Updated Minimum Security Criteria - New Focus Areas
Supply Chain Security Mission Statement

Establish a multi-layered security approach to effectively deter, detect, delay, and deny any infiltration of Academy’s Supply Chain.
Objectives

- New Focus Areas
- Best Practices Formula
- Security Vision & Responsibility
- Business Partner Screening – Trade Based Money Laundering
- Cyber Security
- Agriculture (AG) Security
- Contact
New Focus Areas

- **Security Vision and Responsibility** – Promotes a culture of security and a commitment to supply chain security.

- **Trade Based Money Laundering** – Prevention of trade based money laundering and terrorist financing; and

- **Cybersecurity** – To help ensure the security of critical IT systems and the trade data that moves across cyberspace;

- **Agricultural Security** – To protect the supply chain from agricultural contaminants and pests;
Best Practices

Senior Management Support
- Inspires innovation and continuous improvement, and provides adequate resources

Evidence of Implementation
- Verifies security via SCSS observation and documentation

Innovative Business, Process, & Technology
- Increases automation, adaptability, and efficiency

Documented Process
- Ensures consistency and continuity via written policies

Systems of Checks, Balances, and Accountability
- Supports reliability via recurring tests and internal/external audits

Best Practices Framework
Corporate Security

Security Vision & Responsibility
Security Vision & Responsibility – Best Practice

• Business Partners should demonstrate their commitment to supply chain security through a statement of support. This statement should be signed by at least one senior company official and displayed in appropriate company locations.

• The statement of support should highlight the importance of protecting the supply chain from criminal activities such as drug trafficking, terrorism, human smuggling, and illegal contraband.

• Senior company officials who should sign and support the statement may include the President, CEO, General Manager, or Security Director.

• Areas to display the statement of support include the company’s website, on posters in key areas of the company (reception; packaging; warehouse; etc.), and/or be part of the company’s security seminars, etc.
Corporate Security

Trade Based Money Laundering
The Financial Action Task Force (“FATF”) defines Trade Based Money Laundering (“TBML”) as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins.”
• **Overvaluation Scheme:** Reporting goods as more than what they are actually worth (over – invoicing). Allows the importer to move illicit proceeds out the country under false representations made in the invoice (compare invoice, Bill of Laden or “BOL” to known Fair Market Value or “FMV”).

• **Over Shipment:** Exporter ships less goods than what is actually declared on invoice, BOL, etc. Effectively allowing the importer to move value (illicit proceeds) back to the exporter.

• **False Invoicing:** i.e. Reporting different commodities that what is actually shipped or ghost shipments.

• **Undervaluation Scheme:** Reporting goods as less than what they are actually worth (under – invoicing). Allows the exporter to move illicit proceeds (in the form of goods) out of the country under the false representations made in the invoice (compare invoice, BOL to known FMV).

• **Under Shipment:** Exporter ships more goods than what is actually declared on invoice, BOL, etc. Effectively moving value to the importer in the form of additional goods.
Trade Based Money Laundering (TBML) Schemes Continued

Exporter billed $2 million, actually exported $1 million in goods.

Importer paid $1 million, actually received $2 million in goods.
What Risks Do Your Business Partners Pose?

Levels of Risk

The International Association of Certified Anti – Money Laundering Specialists (“ACAMS”) define four levels of risks.

- **Prohibited**: The business will not tolerate any dealings of any kind given the risk. Countries subject to economic sanctions or designated as state sponsors of terrorism, such as Sudan or Iran, are prime candidates for prohibited transactions. Prohibited customers would include shell banks.

- **High Risk**: The risks here are significant, but are not necessarily prohibited. To mitigate the heightened risk presented, the firm should apply more stringent controls to reduce the risk, such as conducting enhanced due diligence and more rigorous transaction monitoring. Countries that are noted for corruption or drug trafficking are generally deemed high risk.

- **Medium Risk**: Medium risks are more than a low or standard risk of money laundering, and merit additional scrutiny, but do not rise to the level of high risk.

- **Low or Standard Risk**: This represents the baseline risk of money laundering; normal business rules apply. “FATF” member countries and domestic retail customers are frequently, but not always, considered to be standard or low risk.
Know Your Customers (“KYC”): On-boarding New Customers

- **KYC:** Conduct thorough due diligence on the front end and periodically verify that established customer profile is in line with expectations: Some examples include:
  - Identification and verification of the identity of customers, counterparties, and their beneficial owners, obtaining information on the purposes and intended nature of the business relationships, and conducting ongoing due diligence.
  - Historical and expected volume of trade
  - Typical valuation of commodities
  - Understanding the type of commodities traded
  - Knowing if the customers sales are cyclical or not; if so, what months are sales concentrated in
  - Knowing the customers primary market(s)
  - Understanding the revenue collection/accounts receivable operating cycle
  - Understanding the accounts (A/P) operating cycle; how does your customer typically pay their A/P (i.e. wire transfer, ACH, cashier's check, business checks, money orders)?
Corporate Security

Cybersecurity
Cybersecurity

- Economic vitality and the security of business partner transactions depends on cyberspace -- interdependent and critical networks, systems, services and resources.

- Cyberspace has transformed economic and governmental services and is at risk of cyber attack.

- Cyber intrusions and attacks have increased dramatically over the last decade. They can be categorized as a computer network attack (CNA) or computer network exploitation (CNE)
• **Cybersecurity** — Cybersecurity is the activity or process that focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change or destruction. It is the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits taken.

• **Information Technology (IT)** — Computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure, and exchange all forms of electronic data.
Business Partner Requirement

• Business partners must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all of the individual Cybersecurity criteria.

• Partners are encouraged to follow cybersecurity protocols that are based on recognized industry frameworks/standards. e.g. The National Institute of Standards and Technology (NIST) [https://www.nist.gov/](https://www.nist.gov/) cyber framework.
• A company must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in Partners' computer systems.

• Partners must ensure that their security software is current and receives regular security updates. Partners must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or other unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.
• Business partners utilizing network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.

• A vulnerability scan (VS) identifies openings on your computers (open ports and IP addresses), their operating systems, and software through which a hacker could gain access to the company’s IT system.

• The frequency of the testing will depend on various factors to include the company’s business model and level of risk.
Business Partner Requirements

• A system must be in place to identify unauthorized access of IT systems/data or abuse of policies and procedures including improper access of internal systems or external websites and tampering or altering of business data by employees or contractors. All violators must be subject to appropriate disciplinary actions.

• Cybersecurity policies and procedures must be reviewed annually, or more frequently, as risk or circumstances dictate. Following the review, policies and procedures must be updated if necessary.

• User access must be restricted based on job description or assigned duties. Authorized access must be reviewed on a regular basis to ensure access to sensitive systems is based on job requirements. Computer and network access must be removed upon employee separation.
Business Partner Requirements

• Individuals with access to Information Technology (IT) systems must use individually assigned accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication and user access to IT systems must be safeguarded.

• User access must be safeguarded by going through an authentication process. Two-factor authentication (2FA) or multi-factor authentication (MFA) are preferred.

• The use of long, easy to remember passphrases instead of words with special characters is recommended.
Business Partner Requirements

• Partners that allow their users to remotely connect to a network must employ secure technologies, such as virtual private networks (VPNs), to allow employees to access the company’s intranet securely when located outside of the office. Members must also have procedures designed to prevent remote access from unauthorized users.

• If business partners allow employees to use personal devices to conduct company work, all such devices must adhere to the company’s cybersecurity policies and procedures to include regular security updates and a method to securely access the company's network.
Business Partner Requirements

- All media, hardware, or other IT equipment that contains sensitive information regarding the import/export process must be accounted for through regular inventories. When disposed, they must be properly sanitized and/or destroyed in accordance with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization, the partner’s governing authority or other appropriate industry guidelines.
Cybersecurity policies should address how business partners share information on cybersecurity threats with the Government and other business partners.
Best Practices

• Cybersecurity policies and procedures should include measures to prevent the use of counterfeit or improperly licensed technological products.

• Business partners may want to have a policy that requires Product Key Labels and Certificates of Authenticity to be kept when new media is purchased.

• Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.

• Daily backups may be needed because of the effect that data loss may have on multiple personnel. Media used to store backups should preferably be stored at a facility offsite.
Cyber Security Cycle

1. IDENTIFY
   - Identify and control who has access to your business information
   - Conduct background checks
   - Require individual user accounts for each employee
   - Create policies and procedures for cybersecurity

2. PROTECT
   - Limit employee access to data and information
   - Install Surge Protectors and Uninterruptible Power Supplies (UPS)
   - Patch your operating systems and applications routinely
   - Install and activate software and hardware firewalls on all your business networks
   - Secure your wireless access point and networks
   - Set up web and email filters
   - Use encryption for sensitive business information
   - Dispose of old computers and media safely
   - Train your employees

3. DETECT
   - Install and update anti-virus, anti-spyware, and other anti-malware programs
   - Maintain and monitor logs

4. RESPOND
   - Develop a plan for disasters and information security incidents

5. RECOVER
   - Make full backups of important business data and information
   - Continue to schedule incremental backups
   - Consider cyber insurance
   - Make improvements to processes/procedures/technologies
Transportation Security

Agriculture Security
US CBP defines Agriculture (AG) Security as: Agriculture is an Industry and Employment sector in the U.S. and other countries that must be protected from infiltration of invasive and destructive contaminates (plant/animal) that may cause disease. These contaminates can be transferred via international trade vehicles, containers, cargo, etc..

- Contamination Elements:
  - Bugs
  - Eggs
  - Soil (what is inside the soil)
  - Plants
  - Snails (Parasites)
Agriculture Security

- Contamination Pathways of Entry (ways of arrival):
  - Sea
  - Air
  - Rail
  - Land

- Indicators of Pest Activity or Contamination (what to look for):
  - Insects or Insect eggs
  - Pest nests (birds, bees, etc.)
  - Snails or Slugs
  - Any type of soil (contaminates can be within soil)
  - Plant debris and/or Seeds
Contamination Effects

• 2001 Outbreak of Foot-and-Mouth-Disease in the UK requiring slaughter of livestock and banning of export.

• Citrus leaf that contained psyllid bacteria resulting in tree loss devastation.

• Temperate Terrestrial Gastropods (slugs/snails infestations)

• Asian Gypsy Moths – creates vegetation devastation

• Noxious Weed Seeds – Invasive species causing crop loss
Contamination Examples
Implementation Guidance – AG Security Criteria

1. Written procedures to prevent pest contamination
   - Company description of AG Security
   - How company monitors AG Security
   - How company prevents contamination

2. Wood Types Requiring Treatment:
   - Pallets
   - Wood packaging material (wpm)
   - Wood manufactured within the product itself

3. Verify wood is treated
   - ISPM 15 Compliance Regulation =
   - Wood treated for 8 pests
   - Stamped with
   - Accredited company used
   - Verify wood received from other Partners
4. Create internal checklist to self verify:

- Visually check exterior and interior of container prior to loading
- Sweep, vacuum, or wash out container prior to loading
- Check that cargo is clean and free of contaminants
- Check that cargo staging area free from plants and pests?
- Monitor/check lighting in staging area that might increase insect infestation

Wood Marking Example
Risk & Mitigation

- Vulnerable areas for contamination exposure:
  - Heavy rains, that may increase soil contamination transfer
  - Containers stored in areas near livestock pens or pastures
  - Containers/trucks driven through routes of wastewater or manure or farmland roads
  - Unclean cargo staging area – open to pests, insects, vegetation, etc..

- What to do if contamination exposed to elements/pests found:
  - Fumigate and ventilate
  - Treat wood (insects cannot infest properly treated wood)
  - Clean containers – sweep, wash, vacuum, etc..
If you have questions, please contact us at the following email address:

CTPAT@ACADEMY.COM