



~~1~~ ~~2~~ ~~3~~ ~~4~~ ~~5~~ ~~6~~ ~~7~~ ~~8~~ ~~9~~ ~~10~~ ~~11~~ ~~12~~ ~~13~~ ~~14~~ ~~15~~ ~~16~~ ~~17~~ ~~18~~ ~~19~~ ~~20~~ ~~21~~ ~~22~~ ~~23~~ ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ ~~29~~ ~~30~~ ~~31~~ ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ ~~37~~ ~~38~~ ~~39~~ ~~40~~ ~~41~~ ~~42~~ ~~43~~ ~~44~~ ~~45~~ ~~46~~ ~~47~~ ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ ~~53~~ ~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ ~~59~~ ~~60~~ ~~61~~ ~~62~~ ~~63~~ ~~64~~ ~~65~~ ~~66~~ ~~67~~ ~~68~~ ~~69~~ ~~70~~ ~~71~~ ~~72~~ ~~73~~ ~~74~~ ~~75~~ ~~76~~ ~~77~~ ~~78~~ ~~79~~ ~~80~~ ~~81~~ ~~82~~ ~~83~~ ~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ ~~89~~ ~~90~~ ~~91~~ ~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ ~~97~~ ~~98~~ ~~99~~ ~~100~~

N : Criteria ID numbers may not be sequential. ID numbers not listed are not applicable to Consolidators.

5 6 7

- 1** ~~1~~ ~~2~~ ~~3~~ ~~4~~ ~~5~~ ~~6~~ ~~7~~ ~~8~~ ~~9~~ ~~10~~ ~~11~~ ~~12~~ ~~13~~ ~~14~~ ~~15~~ ~~16~~ ~~17~~ ~~18~~ ~~19~~ ~~20~~ ~~21~~ ~~22~~ ~~23~~ ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ ~~29~~ ~~30~~ ~~31~~ ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ ~~37~~ ~~38~~ ~~39~~ ~~40~~ ~~41~~ ~~42~~ ~~43~~ ~~44~~ ~~45~~ ~~46~~ ~~47~~ ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ ~~53~~ ~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ ~~59~~ ~~60~~ ~~61~~ ~~62~~ ~~63~~ ~~64~~ ~~65~~ ~~66~~ ~~67~~ ~~68~~ ~~69~~ ~~70~~ ~~71~~ ~~72~~ ~~73~~ ~~74~~ ~~75~~ ~~76~~ ~~77~~ ~~78~~ ~~79~~ ~~80~~ ~~81~~ ~~82~~ ~~83~~ ~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ ~~89~~ ~~90~~ ~~91~~ ~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ ~~97~~ ~~98~~ ~~99~~ ~~100~~ – For a CTPAT Member’s supply chain security program to become and remain effective, it must have the support of a company’s upper management. Instilling security as an integral part of a company’s culture and ensuring that it is a companywide priority is in large part the responsibility of the company’s leadership.

D	5	6	7/8
1.1	In promoting a culture of security, CTPAT Members should demonstrate their commitment to supply chain security and the CTPAT Program through a statement of support. The statement should be signed by a senior company official and displayed in appropriate company locations.	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 support and sign 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;0.1.1 9qwa(e)9 10.0 8;0.1.1 9qwa(e) .5	
	To build a robust Supply Chain Security Program, a company should incorporate representatives from all of the relevant departments into a cross-functional team. These new security measures should be included in existing company procedures, which creates a more sustainable structure and emphasizes that supply chain security is everyone's responsibility.	Supply Chain Security has a much broader scope than traditional security programs. It is intertwined with Security, in many departments such as Human Resources, Information Technology, and Import/Export offices. Supply Chain Security programs built on a more traditional, security department-based model may be less viable over the long run because the responsibility to carry out the security measures are concentrated among fewer employees, and, as a result, may be susceptible to the loss of key personnel.	Should

D	6	6	W/6
---	---	---	-----

1.3 The supply chain security program must be designed with, supported by, and implemented by an appropriate written review component. The purpose of this review component is to document that a system is in place whereby personnel are

2 ~~Rn~~ _____ – The continuing threat of terrorist groups and criminal organizations targeting supply chains underscores the need for Members to assess existing and potential exposure to these evolving threats. CTPAT recognizes that when a company has multiple supply chains with numerous business partners, it faces greater complexity in securing those supply chains. When a company has numerous supply chains, it should focus on geographical areas/supply chains that have higher risk.

When determining risk within their supply chains, Members must consider various factors such as the business model, geographic location of suppliers, and other aspects that may be unique to a specific supply chain.

~~RD~~ ~~R~~ -

D	B	B	M/B
2.3	Risk assessments must be reviewed annually, or more frequently as risk factors dictate.	Circumstances that may require a risk assessment to be reviewed more frequently than once a year include an increased threat level from a specific country, periods of heightened alert, following a security breach or incident, changes in business partners, and/or changes in corporate structure/ownership such as mergers and acquisitions etc.	Must
2.4	CTPAT Members should have written procedures in place that address crisis management, business continuity, security recovery plans, and business resumption.	A crisis may include the disruption of the movement of trade data due to a cyberattack, a fire, or a carrier driver being hijacked by armed individuals. Based on risk and where the Member operates or sources from, contingency plans may include additional security notifications or support; and how to recover what was destroyed or stolen to return to normal operating conditions.	Should

3 B _____ – CTPAT Members engage with a variety of business partners, both domestically and internationally. For those business partners who directly handle cargo and/or import/export documentation, it is crucial for the Member to ensure that these business partners have appropriate security measures in place to secure the goods throughout the international supply chain. When business partners subcontract certain functions, an additional layer of complexity is added to the equation, which must be considered when conducting a risk analysis of a supply chain.

B _____ A business partner is any individual or company whose actions may affect the chain of custody security of goods being imported to or exported from the United States via a CTPAT Member’s supply chain. A business partner may be any party that provides a serv

D	B	
---	---	--

CTPAT Minimum Security Criteria –

D	B	B	M/B
3.7	<p>To ensure their business partners continue to comply with CTPAT's security criteria, Members should update their security assessments of their business partners on a regular basis, or as circumstances/risks dictate.</p>	<p>Periodically reviewing business partners' security assessments is important to ensure that a strong security program is still in place and operating properly. If a member never required updates to its assessment of a business partner's security program, the Member would not know that a once viable program was no longer effective, thus putting the member's supply chain at risk.</p> <p>Deciding on how often to review a partner's security assessment is based on the Member's risk assessment process. Higher risk supply chains would be expected to have more frequent reviews than low risk ones. If a Member is evaluating its business partner's security by in person visits, it may want to consider leveraging other types of required visits. For example, cross-train personnel that test for quality control to also conduct security verifications.</p> <p>Circumstances that may require the self-assessment to be updated more frequently include an increased threat level from a source country, changes in source location, new critical business partners (those that actually handle the cargo, provide security to a facility, etc.).</p>	Should

D	B	B	M/B
4.2	To defend Information Technology (IT) systems against common cybersecurity threats, a company must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in Members' computer systems. Members must ensure that their security software is current and receives regular security updates. Members must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or another unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.		Must
4.3	CTPAT Members using 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 secure computer network is of paramount importance to a business, and ensuring that it is protected requires testing on a regular basis. This can be done by scheduling vulnerability scans. Just like a security guard checks for open doors and windows at a business, 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)10.4 (s)10.5 (d)-3 (s)10.4 (s)10.5 (t)2C5166.1 (a)2.1 (i)5 3 0 Td(u(c)c)6.	

D	B	B	B 1 B
4.4	Cybersecurity policies should address how a Member shares information on cybersecurity threats with the government and other business partners.	Members are encouraged to share information on cybersecurity threats with the government and business partners within their supply chain. Information sharing is a key part of the Department of Homeland Security's mission to create shared situational awareness of malicious cyber activity. CTPAT Members may want to join the National Cybersecurity and Communications Integration Center (NCCIC - https://www.us-cert.gov/nccic). The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost.	Should
4.5	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.		Must
4.6	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.	An example of a circumstance that would dictate a policy update sooner than annually is a cyber attack. Using the lessons learned from the attack would help strengthen a Member's cybersecurity policy.	Must
4.7	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.		Must

D	B	B	M/B
4.10	If Members 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.	Personal devices include storage media like CDs, DVDs, and USB flash drives. Care must be taken if employees are allowed to connect their personal media to individual systems since these data storage devices may be infected with malware that could propagate using the company's network.	Must
4.11	Cybersecurity policies and procedures should include measures to prevent the use of counterfeit or improperly licensed technological products.	Computer software is intellectual property (IP) owned by the entity that created it. Without the express permission of the manufacturer or publisher, it is illegal to install software, no matter how it is acquired. That permission almost always takes the form of a license from the publisher, which accompanies authorized copies of software. Unlicensed software is more likely to fail as a result of an inability to update. It is more prone to contain malware, rendering computers and their information useless. Expect no warranties or support for unlicensed software, leaving your	

D	S	M	W/S
4.12	Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.	<p>Data backups should take place as data loss may affect individuals within an organization differently. Daily backups are also recommended in case production or shared servers are compromised/lose data. Individual systems may require less frequent backups, depending on what type of information is involved.</p> <p>Media used to store backups should preferably be stored at a facility offsite. Devices used for backing up data should not be on the same network as the one used for production work. Backing up data to a cloud is acceptable as an "offsite" facility.</p>	Should
4.13	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		



D	B	B	M/B
		<p>added to the security inspection process.</p> <p>Pest contamination is defined as visible forms of animals, insects or other invertebrates (alive or dead, in any lifecycle stage, including egg casings or rafts), or any organic material of animal origin (including blood, bones, hair, flesh, secretions, excretions); viable or non-viable plants or plant products (including fruit, seeds, leaves, twigs, roots, bark); or other organic material, including fungi; or soil, or water; where such products are not the manifested cargo within instruments of international traffic (i.e. containers, unit load devices, etc.).</p>	
5.3	<p>CTPAT Members must ensure that the following systematic CTPAT security and agricultural inspections are conducted. Requirements for these inspections will vary depending upon if the supply chain is land-based (Canada or Mexico) or if the supply chain originates overseas (ocean and air modes). Prior to stuffing/packing, all empty Instruments of International Traffic (IIT) must be inspected, and conveyances must also be inspected when they are crossing land borders into the United States.</p> <p><u>Inspection requirements for CTPAT shipments via ocean, air, and land borders (as applicable) by rail or intermodal freight:</u></p> <p>A seven-point inspection must be conducted on all empty containers and unit load devices (ULDs); and an eight-point inspection must be conducted on all empty refrigerated containers and ULDs:</p> <ol style="list-style-type: none"> 1. Front wall; 2. Left side; 3. Right side; 4. Floor; 5. Ceiling/Roof; 6. Inside/outside doors, including the reliability of the 	<p>Security and agricultural inspections are conducted on instruments of international traffic (IIT) and conveyances to ensure their structures have not been modified to conceal contraband or have been contaminated with visible agricultural pests.</p> <p>Expectations for overseas supply chains are to inspect all instruments of IIT at the point of stuffing/packing. However, if an ocean/air based supply chain is higher risk, it may warrant including more extensive inspection procedures to include conveyances and/or inspections at marine port terminals or air logistics facilities. Usually, there are higher levels of risk involved in shipments with land border crossings, which is why both the conveyance and IIT undergo multiple inspections.</p>	

D	B	B	M/ B
---	---	---	------

- locking mechanisms of the doors;
- 7. Outside/Undercarriage; and
- 8. Fan housing on refrigerated containers.

Additional inspection requirements for land border crossings via highway carriers:

Inspections of conveyances and IIT must be conducted at conveyance/IIT storage yards.

Where feasible, inspections must be conducted upon entering and departing the storage yards and at the point of loading/stuffing. These systematic inspections must include 17-point inspections:

- B** _____
1. Bumper/tires/rims;
 2. Doors, tool compartments and locking mechanisms;
 3. Battery box;
 4. Air breather;
 5. Fuel tanks;
 6. Interior cab compartments/sleeper; and
 7. Faring/roof.

D	B	NS	M/ B
---	---	----	------

5.4


CTPAT Minimum Security Criteria –

6 ~~B~~_____ The sealing of trailers and containers to attain continuous seal integrity, continues to be a crucial element of a secure supply chain. Seal security includes having a comprehensive written seal policy that addresses all aspects of seal security, such as using the correct seals per CTPAT requirements; properly placing a seal on IIT, and verifying that the seal has been affixed properly.

D	B	B	W/ B
---	---	---	---------

6.1 CTPAT Members must have detailed, written high-security seal procedures that describe how seals are issued and controlled at the facility and during transit. Procedures

D	B	B	M B
---	---	---	--------


-  :
 - When picking up sealed IIT (or after stopping) verify the seal is intact with no signs of tampering.
 - Confirm the seal number matches what is noted on the shipping documents.
 Seals Broken in Transit:
 - If a load is examined,

CTPAT Minimum Security Criteria –

D	B	B	M/B
7.8	<p>The shipper or its agent must ensure that bill of ladings (BOLs) and/or manifests accurately reflect the information provided to the carrier, and carriers must exercise due diligence to ensure these documents are accurate. BOLs and manifests must be filed with U.S. Customs and Border Protection (CBP) in a timely manner. BOL information filed with CBP must show the first foreign location/facility where the carrier takes possession of the cargo destined for the United States. The weight and piece count must be accurate.</p>	<p>When picking up sealed Instruments of International Traffic, carriers may rely on the information provided in the shipper's shipping instructions.</p> <p>Requiring the seal number to be electronically printed on the bill of lading (BOL) or other export documents helps guard against changing the seal and altering the pertinent document(s) to match the new seal number.</p> <p>However, for certain supply chains, goods may be examined in transit, by a foreign Customs authority, or by CBP. Once the seal is broken by the government, there needs to be a process to record the new seal number applied to the IIT after examination. In some cases, this may be handwritten.</p>	Must

D	B	B	B 1
7.23	<p>CTPAT Members must have written procedures for reporting an incident, which includes a description of the facility's internal escalation process.</p> <p>A notification protocol must be in place to report any suspicious activities or security incidents (such as drug seizures, discovery of stowaways, etc.) that take place anywhere around the world and which affects the security of the member's supply chain. As applicable, the Member must report any global incidents to its Supply Chain Security Specialist, the closest port of entry, any pertinent law enforcement agencies, and business partners that may be part of the affected supply chain. Notifications to CBP must be made as soon as feasibly possible and in advance of any conveyance or IIT crossing the border.</p> <p>Notification procedures must include the accurate contact information that lists the name(s) and phone number(s) of personnel requiring notification, as well as for law enforcement agencies. Procedures must be periodically reviewed to ensure contact information is accurate.</p>	<p>Examples of incidents warranting notification to U.S. Customs and Border Protection include (but are not limited to) the following:</p> <ul style="list-style-type: none"> • Discovery of tampering with a container/IIT or high-security seal; • Discovery of a hidden compartment in a conveyance or IIT; • An unaccounted new seal has been applied to an IIT; • Smuggling of contraband, including people; stowaways; • Unauthorized entry into conveyances, locomotives, vessels, or 	



8  _____ – Agriculture is the largest industry and employment sector in the U.S. It is also an industry threatened by the introduction of foreign animal and plant contaminants such as soil, manure, seeds, and plant and animal material which may harbor invasive and destructive pests and diseases. Eliminating contaminants in all conveyances and in all types of cargo may decrease CBP cargo holds, delays, and commodity returns or treatments. Ensuring compliance with CTPAT’s agricultural requirements will also help protect a key industry in the U.S. and the overall global fo Cereoa1 fotrc (e)9 (rall6D a)4 eria l001 Tw 15.62GTc -0.0019

D	B	NS	M/ B
---	---	----	------

9.6 Adequate lighting must be provided inside and outside the facility

D	B	
---	---	--

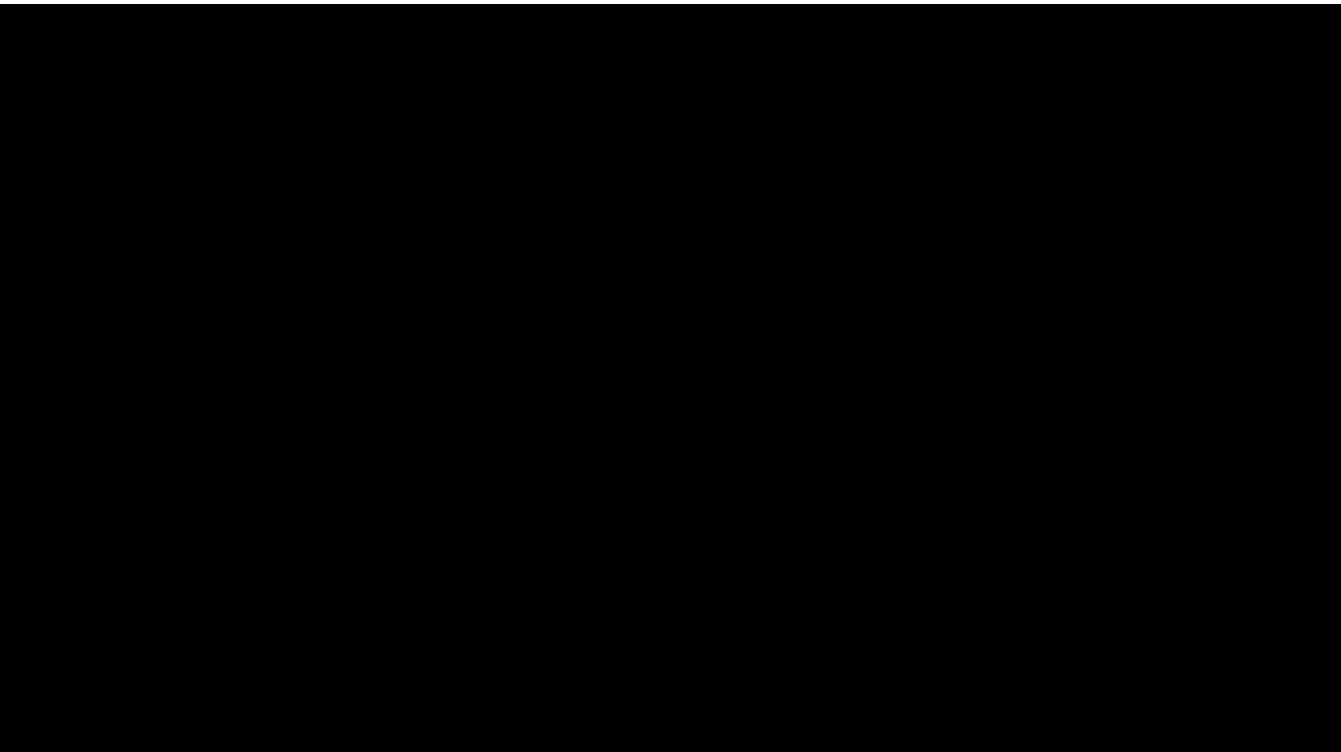
D	B	B	M/B
9.15	If camera systems are deployed, periodic, random reviews of the camera footage must be conducted (by management, security, or other designated personnel) to verify that cargo security procedures are being properly followed in accordance with the law. Results of the reviews must be summarized in writing to include any corrective actions taken. The results must be maintained for a sufficient time for audit purposes.	If camera footage is only reviewed for cause (as part of an investigation following a security breach etc.), the full benefit of having come	

D

6

D	B	B	B1 B
---	---	---	---------

10.2 Visitors, vendors, and service providers must present photo identification upon arrival. 8 (n u) 18.3 (a) 8 (l (n u),) 2 (a) 2.1 (nd a) 2.1 (li) 5.1 (o) 192 (g) 6.1 (mf) 8.8 (us) 10.5 (t) 2.6 (bde) 9 (mf) 8 (n u) (nt) 2.6 (a) 2.1 (8 (n u) (de) 9 d (t) 2.7 h(a) 2.1



CTPAT Minimum Security Criteria –

CTPAT Minimum Security Criteria –

2 ~~511v~~ CTPAT's security criteria are designed to form the basis of a layered security system. If one layer of security is overcome, another layer should prevent a security breach, or alert a company to a breach. Implementing and maintaining a layered security program needs the active participation and support of several departments and various personnel. One of the key aspects to maintaining a security program is training. Educating employees on what the threats are and how their role is important in protecting the company's supply chain is a significant aspect to the success and endurance of a supply chain security program. Moreover, when employees understand why security procedures are in place, they are much more likely to adhere to them.

D	E	P	M/6
---	---	---	-----

12.1 Members must establish and maintain a security training and awareness program to recognize and foster awareness of the security vulnerabilities to facilities, conveyances, and cargo at each point in the supply chain, which could be exploited by terrorists or contraband smugglers. The training program must be comprehensive and cover all of CTPAT's security requirements. Personnel in sensitive positions must receive additional specialized training geared toward the responsibilities that the position holds.

One of the key aspects of a security program is training. Employees who understand why security measures are in place are more likely to adhere to them. Security training must be provided to employees, as required, based on their functions and position on a regular basis, and newly hired employees must receive this training as part of their orientation/6 (a)ut(t)-3.3 2 (e)9 (-31.446 -1.22a)ut(p.li)-0.9 (o)-4.2 (k4.1 (r)-1.4 (i)-1.4.4 (o)-4.1 (79 (o)-.9 (n)-6.2 (i)-0.9 (n)-6.1

D	B	B	B/1 B
12.2	<p>Drivers and other personnel that conduct security and agricultural inspections of empty conveyances and Instruments of International Traffic (IIT) must be trained to inspect their conveyances/IIT for both security and agricultural purposes.</p> <p>Refresher training must be conducted periodically, as needed after an incident or security breach, or when there are changes to company procedures.</p> <p>Inspection training must include the following topics:</p> <ul style="list-style-type: none"> • Signs of hidden compartments; • Concealed contraband in naturally occurring compartments; and • Signs of pest contamination. 		Must
12.4	CTPAT Members should have measures in place to verify that the training provided met all training objectives.	Understanding the training and being able to use that training in one's position (for sensitive employees) is of paramount importance. Exams or quizzes, a simulation exercise/drill, or regular audits of procedures etc. are some of the measures that the Member may implement to determine the effectiveness of the training.	Should
12.8	As applicable, based on their functions and/or positions, personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/passphrases and computer access.	Quality training is important to lessen vulnerability to cyberattacks. A robust cybersecurity training program is usually one that is delivered to applicable personnel in a formal setting rather than simply through emails or memos.	Must
12.9	Personnel operating and managing security technology systems must receive operations and maintenance training in their specific areas. Prior experience with similar systems is a		

D	B	B	M/ B
12.10	Personnel must be trained on how to report security incidents and suspicious activities.	Procedures to report security incidents or suspicious activity are extremely important aspects of a security program. Training on how to report an incident can be included in the overall security training. Specialized training modules (based on job duties) may have more detailed training on reporting procedures, including specifics on the process, such as, what to report, to whom, how to report the incident, and what to do after the report is completed.	Must

Publication Number 0992-1119