba
Australia
Austria
Bahamas
Barbados
Belgium
Brazil
Canada
Croatia
Denmark
Dominica
Ecuador
Finland
France
Germany
Greece
Hong Kong
Hungary
Iceland
Ireland
Italy
Japan
Kenya
Luxembourg
Monaco
Netherlands
New Zealand
Norway
Poland
Portugal
St. Kitts & Nevis
St. Vincent/Grenadines
Seychelles
Singapore
Spain
Sweden
Switzerland
Trinidad & Tobago
Turkey
Uruguay
United Kingdom

PART 742--[AMENDED]

20. Section 742.15 is amended:

a. By revising paragraph (b)(1);

b . By revising the phrase ``up to 56-bit key length DES or equivalent strength'' to read ``56-bit DES or equivalent'' in paragraph (b)(3) wherever it appears;

c.-d. By revising the phrase ``The use of License Exception KMI'' in the seventh sentence of paragraph (b)(3)(i) to read ``Authorization to use License Exception KMI';

e. By redesignating paragraphs (b)(4) and (5) as (b)(6) and (7);

f. By adding new paragraphs (b)(4) and (b)(5); and

g. By revising newly designated paragraph (b)(6)(i) to read as follows:

Sec. 742.15 Encryption items.

* * * * *

(b) * * *

(1) Certain mass-market encryption software. (i) Consistent with E.O. 13026 of November 15, 1996 (61 FR 58767), certain encryption software that was transferred from the U.S. Munitions List to the Commerce Control List pursuant to the Presidential Memorandum of November 15, 1996 may be released from EI controls and thereby made eligible for mass market treatment after a one-time technical review. To determine eligibility for mass market

[[Page 50523]]

treatment, exporters must submit a classification request to BXA. 40-bit mass market encryption software using RC2 or RC4 may be eligible for a 7-day review process, and company proprietary software or 40-bit DES implementations may be eligible for 15-day processing. Refer to Supplement No. 6 to part 742 and Sec. 748.3(b)(3) of the EAR for additional information. Note that the one-time technical review is for a determination to release encryption software in object code only unless otherwise specifically requested. Exporters requesting release of the source code should refer to paragraph (b)(3)(v)(E) of Supplement No. 6 to part 742.

(ii) If, after a one-time technical review, BXA determines that the software is released from EI controls, such software is eligible for all provisions of the EAR applicable to other software, such as License Exception TSU for mass-market software. Furthermore, for such software released from EI controls, subsequent bundling, updates, or releases consisting of or incorporating this software may be exported and reexported without a separate one-time technical review, so long as the functional encryption capacity (e.g., algorithm, key modulus) of the originally reviewed mass-market encryption software has not been modified or enhanced. However, if BXA determines that the software is not released from EI controls, a license is required for export and reexport to all destinations, except Canada, and license applications will be considered on a case-by-case basis.

(2) * * *

(3) * * *

(4) General purpose non-recoverable encryption commodities or software of any key length for use by banks/financial institutions. (i) Commodities and software that have already received a one-time technical review through a classification request or have been licensed for export under an Encryption Licensing Arrangement or a license are eligible for export under License Exception KMI (see Sec. 740.8(b)(2)(iii) of the EAR) without an additional one-time technical review, providing that the export meets all the terms and conditions of License Exception KMI.

(ii) For exports not eligible under License Exception KMI, exports of general purpose non-recoverable non-voice encryption commodities or software of any key length will be permitted under an Encryption Licensing Arrangement for use by banks and financial institutions as defined in part 772 of the EAR in all destinations except Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan. No business or marketing plan is required. Applications for such commodities and software will receive favorable consideration when the end-use is limited to secure business financial communications or transactions and financial communications/ transactions between the bank and/or financial institution and its customers, and provided that there are no concerns about the country or financial end-user. No customer to customer communications or transactions are allowed. Furthermore, licenses for such exports will require the license holder to report to BXA information concerning the export such as export control classification number, number of units in the shipment, and country of ultimate destination. Note that any country or end-user prohibited to receive encryption commodities and software under a specific Encryption Licensing Arrangement is reviewed on a case-by-case basis, and may be considered by BXA for eligibility under future Encryption Licensing Arrangement requests.

(5) Non-recoverable financial-specific encryption items of any key length. After a one-time technical review via a classification request, non-recoverable financial-specific encryption items of any key length that are restricted by design (e.g. highly field-formatted and validation procedures, and not easily diverted to other end-uses) for financial applications will be permitted for export and reexport under License Exception KMI (see Sec. 740.8 of the EAR). No business and marketing plan is required.

(6) All other encryption items. (i) Encryption licensing arrangement. Applicants may submit license applications for exports and reexports of certain encryption commodities and software in unlimited quantities for all destinations except Cuba, Iran, Iraq, Libya, North Korea, Syria, and Sudan. Applications will be reviewed on a case-by-case basis. If approved, encryption licensing arrangements may be valid for extended periods as requested by the applicant in block #24 on Form BXA-748P. In addition, the applicant must specify the sales territory and class(es) of end-user(s). Such licenses may require the license holder to report to BXA certain information such as ECCN, item description, quantity, and end-user name and address.

* * * * *

21. Part 742 is amended by revising Supplement Nos. 4 and 6 to read as follows:

Supplement No. 4 to Part 742--Key Escrow or Key Recoverable Products Criteria

Key Recoverable Feature

(1) The key(s) or other material/information required to decrypt ciphertext shall be accessible through a key recoverable feature.

(2) The product's cryptographic functions shall be inoperable until the key(s) or other material/information required to decrypt ciphertext is recoverable by government officials under proper legal authority and without the cooperation or knowledge of the user.

(3) The output of the product shall automatically include, in an accessible format and with a frequency of at least once every three hours, the identity of the key recovery agent(s) and information sufficient for the key recovery agent(s) to identify the key(s) or other material/information required to decrypt the ciphertext.

(4) The product's key recoverable functions shall allow access to the key(s) or other material/information needed to decrypt the

ciphertext regardless of whether the product generated or received the ciphertext.

(5) The product's key recoverable functions shall allow for the recovery of all required decryption key(s) or other material/ information required to decrypt ciphertext during a period of authorized access without requiring repeated presentations of access authorization to the key recovery agent(s).

Interoperability Feature

(6) The product's cryptographic functions may:

(i) Interoperate with other key recoverable products that meet these criteria, and shall not interoperate with products whose key recovery feature has been altered, bypassed, disabled, or otherwise rendered inoperative;

(ii) Send information to non-key recoverable products only when assured access is permitted to the key(s) or other material/ information needed to decrypt ciphertext generated by the key recoverable product. Otherwise, key length is restricted to less than or equal to 56-bit DES or equivalent.

(iii) Receive information from non-key recoverable products with a key length restricted to less than or equal to 56-bit DES or equivalent.

Design, Implementation and Operational Assurance

(7) The product shall be resistant to efforts to disable or circumvent the attributes described in criteria one through six.

(8) The product's cryptographic function's key(s) or other material/information required to decrypt ciphertext shall be escrowed with a key recovery agent(s) (who may be a key recovery agent(s) internal to the user's organization) acceptable to BXA, pursuant to the criteria in supplement No. 5 to part 742. Since the establishment of a key management infrastructure and key recovery agents may take some time, BXA will, while the infrastructure is being built, consider exports of key recoverable encryption products which facilitate establishment of the key management infrastructure before a key recovery agent is named.

[[Page 50524]]

Supplement No. 6 To Part 742--Guidelines for Submitting a Classification Request for a Mass Market Software Product That Contains Encryption

Classification requests for release of certain mass market encryption software from EI controls must be submitted on Form BXA-748P, in accordance with Sec. 748.3 of the EAR. To expedite review of the request, clearly mark the envelope ``Attn.: Mass Market Encryption Software Classification Request". In Block 9: Special Purpose of the Form BXA-748P, you must insert the phrase ``Mass Market Encryption Software. Failure to insert this phrase will delay processing. In addition, the Bureau of Export Administration recommends that such requests be delivered via courier service to: Bureau of Export Administration, Office of Exporter Services, Room 2705, 14th Street and Pennsylvania Ave., NW, Washington, DC 20230.

In addition, send a copy of the request and all supporting documents by Express Mail to: Attn: Mass Market Encryption Request Coordinator, P.O. Box 246, Annapolis Junction, MD 20701-0246.

(a) Requests for mass market encryption software that meet the criteria in paragraph (a)(2) of this Supplement will be processed in seven (7) working days from receipt of a properly completed request. Those requests for mass market encryption software that meet the criteria of paragraph (a)(1) of this supplement only will be processed in fifteen (15) working days from receipt of a properly completed request. When additional information is requested, the request will be processed within 15 working days of the receipt of the requested information.

(1) A mass market software product that meets all the criteria established in this paragraph will be processed in fifteen (15) working days from receipt of the properly completed request:

(i) The commodity must be mass market software. Mass market software is computer software that is available to the public via sales from stock at retail selling points by means of over-the-counter transactions, mail order transactions, or telephone call transactions;

(ii) The software must be designed for installation by the user without further substantial support by the supplier. Substantial support does not include telephone (voice only) help line services for installation or basic operation, or basic operation training provided by the supplier; and

(iii) The software includes encryption for data confidentiality.

(2) A mass market software product that meets all the criteria established in this paragraph will be processed in seven (7) working days from receipt of the properly completed request:

(i) The software meets all the criteria established in paragraph (a)(1)(i) through (iii) of this supplement;

(ii) The data encryption algorithm must be RC4 or RC2 with a key space no longer than 40-bits. The RC4 and RC2 algorithms are proprietary to RSA Data Security, Inc. To ensure that the subject software is properly licensed and correctly implemented, contact RSA Data Security, (415) 595-8782;

(iii) If any combination of RC4 or RC2 are used in the same software, their functionality must be separate. That is, no data can be operated sequentially on by both routines or multiply by either routine;

(iv) The software must not allow the alteration of the data encryption mechanism and its associated key spaces by the user or any other program;

(v) The key exchange used in data encryption must be:

(A) A public key algorithm with a key space less than or equal to a 512-bit modulus and/or;

(B) A symmetrical algorithm with a key space less than or equal to 64-bits; and

(vi) The software must not allow the alteration of the key management mechanism and its associated key space by the user or any other program.

(b) To submit a classification request for a product that is eligible for the seven-day handling, you must provide the following information in a cover letter to the classification request. Send the original to the Bureau of Export Administration. Send a copy of the application and all supporting documentation by Express Mail to: Attn.: Mass Market Encryption Request Coordinator, P.O. Box 246, Annapolis Junction, MD 20701-0246.

Instructions for the preparation and submission of a classification request that is eligible for seven day handling are as follows:

(1) If the software product meets the criteria in paragraph (a)(2) of this supplement, you must call the Department of Commerce on (202) 482-0092 to obtain a test vector, or submit to BXA a copy

of the encryption subsystem source code. The test vector or source code must be used in the classification process to confirm that the software has properly implemented the approved encryption algorithms.

(2) Upon receipt of the test vector, the applicant must encrypt the test plain text input provided using the commodity's encryption routine (RC2 and/or RC4) with the given key value. The applicant should not pre-process the test vector by any compression or any other routine that changes its format. Place the resultant test cipher text output in hexadecimal format on an attachment to form BXA-748P.

(3) You must provide the following information in a cover letter to the classification request:

(i) Clearly state at the top of the page ``Mass Market Encryption Software--7 Day Expedited Review Requested'';

(ii) State that you have reviewed and determined that the software subject to the classification request meets the criteria of paragraph (a)(2) of this supplement;

(iii) State the name of the single software product being submitted for review. A separate classification request is required for each product;

(iv) State how the software has been written to preclude user modification of the encryption algorithm, key management mechanism, and key space;

(v) Provide the following information for the software product:

(A) Whether the software uses the RC2 or RC4 algorithm and how the algorithm(s) is used. If any combination of these algorithms are used in the same product, also state how the functionality of each is separated to assure that no data is operated by more than one algorithm;

(B) Pre-processing information of plaintext data before encryption (e.g. the addition of clear text header information or compression of the data);

(C) Post-processing information of cipher text data after encryption (e.g. the addition of clear text header information or packetization of the encrypted data);

(D) Whether a public key algorithm or a symmetric key algorithm is used to encrypt keys and the applicable key space;

(E) For classification requests regarding source code:

(1) Reference the applicable executable product that has already received a one-time technical review;

(2) Include whether the source code has been modified by deleting the encryption algorithm, its associated key management routine(s), and all calls to the algorithm from the source code, or by providing the encryption algorithm and associated key management routine(s) in object code with all calls to the algorithm hidden. You must provide the technical details on how you have modified the source code;

(3) Include a copy of the sections of the source code that contain the encryption algorithm, key management routines, and their related calls; and

(F) Provide any additional information which you believe would assist in the review process.

(c) Instructions for the preparation and submission of a classification request that is eligible for 15-day handling are as follows:

(1) If the software product meets only the criteria in paragraph (a)(1) of this supplement, you must prepare a classification request. Send the original to the Bureau of Export Administration. Send a copy of the application and all supporting documentation by

Express Mail to: Attn.: Mass Market Encryption Request Coordinator, P.O. Box 246, Annapolis Junction, MD 20701-0246.

(2) You must provide the following information in a cover letter to the classification request:

(i) Clearly state at the top of the page ``Mass Market Software and Encryption: 15-Day Expedited Review Requested';

(ii) State that you have reviewed and determined that the software subject of the classification request, meets the criteria of paragraph (a)(1) of this supplement;

(iii) State the name of the single software product being submitted for review. A separate classification request is required for each product;

(iv) State that a duplicate copy, in accordance with paragraph (c)(1) of this supplement, has been sent to the 15-day Encryption Request Coordinator; and

(v) Ensure that the information provided includes brochures or other documentation or specifications relating to the software, as well as any additional information which you believe would assist in the review process.

(3) Contact the Bureau of Export Administration on (202) 482-0092 prior to

[[Page 50525]]

submission of the classification to facilitate the submission of proper documentation.

PART 743--[AMENDED]

Sec. 743.1 [Amended]

22. Section 743.1 is amended by revising the phrase ``and GOV'' in paragraph (b) to read ``GOV and KMI (under the provisions of Sec. 740.8(b)(2)(ii) and (iii) only''.

PART 748--[AMENDED]

23. Section 748.9 is amended by revising paragraph (a)(7) and by adding new paragraph (a)(8) to read as follows:

Sec. 748.9 Support documents for license applications.

(a) * * *

(7) The license application is submitted to export or reexport software or technology.

(8) The license application is submitted to export or reexport encryption items controlled under ECCNs 5A002, 5B002, 5D002 and 5E002.

* * * * *

24. Section 748.10 is amended by revising paragraph (b)(1) to read as follows:

Sec. 748.10 Import and End-User Certificates.

* * * * *

(b) * * *

(1) Any commodities on your license application are controlled for national security (NS) reasons, except for items controlled under ECCN 5A002 or 5B002;

* * * * *

PART 750--[AMENDED]

25. Section 750.3 is amended by revising paragraph (b)(2)(i) to read as follows:

Sec. 750.3 Review of license applications by BXA and other government agencies and departments.

* * * * *

(b) * * *

(2) * * *

(i) The Department of Defense is concerned primarily with items controlled for national security and regional stability reasons and with controls related to encryption items;

* * * * *

26. Section 750.7 is amended:

a. By redesignating paragraphs (c) introductory text through (c)(5) as (c)(1) introductory text through (c)(1)(v);

b. By redesignating paragraphs (c)(6) introductory text through (c)(6)(v) as (c)(1)(vi) introductory text through (c)(1)(vi)(E);

c. By redesignating paragraphs (c)(7) and (8) as (c)(1)(vii) and (viii); and

d. By adding a new paragraph (c)(2) to read as follows:

Sec. 750.7 Issuance of licenses.

* * * * *

(c) * * *

(2)(i) For Encryption Licensing Arrangements issued by BXA for exports and reexports of items controlled under ECCN 5A002, 5B002, and 5D002, and for encryption commodities and software previously on the U.S. Munitions List and currently authorized for export or reexport under a State Department license, distribution arrangement or any other authority of the State Department, you must by letter to BXA a request for approval of any additional country of destination.

(ii) Letters requesting changes pursuant to paragraph (c)(2)(i) of this section should be made by the license holder on company letterhead, clearly identifying the original license number and the requested change. In addition, requests for changes to State licenses or other authorizations must be accompanied by a copy of the original State license or authorization. The requested changes may not take effect until approved in writing by BXA. Send requests for changes to the following address: Office of Strategic Trade, Bureau of Export Administration, U.S. Department of Commerce, Room 2705, 14th Street and Pennsylvania Ave., NW, Washington, DC 20230, Attn: Encryption Division.

* * * * *

PART 752--[AMENDED]

27. Section 752.3 is amended by redesignating paragraphs (a)(5) through (a)(10) as (a)(6) through (a)(11) and adding a new paragraph (a)(5) to read as follows:

Sec. 752.3 Eligible items.

(a) * * *

(5) Items controlled for EI reasons on the CCL;

* * * * *

PART 758--[AMENDED]

28. Section 758.1 is amended by adding a new paragraph (e)(1)(i)(D) to read as follows:

Sec. 758.1 Export clearance requirements.

* * * * *

(e) * * *

(1) * * *

(i) * * *

(D) Exports of tools of trade under License Exception TMP or BAG.

* * * * *

PART 770--[AMENDED]

29. Section 770.2 is amended by revising the section title and adding a new paragraph (m) to read as follows:

Sec. 770.2 Item interpretations.

* * * * *

(m) Interpretation 13: Encryption software controlled for EI reasons. Encryption software controlled for EI reasons under ECCN 5D002 may be pre-loaded on a laptop and exported under the tools of trade provision of License Exception TMP or the personal use exemption under License Exception BAG, subject to the terms and conditions of such License Exceptions. This provision replaces the personal use exemption of the International Traffic and Arms Regulations (ITAR) that existed for such software prior to December 30, 1996. Neither License Exception TMP nor License Exception BAG contains a reporting requirement.

PART 772--[AMENDED]

30. Part 772 is amended by adding, in alphabetical order, new definitions for ``Bank", ``Effective control", ``Encryption licensing arrangement", and ``Financial Institution", and revising paragraph (b) under the definition of ``U.S. person" to read as follows:

* * * * *

Bank. Means any of the following:

(a) Bank, savings association, credit union, bank holding company, bank or savings association service corporation, Edge Act corporation, Agreement corporation, or any insured depository institution, which is organized under the laws of the United States or any State and regulated or supervised by a Federal banking agency or a State bank supervisor; or

(b) A company organized under the laws of a foreign country and regulated or supervised by a foreign bank regulatory or supervisory authority which engages in the business of banking, including without limitation, foreign commercial banks, foreign merchant banks and other foreign institutions that engage in banking activities usual in connection with the business of banking in the countries where such foreign institutions are organized or operating; or

(c) An entity engaged in the business of providing clearing or settlement services, that is, or whose members are, regulated or supervised by a Federal banking agency, a State bank supervisor, or a foreign bank regulatory or supervisory authority; or

(d) A branch or affiliate of any of the entities listed in paragraphs (a), (b), or

[[Page 50526]]

(c) of this definition, regulated or supervised by a Federal banking agency, a State bank supervisor or a foreign bank regulatory or supervisory authority; or

(e) An affiliate of any of the entities listed in paragraph (a), (b), (c), or (d) of this definition, engaged solely in the business of providing data processing services to a bank or financial institution, or a branch of such an affiliate.

* * * * *

Effective control. You maintain effective control over an item when you either retain physical possession of the item, or secure the item in such an environment as a hotel safe, a bonded warehouse, or a locked or guarded exhibition facility. Retention of effective control over an item is a condition of certain temporary exports and reexports.

Encryption licensing arrangement. A license that allows the export of specified products to specified destinations in unlimited quantities. In certain cases, exports are limited to specified end-users for specified end-uses. Generally, reporting of all sales of the specified products is required at six month intervals. This includes sales made under distribution arrangements and distribution and warehousing agreements that were previously issued by the Department of State for encryption items.

* * * * *

Financial Institution. Means any of the following:

(a) A broker, dealer, government securities broker or dealer, self-regulatory organization, investment company, or investment adviser, which is regulated or supervised by the Securities and Exchange Commission or a self-regulatory organization that is registered with the Securities and Exchange Commission; or

(b) A broker, dealer, government securities broker or dealer, investment company, investment adviser, or entity that engages in securities activities that, if conducted in the United States, would be described by the definition of the term ``self-regulatory organization" in the Securities Exchange Act of 1934, which is organized under the laws of a foreign country and regulated or supervised by a foreign securities authority; or

(c) A US board of trade that is designated as a contract market by the Commodity Futures Trading Commission or a futures commission merchant that is regulated or supervised by the Commodity Futures Trading Commission; or

(d) A US entity engaged primarily in the business of issuing a general purpose charge, debit, or stored value card, or a branch of, or affiliate controlled by, such an entity; or

(e) A branch or affiliate of any of the entities listed in paragraphs (a), (b), or (c) of this definition regulated or supervised by the Securities and Exchange Commission, the Commodity Futures Trading Commission, or a foreign securities authority; or

(f) An affiliate of any of the entities listed in paragraph (a), (b), (c), or (e) of this definition, engaged solely in the business of providing data processing services to one or more bank or financial institutions, or a branch of such an affiliate.

* * * * *

U.S. person. (a) * * *

(b) See also Secs. 740.9 and 740.14, and parts 746 and 760 of the EAR for definitions of ``U.S. person" that are specific to those parts.

* * * * *

PART 774--[AMENDED]

31. In Supplement No. 1 to part 774, Category 5--Telecommunications and Information Security is amended by revising ECCNs 5A002 and 5D002 to read as follows:

5A002 Systems, equipment, application specific ``assemblies", modules or integrated circuits for ``information security", and specially designed components therefor.

License Requirements

Reason for Control: NS, AT, EI.

Control(s)	Country chart
NS applies to entire entry...............	NS Column 1.
AT applies to entire entry...............	AT Column 1.

EI applies to encryption items transferred from the U.S. Munitions List to the Commerce Control List consistent with E.O. 13026 of November 15, 1996 (61 FR 58767) and pursuant to the Presidential Memorandum of that date. Refer to Sec. 742.15 of this subchapter.

License Requirement Notes: See Sec. 743.1 of the EAR for reporting requirements for exports of commodities controlled under 5A002 and exported under License Exceptions LVS or GOV.

License Exceptions

LVS: Yes: $500 for components and spare parts only. N/A for equipment.
GBS: N/A
CIV: N/A

List of Items Controlled

Unit: $ value
Related Controls: See also 5A992. This entry does not control: (a) ``Personalized smart cards" or specially designed components therefor, with any of the following characteristics: (1) Not capable of message traffic encryption or encryption of user-supplied data or related key management functions therefor; or (2) When restricted for use in equipment or systems excluded from control under the note to 5A002.c, or under paragraphs (b) through (h) of this note. (b) Equipment containing ``fixed" data compression or coding techniques; (c) Receiving equipment for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to the video, audio or management functions; (d) Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radiocommunications systems) that are not capable of end-to-end encryption; (e) Decryption functions specially designed to allow the execution of copy-protected ``software", provided the decryption functions are not user-accessible; (f) Access control equipment, such as automatic teller machines, self-service statement printers or point of sale terminals, that protects password or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities but does not allow for encryption of files or text, except as directly related to the password or PIN

protection; (g). Data authentication equipment that calculates a Message Authentication Code (MAC) or similar result to ensure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication; (h) Cryptographic equipment specially designed, developed or modified for use in machines for banking or money transactions, and restricted to use only in such transactions. Machines for banking or money transactions include automatic teller machines, self-service statement printers, point of sale terminals, or equipment for the encryption of interbanking transactions.

Related Definitions: For the control of global navigation satellite systems receiving equipment containing or employing decryption (i.e. GPS or GLONASS), see 7A005. Items:

a. Systems, equipment, application specific ``assemblies", modules or integrated circuits for ``information security", and specially designed components therefor:

a.1. Designed or modified to use ``cryptography" employing digital techniques to ensure ``information security";

a.2. Designed or modified to perform cryptoanalytic functions;

a.3. Designed or modified to use ``cryptography" employing analog techniques to ensure ``information security";

Note: 5A002.a.3 does not control the following:

1. Equipment using ``fixed" band scrambling not exceeding 8 bands and in which the transpositions change not more frequently than once every second;

2. Equipment using ``fixed" band scrambling exceeding 8 bands and in which the transpositions change not more frequently than once every ten seconds;

3. Equipment using ``fixed" frequency inversion and in which the transpositions change not more frequently than once every second;

[[Page 50527]]

4. Facsimile equipment;

5. Restricted audience broadcast equipment; and 6. Civil television equipment;

a.4. Designed or modified to suppress the compromising emanations of information-bearing signals;

Note: 5A002.a.4 does not control equipment specially designed to suppress emanations for reasons of health and safety.

a.5. Designed or modified to use cryptographic techniques to generate the spreading code for ``spread spectrum" or the hopping code for ``frequency agility" systems;

a.6. Designed or modified to provide certified or certifiable ``multilevel security" or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) or equivalent;

a.7. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion.

*****

5D002 Information Security--``Software".

License Requirements
Reason for Control: NS, AT, EI

Control(s)	Country chart
NS applies to entire entry...............	NS Column 1.
AT applies to entire entry...............	AT Column 1.

EI applies to encryption items transferred from the U.S. Munitions List to the Commerce Control List consistent with E.O. 13026 of November 15, 1996 (61 FR 58767) and pursuant to the Presidential Memorandum of that date. Refer to Sec. 742.15 of the EAR.

Note: Encryption software is controlled because of its functional capacity, and not because of any informational value of such software; such software is not accorded the same treatment under the EAR as other ``software''; and for the export licensing purposes encryption software is treated under the EAR in the same manner as a commodity included in ECCN 5A002. License Exceptions for commodities are not applicable.

Note: Encryption software controlled for EI reasons under this entry remains subject to the EAR even when made publicly available in accordance with part 734 of the EAR, and it is not eligible for the General Software Note (``mass market'' treatment under License Exception TSU for mass market software). After a one-time BXA review, certain encryption software may be released from EI controls and made eligible for the General Software Note treatment as well as other provisions of the EAR applicable to software. Refer to Sec. 742.15(b)(1) of the EAR, and Supplement No. 6 to part 742 of the EAR.

License Requirement Notes: See Sec. 743.1 of the EAR for reporting requirements for exports of software controlled under 5D002 and exported under License Exception GOV.

License Exceptions

CIV: N/A
TSR: N/A

List of Items Controlled

Unit: $ value
Related Controls: See also 5D992. This entry does not control ``software'' ``required'' for the ``use'' of equipment excluded from control under to 5A002 or ``software'' providing any of the functions of equipment excluded from control under 5A002.
Related Definitions: N/A
Items:
a. ``Software'' specially designed or modified for the ``development'', ``production'' or ``use'' of equipment or ``software'' controlled by 5A002, 5B002 or 5D002.
b. ``Software'' specially designed or modified to support ``technology'' controlled by 5E002.
c. Specific ``software'' as follows:
c.1. ``Software'' having the characteristics, or performing or simulating the functions of the equipment controlled by 5A002 or

5B002;
c.2. ``Software" to certify ``software" controlled by 5D002.c.1.

Dated: September 14, 1998.
R. Roger Majak,
Assistant Secretary for Export Administration.
[FR Doc. 98-25096 Filed 9-21-98; 8:45 am]
BILLING CODE 3510-33-P