FORTRA™

**WHITE PAPER** (DIGITAL GUARDIAN)

# Digital Guardian For Data Protection And Export Control Compliance

## Executive Summary

This white paper:

- Explains how a context-aware data protection solution is capable of addressing a wide range of real-world use cases for export controlled products and services.
- Summarizes conceptually and technically how an enterprise deployment of a context-aware data protection solution facilitates security while maintaining productivity throughout highly complex workflows and collaborative ecosystems.
- Defines the elements of risk and cost associated with export control compliance and demonstrates how Fortra™'s Digital Guardian®'s unique design and technology support both compliance and productivity.

## ITAR And EAR Overview

International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) are federally mandated regulations interpreted and enforced by the United States Department of State and the Department of Commerce. These regulations control the export and sale of defense-related articles and services on the United States Munitions List (USML) as well as commercial or dual-use technologies on the Commerce Control List (CCL).

ITAR governs the import and export regulations of information and materials pertaining to defense and military-related technologies that are restricted to only U.S. citizens with proper security clearances, unless explicitly exempted by the Department of State. EAR governs the import and export of commercial items, many of which may be dual-use items that could be used for defense or national security purposes in addition to commercial use.

Together, ITAR and EAR define the lawful conditions under which sensitive scientific and technical information and materials that are considered critical to U.S. national security may be shared with foreign entities. Persons or companies that violate export control regulations face substantial civil and/or criminal penalties, which typically compel organizations to designate an internal Office of Export Control to ensure all products, services, and employees are in legal compliance.

## Export Control Compliance: Conditions, Costs, And Consequences

Before undertaking an export control compliance project it is essential to understand the extent to which your product, service, or technology is bound by ITAR and EAR. The United States Munitions List (USML) is divided into twenty categories of defense-related technology, from firearms to energetic materials (explosives), whose import and export are controlled. The Commerce Control List (CCL) helps you determine whether you need an export license. The list is divided into ten categories each of which is subdivided into five product groups. The CCL contains a broad list of dual-use items such as electronics that may be used for either commercial or military purposes. Adding further complexity is the overlap or conflict that often occurs between the USML and the CCL because dual-use items can be challenging to categorize. It is imperative, therefore, to carefully design, implement, document, and consistently enforce a data protection program across the entire business process. Such a program ensures that you know at all times exactly what, when, how, and by whom controlled data is handled in the event of an audit or an incident.

## Commerce Control List

### Categories

- 0 = Nuclear materials, facilities and equipment (and miscellaneous items).
- 1 = Materials, Chemicals, Microorganisms and Toxins
- 2 = Materials Processing
- 3 = Electronics
- 4 = Computers
- 5 = Telecommunications and Information Security
- 6 = Sensors and Lasers
- 7 = Navigation and Avionics
- 8 = Marine
- 9 = Propulsion Systems, Space Vehicles, and Related Equipment

### Product Groups

- A. Systems, Equipment and Components
- B. Test, Inspection and Production
- C. Material
- D. Software
- E. Technology

## The United States Munitions List

- I. Firearms, Close Assault Weapons and Combat Shotguns
- II. Guns and Armament
- III. Ammunition/Ordnance
- IV. Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines
- V. Explosives and Energetic Materials, Propellants, Incendiary Agents, and Their Constituents
- VI. Surface Vessels of War and Special Naval Equipment
- VII. Ground Vehicles
- VIII. Aircraft and Related Articles
- IX. Military Training Equipment and Training
- X. Personal Protective Equipment
- XI. Military Electronics
- XII. Fire Control, Range Finder, Optical and Guidance and Control Equipment
- XIII. Materials and Miscellaneous Articles
- XIV. Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
- XV. Spacecraft and Related Articles
- XVI. Nuclear Weapons Related Articles
- XVII. Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated
- XVIII. Directed Energy Weapons
- XIX. Gas Turbine Engines and Associated Equipment
- XX. Submersible Vessels and Related Articles
- XXI. Articles, Technical Data, and Defense Services Not Otherwise Enumerated

Achieving export control compliance can be burdensome and expensive due to its variable application across complex projects. There are two key cost areas to consider. The first is the total cost of compliance, including the employee costs and costs of managing the program, as well as costs to deploy and maintain supporting technical tools. The second is the cost of non-compliance, which can include fines, export prohibitions, suspension of operations, forfeiture of current or future government contracts, or incarceration in certain instances.

The employee costs and technical controls required for compliance are associated with the complexity of export control regulations. For instance, the following parameters must be considered to determine point-in-time compliancy for all export controlled files:

- Status on current USML and/or CCL
- File security status
- Storage device security status
- Transmission security status
- Destination device security status
- Citizenship status of user
- Government security status of user
- Corporate security status of user
- Geographic location of user
- File operations (Open, Delete, Save/Save As, Copy/Move)
- Extenuating IT conditions (online, offline, connection type, image state, specialized hardware, application compliance)


Due to the difficulty of managing so many changing variables organizations often limit their compensating control strategies to simply addressing obvious security holes, and trusting that business procedures are in place to ensure that only authorized users can access export controlled information. Furthermore, because of the impracticality and compliance cost using traditional security technology, companies often delay investing in more sophisticated security measures until an audit – or incident – exposes a specific deficiency, and even then they often limit the response to merely plugging the gap.

The need for an authoritative, persistent, and flexible solution that enables the productive and safe use of export controlled information is increasingly important. This is especially underscored as business expansion and the need to access sensitive data intertwine and cloud the distinction between collaborator and competitor in a globally-dispersed workspace.

## Addressing Export Control With Situational Awareness And Response

To establish a programmatic and effective response to meeting export control requirements, an organization must understand the interaction between export control related data, people, process, and technology. To start with, the organization must answer these basic usage and policy questions:

- Where is the data stored, and from where is it accessed?
- Who is authorized to use the data (employees, contractors and third parties)?
- How are data usage policies deployed and verified?
- In what ways can the data be used?
- Under what conditions can the data not be used?

It is evident that these questions involve the description and status of data, usage policies, and/or user verification. However, most security tools such as Data Loss Prevention (DLP), Digital Rights Management (DRM), Network Access Control (NAC), and various encryption products can only address discrete areas of operation where sensitive data most likely (but not necessarily) resides or is used. They fail to consider the context of events surrounding the use of controlled data and therefore cannot enforce policy logic based on the current level of risk.

The most effective technology to enforce export control policy requires data-level insight and control without reliance upon specific network infrastructure or workflow. Regardless of where data resides or is used, the ideal solution must provide exact and complete insight about the file's meta-information at all times, including its sensitivity, origin, destination, user, and attempted operation. The ideal security must also be capable of determining and executing an automated and risk-appropriate response using policy logic based on the context of the event.

This response (control) should include: the user's authority; the compliance state of the resources in use; and whether an overriding condition (for example, the user's geographic location) supersedes the user's normal access and usage rights.

Of the solutions used to demonstrate export control compliance, only those that monitor file usage in context and in real time can determine if an action is compliant or may lead to a violation. Furthermore, only solutions that accurately determine compliance can then apply the appropriate logic at the user and data levels, and be capable of interceding to prevent violations before they occur.

## Digital Guardian For Contextual Understanding & Policy Control

Digital Guardian is a data-centric security platform that is deployed to laptops, workstations, or servers and leverages a flexible back end infrastructure to deliver value that best aligns with your organization. Digital Guardian can be deployed either on premise, from within the Digital Guardian secure cloud, or as a hybrid solution where Digital Guardian security teams manage the deployment within your infrastructure. Digital Guardian Agents support Windows, OS X, and Linux operating systems, including virtual and cloud environments, and work in conjunction with virtually any distributed network or role-based administrative models.

### Digital Guardian Deployment Options

#### On-Premise

- Infrastructure hosted, managed, and maintained on site by customer

#### Hybrid

- Infrastructure hosted and maintained on site
- Digital Guardian manages security operations

#### Managed Security Program

- Infrastructure hosted and maintained by Digital Guardian

The Digital Guardian Agent operates simultaneously in user and kernel modes, and is aware of each authenticated user and login session. As a set of low-level drivers independent of the operating system, the Digital Guardian Agent can dynamically insert itself into any application or system operation to monitor and apply policy-based control before a command is allowed to execute. Digital Guardian "knows" at a forensic level the machine's and user's identity and policy and has visibility into file classification, disk inventory, network activity, application manifest, peripherals attached, IP subnet, connection type, and so on. All of these parameters can be used by themselves, or concurrently, to understand and apply export control policy.

Digital Guardian is designed to conform to any workflow process and remain a passive event monitor until a condition exists that requires a response control. A low-overhead Agent can be installed in stealth mode to further limit any interruptions to business process. Responses are automated and based on events, from taking no action (log only), to block, justify, or encrypt. Digital Guardian is also capable of alerting the user to a risk and instructing the user on appropriate use or alternative actions to enable self-remediation.

**DLP automation allows organizations to define what policy violations trigger:**

- **Log –** Create an event for future review.
- **Alert –** Send a notice to a defined group of responders.
- **Prompt –** Generate message to user to alert them of prohibited behavior and allow for optional continuation with justification.
- **Encrypt –** Enforce encryption on a document that contains sensitive information.
- **Block –** Deny the action to prevent sensitive data loss.

As an audit and compliance tool, Digital Guardian is unique. Designed to eliminate threats to data regardless of when, where, who, how, or why a risky event takes place, it provides continuous contextual insight and control of data throughout the entire data lifecycle, and provides alerts that are applied when data is leaving the control of the organization and entering a realm where data control and protection may no longer exist.

Digital Guardian produces tamper-resistant event logs that have been successfully used to prove chain of custody and intent in both civil and criminal proceedings in the U.S. and E.U. Activity by any user, regardless of their administrative privilege (including Digital Guardian administrators), is forensically logged by machine, device, user, file name/type, and operation whether the user is on or offline. Event logs are bundled, hashed, and encrypted on the local machine until they can be securely uploaded to the management server for alerting and reporting at a configurable frequency whenever any network or standard Internet connection is established.

This unique intersection of visibility, audit and control capabilities drives business flexibility while ensuring absolute accountability. With Digital Guardian, export control officers and policy administrators can easily determine the exact nature and type of compliance risk to sensitive files throughout their lifecycle, and use this knowledge to create and modify policies that apply appropriate security controls without having to predict every violation event beforehand. Digital Guardian allows the business to determine how and when export control-specific risks are defined, and can be used to track and prove the real-time and historical status of files with certainty.

## Digital Guardian For Export Control Compliance

Digital Guardian is used by organizations primarily for enterprise IP protection and regulatory compliance. Export control can be considered a set of specialized conditions spanning both categories. Digital Guardian integrates into existing authentication and provisioning models to provide accurate, auditable event records. It also controls data access and usage at the root system level, and thus enforces precise policies based on the user's authority, machine, application, file/email operation, and conditional risk to the data. When mapped to the complex workflows requiring export control compliance, Digital Guardian is unparalleled in its value.

## File Security Status

Digital Guardian can determine a file's sensitivity and permanently designate classification automatically by using any combination of content-based (keywords, regular expressions, patterns) or context-based (file type, source application, source network path, user status) parameters defined by policy. This classification tag can be assigned while the file is at rest, in motion, or at the moment of creation. Tags are a fundamental element (along with elements such as user status) for export control policy enforcement because they persist with files identified as export controlled and are inherited by derivative files that include any part of the original.


### Digital Guardian Export Control Customer Success Story

#### Industry

- Technology

#### Environment

- 12,000 workstations
- Linux
- Windows

#### Challenges

- Comply with ITAR regulations that prohibit foreign nationals accessing export controlled designs
- Integration with multiple source code control, CAD and simulation applications
- Allow, but control, Internet access for users
- Monitor activities of foreign nationals

#### Results

- Enterprise-wide discovery of export controlled information
- Over $4 million in annual savings from duplicate facility consolidation
- Improved productivity through enabling controlled access to designs from any location
- Achieved virtual network segmentation and a more streamlined physical infrastructure
- Identification, arrest, and prosecution of foreign national attempting to steal designs

## Origination And Destination Device Security Status

Digital Guardian Agents are authenticated and validated within the same managed deployment. The Agent and its operating state are tamper-resistant, regardless of a user's system privileges, so the organization can be reasonably assured the visibility and status delivered are accurate. As long as the policy deployed to the Agent renders the security state of the machine export control-compliant, then the machine will remain controlcompliant for all files, users, and sessions.

## Transmission Security Status

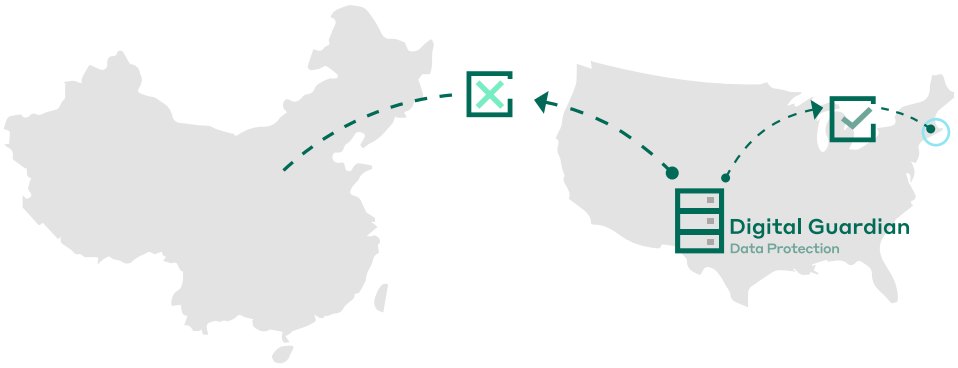
Digital Guardian has complete authority over all modes of egress from which a file can be transferred off the machine. Along with the conditional controls that can be applied to block or allow a user to transport a sensitive file, encryption can be automatically applied if a file is authorized to be emailed internally or externally, or moved to a removable storage device such as a USB stick. Moreover, because Digital Guardian is also application-aware, it can apply policy to require a user to enable additional security before file transmission, even if the application cannot natively enforce the same action.


## User Status: Citizenship, Government, And Organizational Clearance

Export control fundamentally prohibits users whose clearance is outside a certain status category from handling controlled information, regardless of their clearance within an organization or their home country. Organizations can associate personal attributes like citizenship and security status during login using identity management systems (such as Active Directory). Digital Guardian can sync with an identity management system and apply user attributes as a basis for policy management and provisioning. For instance, within a collaborative environment among citizens and non-citizens of equal security clearance, only citizens could access export controlled project files.

## Geographic Location Of User

Export controls stipulate that even if all other compliance conditions are met, controlled information cannot be accessed outside U.S. territories. Even if a machine does not have export controlled data stored locally, a user who is located outside the U.S. is nevertheless prohibited from accessing an export controlled resource originating within the U.S. This prohibition is especially problematic because a single condition (geography) suspends all other policies, even if the user is otherwise authorized to handle export controlled data. Digital Guardian can be used to help maintain compliance in this situation by using geographic-based parameters (such as host name on the internal network, or IP subnet in the cloud) to determine when an authorized user is accessing the network from outside the U.S. When combined with other perimeter control methods, Digital Guardian provides an effective layer of verification, particularly for reducing the risk of inadvertent access violations.




## File Operation

A file operation must be controlled if it directly leads to an export-control violation. This can include attaching a file to a personal webmail account; performing a copy/paste into an instant messaging application; or not automatically encrypting when export controlled data is moved to a removable device. Digital Guardian is capable of prohibiting any usage scenario that an organization deems inappropriate or risky, regardless of a user's status, while allowing the same operation for non-sensitive files. Digital Guardian uniquely provides fully integrated and automated file and removable media encryption as a control to further mitigate the risk of an export control violation.

## Extenuating Conditions

Because export control compliance is heavily determined by the current state of the IT environment, it can be explicitly invoked by the sudden change of a single parameter (such as location), or become implicitly more likely based on more subtle or unpredictable changes in the security state of the machine. For instance, a particular application may not be prohibited by export control, but the organization may use Digital Guardian to deny execution of an application outside an approved whitelist under any circumstance – or simply prohibit its use when the user is connected to a file share that contains export controlled data.

Another example would be the case where a critical operating systems security patch was issued, at which time a policy provided by Digital Guardian could be easily deployed to suspend authorized transmission of an exportcontrolled file from a machine until the patch has been applied.

## Conclusion

Export control compliance is one of the most difficult and expensive mandates that a company must address, particularly because the penalties for non-compliance can affect the company's revenue, brand, and more. However, most infrastructure-based security technologies cannot offer the insight, automation, or flexibility required to prevent violations. Export controls are fundamentally a set of rules that determine the authorized relationship between file, user privilege, action, and operational status. As such, export control compliance requires a complete and cost-effective solution that can forensically monitor and control every facet of multiple risk conditions simultaneously.

Digital Guardian is the only commercially available solution that can implement risk-aware policy for every export controlled data type, and control the use of data based on the compliant state of the user and their operating environment, independent of infrastructure. Digital Guardian can interface with centralized enterprise provisioning and authentication systems to automatically enforce individual export control usage rights on authorized systems based on verifiable attributes. Moreover, Digital Guardian is capable of invoking temporary controls when an operating condition exists (for example, an authorized user on a foreign network) that requires the suspension of normal usage rights until a compliant condition is restored.

Digital Guardian is designed to be extremely flexible and unobtrusive to existing workflows and procedures. Digital Guardian instantly creates value out of the box and without any configuration by providing continuous data-level visibility for real-time alerting and compliance auditing. Through each successive phase of implementation, Digital Guardian provides measurable and actionable results that demonstrate the organization's ability to comply with export control regulations.

The burden of export control can be mitigated over time by using the Digital Guardian platform to break down the essential elements that determine compliance, enforce policy around those elements, and then manage remaining risks by exception. Export control compliance is an iterative process that requires time, awareness, and analysis, but for a system like Digital Guardian - designed specifically to manage policy variance and exception at fundamental levels - it can be done more easily, more broadly, and for far less cost than a collection of disparate solutions. More than any single solution, Digital Guardian allows companies to better comply with this important law.

FORTRA™

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.