



blackduck<sup>™</sup>

A Guide to  
Software Encryption Export Compliance



## Introduction

Why do you need a guide to software encryption export compliance? The reason is simple. A bevy of complex U.S. laws apply to exporting software containing encryption, and you need a guide to comply with those laws.

If you are an engineer, you know about encryption, and your company's legal staff or export compliance manager probably does not. They rely on you to tell them what encryption is in your software so they can properly document it to comply with the law. If you are an export compliance manager, you need to know enough about encryption export requirements to work with your engineering and legal staffs to ensure your export classifications are approved by the Government as necessary and are complete and accurate.

According to the Wikipedia, encryption "is the process of obscuring information to make it unreadable without special knowledge, sometimes referred to as scrambling". The term cryptography, which is often used synonymously with encryption, is defined as "the study of message secrecy".

In this paper we explain why you need to identify all of the encryption functions in your software – and the challenge that poses. Then we explain the need for an automated means to identify encryption functions and to guide you through the compliance process. Finally, we describe how Black Duck's exportIP system helps make your job easier.

## Encryption Is Everywhere

Encryption is everywhere – even where you might not expect it. Although most people don't know it, encryption is integral to our daily lives, and is embedded into ubiquitous software such as Microsoft's Word, Excel, and Internet Explorer. Most

modern software programs have some encryption functions. When you buy or sell over the Web, bank on line, check your frequent flier miles, or connect to your office using a virtual private network, you are using encryption. Encryption is essential to secure data from thieves and prying eyes, thus it is essential for online commerce.

## Why the Government Cares about Exporting Encryption

The U.S. government has designated encryption as a "dual-use" technology, meaning it can be used for both peaceful and military aims. Darryl W. Jackson, U.S. Assistant Secretary of Commerce for Export Enforcement explains the dual-use designation to exporters in a brochure ominously entitled Don't Let this Happen to You!: Actual Investigations of Export Control and Antiboycott Violations:

"The United States is preeminent in developing high technology items, and our economy depends upon legitimate international trade. You – the members of the exporting community – are on the front lines of protecting U.S. national security as you engage in such trade. Many of the items exported from the United States are dual-use goods; they have legitimate commercial applications, but can also be used in weapons of mass destruction, in conventional arms, or by terrorists."

The government attempts to balance encryption's vital role in commerce with its potential use by malevolent individuals and organizations to hide dangerous and illicit communications from law enforcement and national security agencies. Consider the importance deciphering code played in ending World War II and thus saving countless lives. Such is the challenge and responsibility of the

federal government to understand and manage the use of encryption.

Up until 1996, the government imposed draconian military product controls over exporting strong encryption, but this proved impractical with increased commercial use of encryption during the rise of the internet. After a series of liberalizations, today's export laws focus on disclosing information on new encryption products so the government knows what encryption is being exported rather than curtailing or forbidding that export – except to countries designated as state sponsors of terrorism (sometimes called the T-5 countries) Cuba, Iran, North Korea, Sudan, and Syria. Only military specific and a few types of commercial programs remain subject to strict controls.

According to renowned export lawyer Ben Flowe of the law firm Berliner, Corcoran & Rowe, U.S. export regulations are complex and subject to frequent changes. “We’ve had about nine different policy changes on encryption. We’ve gone from being unable to legally export any kind of encryption other than for military or banking applications – which didn’t really work with the rise of the Internet – to now where you can export virtually all products that have encryption functions. But usually if you have data encryption (beyond limited functions like just protecting PINs and passwords), you need to ask the government ‘May I?’.”

## Why You Should Know What Encryption Is In Your Code

It is important to identify all of the encryption in your code because you need that information to comply with export regulations. As an additional benefit, this information also helps ensure that the encryption code in your products meets


your corporate software licensing requirements. Although not an export issue, this is prudent corporate policy.

As it turns out, most encryption algorithms – even those widely available as open source code – are subject to export regulation. To give you a sense of what encryption is subject to regulation, here is an abbreviated list:

- open source cryptography libraries for C and C++, including OpenSSL, Libgcrypt, Crypto++, Bouncy Castle, BeeCrypt, and Botan
- built-in encryption libraries for Java and .NET (C#, et al.), which when called count as yours
- encryption libraries for Perl, Ruby, and Python
- RSA2, RSA4, Diffie-Hellman, AES, Blowfish, IDEA.

To their peril, many exporters don't actually know what encryption is in their code, and it's hard for them to find out. Companies rely on their engineers to tell them, but this poses a dilemma. Many engineers don't think open source derived encryption is regulated, so when asked to identify the encryption, they often don't think to list it. It is not unusual for engineers to say: “I'm sure it's not controlled because the encryption functions I got are from open sources, like open SSL. Everybody uses them.”

Unfortunately, they are mistaken. As export lawyer Ben Flowe explains: “Software is considered encryption software if it has any encryption function whatsoever. Often encryption is an ancillary or minor function,



but most software does have encryption functions. For example, if software connects to the Internet it usually has some encryption function, or it's calling on other products to do the encryption – and the regulations say if you have any encryption functions, even if it's the hair on the pimple on the butt of the elephant, it's treated as encryption software.”

To make matters even more challenging, encryption has a way of sneaking into code. According to Flowe: “We do a lot of work with blue chip companies, large and small, and even the best often find to their surprise that they've got an encryption function that was buried in a toolkit or somewhere that they didn't know about.”

Developers are often flummoxed about how the encryption got there, and after investigating discover that it came in the payload of open source components or SDKs used for other purposes. Finding these encryption components is hard because they take many forms, and are undetectable with existing tools or string searches.

But even encryption code that sneaks into your software without your knowledge is subject to U.S. government encryption export regulations. Export controls apply whether you know that you have encryption in your code or not. So knowing what encryption you have is essential for full compliance with the law.

## U.S. Government Encryption Export Regulations

Export regulations covering encryption software are spelled out in the U.S. Export Administration Regulations (referred to as “the” EAR), and these are enforced by the U.S. Commerce Department's Bureau of Industry and Security

(BIS). The EAR covers what you can export, to whom, and for what use. Determining factors include: encryption “strength”, function of encryption, destination country, intended use, and even the destination organization and users. The regulations have a reputation for being intimidating because they are long and complicated, and they have morphed many times since first being applied to all commercial encryption products in 1996.

The regulations address key areas of concern such as export to the designated terrorist supporting countries mentioned earlier, designated terrorist organizations (e.g., Al Qaeda and Hamas), and individuals on a Denied Persons List (DPL) maintained by BIS. Unique export restrictions apply to China, and regulations apply differently depending on the destination country (e.g., exports to Canada and EU member countries are subject to fewer requirements). Proprietary source code, network infrastructure products like firewalls and VPNs, software with an open cryptographic interface, and certain other products are subject to stricter controls than most products with encryption.

Surprising to many is the fact that software created by third-party offshore development partners is subject to export regulation. Although work products exchanged between a U.S. firm and a foreign subsidiary or subcontractor are exempt, code being developed by third parties is not. According to Flowe, “If a third party in another country is writing code for you, you need a license or a classification in order to export the draft code to them. Most companies are out of compliance with their offshore development and testing.”

## Why Care about Compliance?

Here's how the export approval process generally works. You file an application with BIS that they subsequently review to understand your encryption. BIS then applies one of several possible labels or classifications that determine the rules under which you can export.

Encryption code is assigned what is called an Export Control Classification Number (ECCN), and whether it is eligible for export under a License Exception (or export with No License Required), and under what conditions. Most software products qualify for a classification that lets you export with no license, or under a license exception. In these cases you can simply fill out your export shipping paperwork if required (it's not required for downloads) and you're done, for most exports.

"After you go through these hoops" says Flowe, "80 to 90 percent of software that has encryption functions can be exported legally without a license to all end users and all countries except the five currently embargoed terrorist supporting countries – but only if you go through this formal classification with the government. If you don't, you can still export it, but it's unlawful, and penalties on a strict liability basis can easily reach the statutory limit of \$50,000 per violation, and there are also criminal penalties. It's not that difficult to comply after you learn how, and the risk is fairly high if you don't."

Unfortunately, exporting without complying with regulations can lead to unpleasant consequences. If you export a software product and subsequently discover that the product contains encryption code, you must decide whether to voluntarily disclose what you know to the government. According to Flowe you

must "confess your violations, and explain why [the BIS] should treat you nicely, or you hold your breath for five years until the statute of limitations runs out." He goes on to warn that, "Once you have knowledge [of encryption in the exported code], you can't continue to do the same thing because unlawful exports becomes knowing and willful and criminal." This can lead to missed delivery dates, unhappy customers, and delayed payments.

## What You Need to Know

There are five essential questions you need to answer to get your encryption export house in order. They are:

- Are there any encryption components in this code?
- What are they?
- How do we legally export this product?
- Where can I export this software without a license?
- Can I get a license exception?

## How Can You Find Out?

There are two ways to gather the information needed to ensure that you properly comply with U.S. export regulations covering encryption - one is hard, and the other makes it easy.

The hard way requires you to perform laborious "string" searches, interview your engineers, and manually review code. It also requires hours of internal and/or external counsel time, lengthy review forms, and hit or miss BIS approvals (with long delays should BIS withhold or delay approval). Not only is this process laborious, expensive, and subject to error

– those involved usually have better things to do with their time.

The easy way involves a tool that automates the painstaking work required to identify all encryption components in your software, and walks you through the process of determining which laws apply to your code and what you need to do to get approval to export your software product legally.

## How exportIP Can Help

Black Duck's exportIP product offers an easy, reliable, and fast path to software encryption export compliance. The first and only solution of its kind, exportIP automatically analyzes your code, compares it to an enormous and continuously updated KnowledgeBase of encryption algorithms, and generates a complete list of the encryption algorithms in your source code. Once the encryption code is identified, exportIP walks you through a process to determine how to classify your encryption code, and how to complete and submit the proper export documentation to the Commerce Department to get approval to export under proper regulatory authorities.

Black Duck has compiled and constantly updates a library of encryption code that exportIP compares to your code. exportIP then identifies and reports on all code matches - down to a few lines of code. In essence we "boil the ocean" for you by searching the Internet and other sources for encryption code and collecting applicable code patterns, which we incorporate into our proprietary KnowledgeBase. This allows you to rely on us to do this very difficult and time consuming work and to catch

encryption functions that you otherwise might miss.

On the legal side Black Duck has transformed export encryption requirements into coded rubrics that underlie a business rules engine that guides you through the export encryption compliance process. Essentially we have captured the knowledge of a cadre of experienced export lawyers and embedded it into our easy-to-use tool.

Although exportIP does not completely replace a legal professional, it takes the drudgery out of encryption export compliance by automating much of the difficult foundation work compliance requires. Contextual help and prepackaged forms allow you as a non-lawyer to help with the compliance process in a way not possible until now.

After exportIP identifies an encryption algorithm, you can drill down and select the particular implementation and the key length used. Once that is done, exportIP determines which BIS and National Security Agency (NSA) export requirements apply and it generates a

*Figure 1: Sample exportIP Email Notification Form*

**Basic Info**  
Type: Type of notification being performed.  
No License Required (NLR)

\* **Submitter:** Name of submitter.  
John Smith

\* **Exporting organization:** Name of company or person exporting the encryption item.  
Black Duck Software

\* **Contact point:** Name of person to be the contact point about this encryption item.  
John Smith

\* **Phone number:** Phone number of the contact point for this encryption item.  
781-891-5000

**Fax number:** Fax number of the contact point for this encryption item.  
781-891-5101

**Manufacturer:** Name of the manufacturer, if relevant.  
Black Duck Software

\* **Product Name or Model Number:** Name of the product or model number including the encryption.  
Banking Application

**ECCN:** Export Control Classification Number  
5D992  
Save

**SUPPLEMENT 6 TO PART 742 OF THE EAR**

\* **Algorithms used:** Description of all the symmetric and asymmetric encryption algorithms and ke which encryption modes are supported(e.g., cipher feedback mode or cipher block chaining mode).

Name	Type	Key Length	Mode
DES	Symmetric Key	0-56 Bits	
EIGamal	Asymmetric/Public Key	0-512 Bits	
RSA	Asymmetric/Public Key	0-512 Bits	

\* **Key management algorithms used:** State the key management algorithms, including modulus size

“punch list” of instructions for how to achieve export compliance.

Based on the nature of the encryption algorithms found, the intended use of the software product, and your export destinations, exportIP instructs you as to which agencies must be notified before shipment, and streamlines the preparation and submission of notifications and applications for approval to BIS and NSA.

exportIP provides and explains a form that generates email notifying BIS as shown in Figure 1. This may be all that is required. Should you need to file for mass market approval or to qualify for export under a license exception, exportIP walks you through the necessary steps. For example, exportIP guides you through the BIS online license application form called SNAP-R, and it helps generate any required BIS and NSA email notification.

For auditing purposes, exportIP keeps a detailed work record so you can document what you have done. This is extremely useful, should questions or potential issues arise.

A number of factors have converged to make exportIP a reality, including the wealth of Internet-searchable information, the staggering amount of computing power now available, ubiquitous high-speed Internet access, and low cost storage.

## exportIP Makes Financial Sense

While it is clear that exportIP can make your life easier, how can this translate into value for your enterprise? Let’s start by examining some back-of-the-envelope calculations for a common scenario for completing the BIS 748P export license form.

Without exportIP, encryption export specialists tell us that it generally takes between six and twelve hours of an export compliance

*Figure 2: Estimated Cost Range for a Form BIS-748P Filing*

Job Title	Low-end			High-end		
	Hours	Hourly Rate	Total	Hours	Hourly Rate	Total
Export Manager	6	\$ 150	\$ 900	12	\$ 150	\$ 1,800
Engineer	10	\$ 90	\$ 900	40	\$ 90	\$ 3,600
Outside Counsel	3	\$ 400	\$ 1,200	20	\$ 400	\$ 8,000
<b>Value of Labor Saved</b>	<b>80%</b>	<b>\$ 2,400</b>				<b>\$ 10,720</b>

manager’s time, 10 to 40 hours of a quality engineer’s time, and three to 20 hours of an external lawyer’s time to complete BIS’ Form 847P. Given the average hourly rates for these professionals, as Figure 2 shows, we estimate that the average cost per filing is \$8.2K and the maximum exceeds \$13K.

Assuming you have to go through this process several times each year, the costs add up – and these estimates do not include the heady costs of resubmissions, updates, and periodic filings.

With exportIP in place, our experience shows that you can expect at least five times the personnel efficiency of current methods, which translates into a 80% percent or better labor savings. In addition, the exportIP-related time and cost savings multiply with each classification and license application, and exportIP reduces errors, so approvals have fewer reasons for delay.

But the real long-term payoff comes with having a better, more efficient export encryption compliance process. If you incorporate exportIP into your normal software design and build process, such as that shown in Figure 3, you will learn about encryption export issues early

in the game – and as with most such issues – the earlier you discover them, the lower the cost to fix them.

Export lawyer Ben Flowe recommends that software exporters incorporate encryption export compliance into a formalized process. “If a company makes an investment in export compliance and is doing the right things, they will be much better off in the long run. In the case of a violation, they are more likely to get a warning letter or pay a low fine than a company that doesn’t appear to understand the rules, or doesn’t give the impression that they care. The government understands that nobody’s perfect, but they want to see top management attention. They want to see that you have a compliance program – that you’re doing something to comply. If you have compliance processes and are applying sophisticated tools to it, they will be very impressed.

Consider a situation in which you are acquiring a software company to flesh out your product portfolio. If you do not know for certain what

Likewise, if you are cultivating OEM partnerships or looking to sell your enterprise, your interests could be seriously threatened if an OEM or acquisition partner discovers during the deal-making process that you accidentally failed to disclose or you misclassified some encryption code.

Unfortunately, companies could go bankrupt waiting to resolve issues with BIS. In fact, since 2000 some 30 percent of applications were “returned without action” because would-be exporters did something wrong. While such problems remain unresolved, it is dangerous at best to pursue an export-as-usual approach.

## Summary of exportIP Benefits

If exporting software is important to the future of your business, exportIP offers you an impressive array of benefits. Among these are that exportIP:

- Identifies more encryption code than other means, and brings to light any “accidental” or otherwise unknown use of encryption algorithms that could lead to future problems.
- Simplifies legal compliance by helping you determine and comply with the appropriate U.S. government export requirements.
- Reduces business risks associated with unknown encryption algorithms in your code, and reduces risks caused by improper encryption export compliance.
- Helps ensure that your products ship on time.
- Opens international markets by reducing encryption export violation concerns.

**Figure 3: exportIP-based Export Encryption Compliance Process**



encryption is in the acquired code and whether their export shipments have been made lawfully or unlawfully, you could be in for countless legal and business headaches. exportIP can thus be a very useful part of acquisition due diligence.

In a nutshell, by helping you find all the encryption components in your software and helping you navigate the labyrinth of legal code needed to make your products exportable, exportIP helps you reduce your business risks, reach distant markets faster, and open new international markets.

No other offering on the market today can make those claims.

© 2007 Black Duck Software, Inc. Black Duck Software, the Black Duck logo, protexIP and exportIP are trademarks of Black Duck Software, Inc. All other trademarks are property of their respective holders.



## Contact

To learn more, please contact:  
[sales@blackducksoftware.com](mailto:sales@blackducksoftware.com)  
or call +1 781.891.5100

Additional information is available  
at Black Duck's website:  
[www.blackducksoftware.com](http://www.blackducksoftware.com)