

# Trade Compliance Programs

*Frequently Asked Questions*

As of April 2019

**DELLEMC**  
PARTNER  
PROGRAM

# Disclaimer

Dell EMC is providing this FAQ document to emphasize your obligations to comply with all applicable Export Control and Sanctions laws. It is not intended as and cannot substitute for legal advice. You remain responsible for complying with these laws and implementing appropriate policies and procedures to ensure your compliance, including a trade compliance program. This guidance in no way modifies or negates any of your legal obligations under the Partner Code of Conduct or the respective Partner agreements with Dell EMC.



# What are my trade compliance obligations?

**The following is a summary and reminder of the obligations set forth in the Partner Code of Conduct.**

**The Partner Code of Conduct states that all Dell EMC products, software and services:**

- Are presumed subject to U.S. export control requirements, in addition to any other applicable countries' requirements
- Must not be provided to any sanctioned or restricted persons, countries, or uses unless authorized by the U.S. government

**Partners must:**

- Understand and comply with the U.S. export control laws and regulations applicable to the Dell EMC products, software and services including any special restrictions
- Obtain any required licenses or other government authorizations as needed to the use, transfer, import, export, or re-export of Dell EMC products, software, technology, or services.
- Not cooperate with any restrictive trade practice or boycott that is prohibited or penalized under U.S. or applicable local laws
- Understand and comply with applicable import and export control laws and regulations of other countries

# What are the U.S. export control and sanctions laws that I need to be concerned with as a Dell EMC Partner?

## Export Administration Regulations (EAR)

- Established and enforced by the U.S. Department of Commerce through the **Bureau of Industry and Security (BIS)**
- EAR regulates exports, reexports, and transfers of many commercial items
- Items subject to the EAR include goods, technology, and software, including those that are specifically listed on the Commerce Control List and items that are not specifically listed that are designated as “EAR99”
- Additional resources on the EAR can be found [here](#)

## OFAC Sanctions

- The economic sanctions laws are administered and enforced by the **Office of Foreign Assets Control (OFAC)** of the US Department of the Treasury
- An overview of the OFAC sanctions together with detailed explanations and FAQs can be found [here](#)



# What is prohibited under the U.S. Export laws?

## Prohibited Countries

- Dell EMC products and services **CANNOT** be sold directly or indirectly through a third party to prohibited countries or to a prohibited country's Embassy or Consulate (wherever located) without a US government license or other official authorization.
- The current list includes:



## Prohibited People and Entities

- Specially Designated Nationals and Blocked Persons (“SDN List”)
- Other individuals and entities on other U.S. government screening lists (such as the Entity List)
- Terrorists
- Drug Traffickers
- Proliferators of Weapons of Mass Destruction
- Criminal Organizations

## Prohibited End-Uses

- Nuclear Technology
- Missile Technology – includes space exploration activities and unmanned aerial vehicle (UAV or drone) activities
- Chemical or Biological Weapons
- Maritime Nuclear Propulsion
- Military End Uses
- Weapons of Mass Destruction
- Certain activities related to oil and gas exploration and production (Russian transaction related)

# What are the consequences if I violate these laws or the Dell EMC's Partner Code of Conduct?

- Dell EMC can enforce its contractual and legal rights including termination of our relationship with you
- U.S. civil penalties may exceed \$1 million USD per export or shipment and criminal penalties of \$1 million USD per export or shipment and up to 20 years imprisonment
- U.S. authorities can also ban companies that are suspected of violating these laws from access to U.S. goods and technology, U.S. banks, and U.S. financial markets, block travel to and from the United States, extradite suspected violators for trial, and list suspected violators on various denied parties lists.

# How can you effectively comply with these laws?

- BIS recommends that each exporter, reexporter or other party in a cross-border transaction establish a **Export Compliance Program (ECP)**
- An ECP helps to ensure that you comply with all applicable export control and sanctions laws, including the EAR and OFAC sanctions as well as applicable local laws
- A well-designed ECP can also help you to manage exports and comply with license conditions and can also help mitigate potential penalties in the event of an inadvertent violation
- **Your ECP should be appropriate to the scope of your business, including your export and re-export activities**

# What are the key elements of an ECP?

## 1. Have a Corporate Compliance Statement

- A compliance statement should be communicated to and acknowledged by all employees.
- This statement should include: (a) affirmations of your company's commitment to export compliance and appropriate resources to comply; (b) statements that you and your employees must be familiar and compliant with export controls; and (c) contact information for the persons at the company who are responsible for trade compliance.

## 2. Risk Assessment

- Identify the export risks that make your company vulnerable.
- Know your customer or end-user, the exported item and its use.

## 3. Screening of Parties and End Use

- Exports, reexports, and transfers to certain restricted parties or for certain end uses may be prohibited or require a license.
- All parties in an export transaction should be screened against a consolidated list of restricted parties.
- Screening may be done manually or by professional software.

## 4. Export License Determination

- License requirements may be product based, destination based, end user based, or end use based.
- It is your responsibility to know your customer and identify red flags related to the transaction.

## 5. Training

- All employees who are involved in export-related functions, as well as top management, contractors, consultants should understand export compliance responsibilities.
- You should provide your employees with sufficient training in order to ensure they possess a working knowledge of current export control regulations as well as the specific requirements of the organization's ECP.

## 6. Record Keeping

- In addition to local recordkeeping requirements, the U.S. Government requires that organizations keep export related documents for a minimum of 5 years from the date of any known export, reexport, or transfer.



# Where can I find guidance on ECPs?

- Guidance on establishing an effective [Export Compliance Program can be found here](#)
- This guidance is provided by BIS and is designed to help organizations comply with EAR and other U.S. export regulations
- You are also responsible for complying with local customs and export control laws. Consult your local legal counsel for advice on compliance with these laws

# Who is responsible for screening and identifying Red Flags?

- Dell EMC Partners are expected to screen their customers or end-user to identify any red flags or potentially restricted circumstances. This screening will be an important part of your ECP.
- A red flag is any circumstance in a transaction that indicates the sale or export may be destined for a restricted end-use, end-user, or to a restricted destination: **Place, Purpose, Product and People**
- The Consolidated Screening List (**CSL**) is a list of parties for which the U.S. Government maintains restrictions on certain exports, reexports or transfers of items. It includes the export screening lists of the Departments of Commerce, State and the Treasury and may be used as an aid to industry in conducting electronic screens of potential parties to regulated transactions. The tools are found [here](#).
- **Knowing your customer or end-user is essential!**
- BIS “Know Your Customer Guidance” is located [here](#).

# What are some of the Red Flags?

## People – Who is involved in the transaction?

- Any involvement with a person on a government denied party list, or a person in a prohibited country (e.g. Iran), or a prohibited country bank.
- Customer:
  - name contains wording of a prohibited country within the name (e.g., Syrian Airlines).
  - wants to use a government bank of a prohibited country (e.g. Bank of Saderat's Paris branch office).
  - is willing to pay cash for a very expensive item when the terms of sale would normally call for financing.
  - asks to omit or change information from invoices.
  - requests anonymity or is unwilling to provide documents to verify identity.
- Routine installation, training, or maintenance services are declined by the customer.

## Product – What product is being requested?

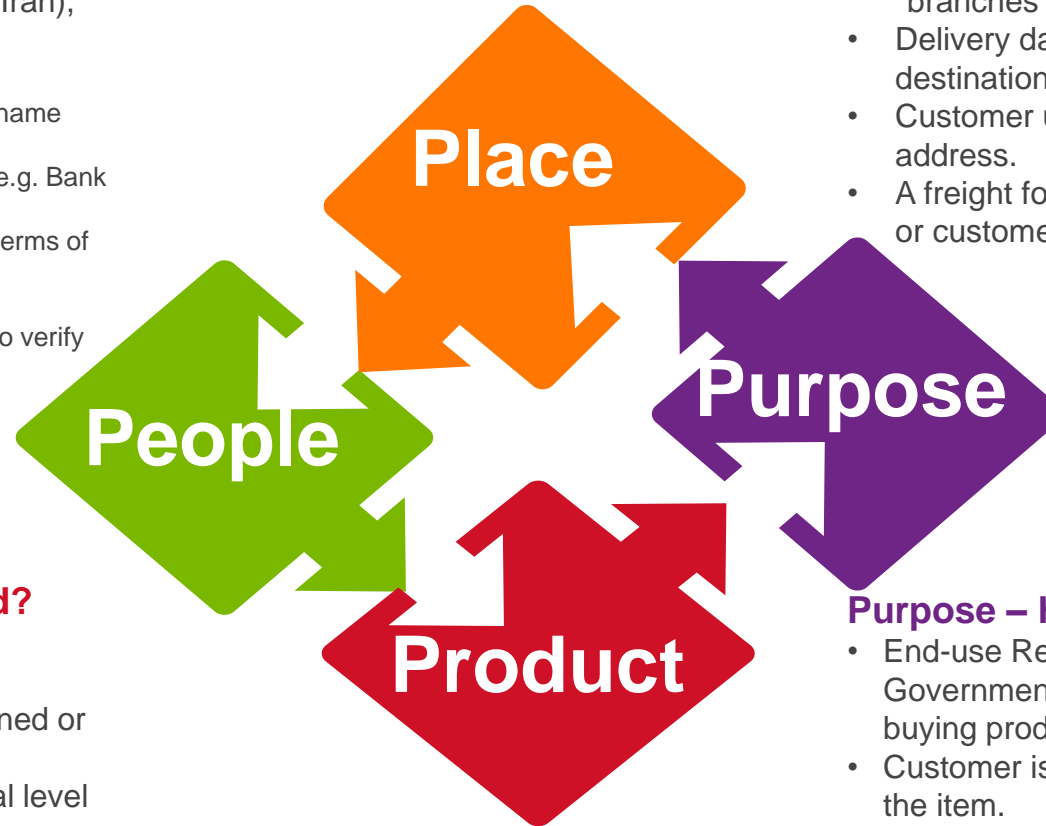
- Some of Dell's products require **export or import licenses**. They include products with advanced encryption capabilities or products specially designed or modified for aerospace/defense end-use.
- The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no semiconductor industry.

## Place – Where is products going?

- Companies headquartered in a prohibited country or branches located abroad in a non-prohibited country.
- Delivery dates are vague, shipping routes are circuitous, final destination is a traditional transshipment point.
- Customer uses a PO Box or UPS Store as their delivery address.
- A freight forwarder is listed as the product's final destination or customer has indicated they will use a freight forwarder.

## Purpose – How will our products be used?

- End-use Restrictions –An export license issued by U.S. Government may be required for sales to individuals or entities buying products or services for any of the prohibited end-uses.
- Customer is reluctant to offer information about the end-use of the item.
- Product's capabilities do not fit the buyer's line of business.
- Customer is a freight forwarder or general trading company located in a traditional transshipment point.



# Key Concepts and Takeaways

- Dell EMC complies with all applicable export control and sanctions laws and our Partners are contractually bound and expected to do the same.
  - Including compliance with the U.S. prohibitions on doing business in or with sanctioned countries (including Cuba, Iran, North Korea, Syria and the Crimea region) and with sanctioned individuals and entities.
  - It also includes end user, end use, and end destination controls under applicable Export Control laws.
- You are responsible for taking all appropriate steps to ensure your compliance with these laws.
  - An ECP is an essential compliance element.
- You are responsible for knowing your customer or end-user as well as taking appropriate steps to ensure that you do not do business with sanctioned individuals and entities.
  - This includes screening all parties to a transaction against the various sanctioned persons lists [found here](#)
- Failure to abide by your compliance obligations can lead to your termination as a Dell EMC Partner and other appropriate action, including civil and criminal penalties.

The Dell EMC logo is centered within a white rectangular border. It features the word "DELL" in a bold, sans-serif font, followed by a stylized icon consisting of three parallel diagonal lines, and then the letters "EMC" in a regular, sans-serif font.

DELL EMC

PARTNER  
PROGRAM



# Anti-bribery and Corruption (ABC) Compliance Programs

*Frequently Asked Questions*

As of April 2019

**DELLEMC**  
PARTNER  
PROGRAM



# Disclaimer

Dell EMC is providing this FAQ document to emphasize your obligations to comply with all applicable anti-bribery and corruption (“ABC”) laws. It is not intended as and cannot substitute for legal advice. You remain responsible for complying with these laws and implementing appropriate policies and procedures to ensure your compliance, including an ABC compliance program. This guidance in no way modifies or negates any of your legal obligations under the Partner Code of Conduct or the respective Partner agreements with Dell EMC.



# What are my ABC compliance obligations?

**The following is a summary and reminder of the obligations set forth in the Partner Code of Conduct.**

**The Partner Code of Conduct states that you:**

- Understand and comply with the Anti-Corruption Laws (U.S. Foreign Corrupt Practices Act, the UK Bribery Act, and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business and other local anti-corruption or anti-bribery laws)
- Will never offer, promise, request, authorize or accept a bribe, directly or indirectly, for any reason
- Agree to maintain reasonable procedures, internal policies, controls and methods designed to ensure compliance with Anti-Corruption Laws
- Adopt a third party due diligence process for vetting third parties you engage in the context of Dell EMC business.
- Not work with any individual or entity that engages in or is suspected of engaging in bribes, kickbacks, fraud or other improper activities

# What are the basic principles of the ABC laws?

- **US Foreign Corrupt Practices Act (1977) / UK Bribery Act 2010**
  - Purpose: to make it unlawful to make payments to foreign government officials to assist in obtaining business
  - Other laws: The U.S. Foreign Corrupt Practices Act (FCPA) and the U.K. Bribery Act are just two examples of government legislation. More than 40 countries have adopted the [OECD Anti-Bribery Convention](#), which establishes legally binding standards to criminalize bribery of foreign public officials in international business transactions. The specifics of regulations vary by region and applicable laws
- **The Basics**
  - Do not give anything of value to a government official with the intent to obtain business. Don't accept bribes or kickbacks. Do not falsify accounting (keep clean books and records). Do not do business with third parties that do either of these things. Note that the UK Bribery Act and other laws also prohibit bribes to non-governmental parties

|                              | U.S. Foreign Corrupt Practices Act                   | UK Bribery Act 2010  |
|------------------------------|--|--|
| <b>Bribery</b>               | Bribery of non-US government officials is prohibited | Bribery of private individuals, corporations and any government official are prohibited  |
| <b>Accepting a bribe</b>     | Not an offense                                       | It is an offense to receive or accept a bribe from anyone, public or private             |
| <b>Facilitation Payments</b> | Not prohibited, but discouraged by the US            | Prohibited   |
| <b>Statutory Defense</b>     | No specific defense articulated                      | One statutory defense – “adequate procedures” in place to prevent bribery from occurring |

# What are the consequences if I violate these laws or the Dell EMC's Partner Code of Conduct?

- Dell EMC can enforce its contractual and legal rights including termination of our relationship with you
- Enforcement actions are often cross border, and fines and penalties can be in the billions
- In 2018, 16 companies paid a record \$2.89 billion to resolve FCPA cases. That includes amounts assessed in resolutions with the DOJ or SEC or both, and through DOJ declinations with disgorgement
  - There were three enforcement actions in the mega-case category -- Petrobras (\$1.78 billion), SocGen (\$585 million), and Panasonic (\$280 million). Petrobras and SocGen followed the new structure for global resolutions, with the DOJ and SEC assessing total penalties but allowing the companies to pay some of the penalties to enforcement agencies and regulators in other countries
- In 2017, 11 companies paid just over \$1.92 billion to resolve FCPA cases.

# What are the basic elements of an ABC compliance program?

The elements of an effective compliance program are:

|   |  |
|---|--|
| <b><i>Tone at the Top</i></b>                           | A commitment from senior management and a clearly articulated policy against corruption.   |
| <b><i>Code of Conduct &amp; Compliance Policies</i></b> | Policies and procedures detailing proper internal controls, auditing practices, documentation policies and disciplinary measures should be in place.                     |
| <b><i>Oversight, Autonomy and Resources</i></b>         | Individuals in charge of oversight should have autonomy from management and should have sufficient resources to ensure the program is implemented correctly.             |
| <b><i>Risk Assessment</i></b>                           | Companies should regularly analyze and address the specific risks they face.   |
| <b><i>Training</i></b>                                  | Companies should take the appropriate steps to ensure that the policies and procedures have been communicated effectively throughout the organization.                   |
| <b><i>Incentives and Disciplinary Measures</i></b>      | Clear disciplinary procedures should be in place and the adherence to compliance policies and procedures should be incentivized throughout the company.                  |
| <b><i>Third-Party Due Diligence &amp; Payments</i></b>  | Third-parties should be assessed regularly and should be informed of the company's compliance program and code of conduct.   |
| <b><i>Reporting</i></b>                                 | Employees must be able to report violations without fear of retaliation. The compliance program and internal controls should be updated after an internal investigation. |
| <b><i>Testing and Review</i></b>                        | Compliance program should be reviewed and tested for effectiveness.  |

# Where can I find guidance on effective ABC compliance programs?

- A robust program depends very much on whether a company has tailored its policies and processes to address its specific risks
- In its [2012 Resource Guide to the U.S. Foreign Corrupt Practices Act \(the “FCPA Guide”\)](#), the DOJ specifically advised: “Effective compliance programs are tailored to the company’s specific business and to the risks associated with that business. They are dynamic and evolve as the business and the markets change”
- The DOJ emphasizes that when it comes to compliance, there is no one-size-fits-all program. Individual companies may have different needs depending on their size and the particular risks associated with their businesses
- Dell EMC’s policy is available upon request as a example. Your policy and ABC program should be tailored to the risk profile of your company.



# What are the basic requirements to comply with ABC laws and the Code?

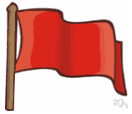
- ✓ DO NOT make any payment or offer any payment intended to induce the recipient to misuse his official position
- ✓ DO NOT accept bribes or kickbacks
- ✓ DO know who and which business entities trigger ABC awareness—foreign officials, close relatives of foreign officials, companies owned in part by the government or by foreign officials
- ✓ DO maintain a list of all of your clients, customers, and sales, marketing or other business contacts who are foreign officials
- ✓ DO cross-check business partners' conduct against the red flags list
- ✓ DO clearly identify all expenses by jurisdiction and type
- ✓ DO report conduct you have good reason to believe violates the Code or any laws prohibiting bribe payments
- ✓ Do have an ABC policy and standards to help prevent wrongdoing.
- ✓ Do have reporting mechanisms for possible wrongdoing
- ✓ Do assess the company's risks and train employees regularly to ensure that the compliance requirements are understood and followed

# What are some examples of red flags?

- ❖ The transaction is in a high-risk country or industry
- ❖ Government official or close ties to government official
- ❖ Unqualified or unidentified third parties
- ❖ Excessive margins or unreasonable charges or cash payments
- ❖ Lack of transparency or documentation in expenses or accounting records
- ❖ Unnecessary middleman or broker
- ❖ Unusual payment patterns or financial arrangements
- ❖ Involvement of a shell or holding company
- ❖ Third party has a poor reputation or has been accused of improper business practices
- ❖ Third party's value is based primarily on connections or access to information
- ❖ Payment to an entity that is owned or influence by a government official
- ❖ Gifts or other payments to or from parties engaged in a competitive bidding process or contract negotiations

# What are examples of prohibited behavior/red flags?

- Your public customer request a trip to visit the manufacturing facility before committing to purchase. The customer in Europe requests this trip to the plant in the U.S. and desires luxury accommodations for him and his family
- Customer requests that you use an agent as an intermediary to help facilitate getting through the “red tape.” Agent’s fees are excessive and the services provided are vague
- You are negotiating with a government minister, and she asked that your company contribute her favorite charity. The amount of the donation is small in comparison to the business and the cause is a good one



In each situation, there is something of value being given to potentially influence a decision maker.

# Do you know your customers?



With whom are we dealing? Do you know the customer and any reps or agents involved?



Who is receiving the payment?



Are the company's processes being followed in the deal?



Can you confidently explain the deal and why the parties are in it?



The Dell EMC logo is centered within a white rectangular border. It features the word "DELL" in a bold, sans-serif font, followed by a stylized icon consisting of three parallel diagonal lines, and then the letters "EMC" in a regular, sans-serif font.

DELL EMC

PARTNER  
PROGRAM