HOW C-TPAT IDENTIFIES BEST PRACTICES

Best practices in a general sense are innovative security measures that exceed the C-TPAT minimum security criteria and industry standards.

In order for best practices to be effective, they should include high-level managerial support, employ a system of checks and balances, and have written and verifiable policies and procedures.

C-TPAT personnel have conducted over 8,000 validations and site visits since the publication of the 2006 Supply Chain Security Best Practices Catalog. The dynamic trade environment and diverse business models of C-TPAT partners have presented the program with new best practices. Included in this pamphlet is a snapshot of new best practices recently identified by the program.

THE BENEFIT OF ADOPTING SECURITY MEASURES

The best practices outlined in this document, if adopted, will protect the security of member companies as well as their economic health. As the global supply chain grows more secure, the United States will become more effective and efficient at preventing terrorists, terrorist weapons, narcotics, and other contraband from entering the country. This, in turn, prevents costly interruptions in the free and fair flow of trade.

OUR MISSION

As a core trade program within CBP, our mission is to:

- **Prevent terrorists and/or terrorist weapons from entering the United States** by partnering with members of the trade community to enhance the security of their international supply chains, with priority focus on foreign manufacturers through CBP clearance process.

- **Facilitate the flow of legitimate cargo** through the provision of partner incentives and benefits, while allowing CBP resources to concentrate on higher risk shipments.

- **Internalize the core principles of supply chain security** through cooperation and coordination with members of the international community, while simultaneously supporting and facilitating other CBP security initiatives (e.g., Free and Secure Trade, Secure Freight Initiative, and Container Security Initiative).

U.S. Customs and Border Protection
Office of Field Operations
C-TPAT Program
1300 Pennsylvania Avenue, NW
Washington, DC 20229
(202) 344-1180
industry.partnership@dhs.gov

Please visit the C-TPAT Portal’s Document Library

CBP Publication No. 0000-0823 April 2009

U.S. Customs and
Border Protection

C-TPAT
Customs-Trade
Partnership Against Terrorism

Customs-Trade Partnership Against Terrorism

Best Practices Update 2009

U.S. Customs and
Border Protection

RESPONDING TO OUR MEMBERS

Many organizations participating in C-TPAT have asked for updated information about today's best practices in supply chain security, and in this brochure we have responded to this need.

Thanks to your participation, the C-TPAT program has been a tremendous success, generating high levels of participation among industry partners, who are doing their part to enhance security policies and procedures at their facilities. In fact, the program has succeeded so well, and the industry has evolved so rapidly, that many of the best practices published in the 2006 Supply Chain Security Best Practices Catalog have essentially become the new industry standard.

Even if you cannot immediately adopt all of the best practices shown here, the more that you can put into practice, the more secure your operations will be—and the greater your potential for eventually reaching Tier 3 status. We encourage you to review the recommendations contained here and implement as many as make sense for your organization.

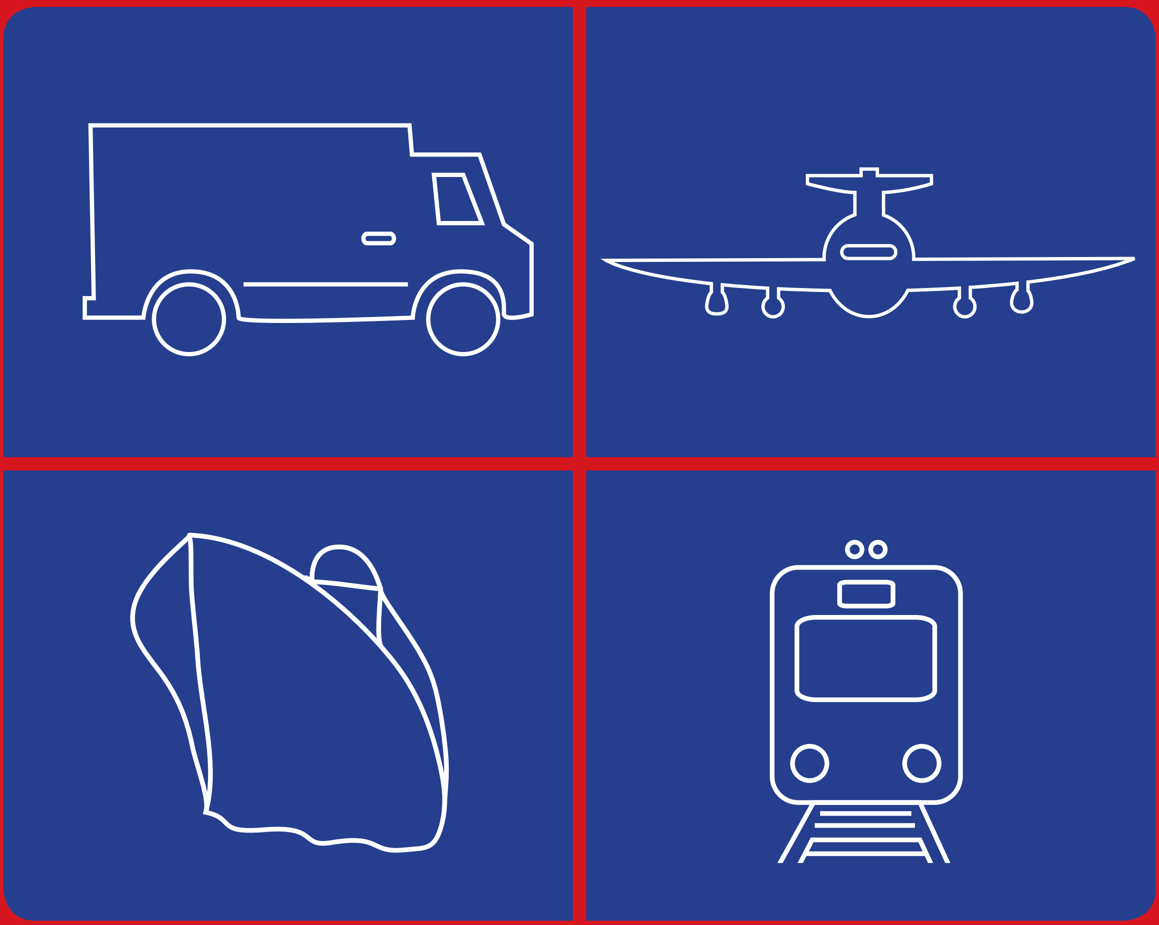
If you have any questions about these recommendations or the C-TPAT program, please contact your Supply Chain Security Specialist at the CBP.

THE WAY FORWARD

In 2006, C-TPAT published a Supply Chain Security Best Practices Catalog, which continues to serve as a valuable tool for the trade community. Building on this foundation, C-TPAT will continue to provide updated best practices on a regular basis via the program's secure web portal.

"C-TPAT is dedicated to meeting the needs of our members while also promoting the highest possible level of cargo security. We hope that this best practices update will be helpful to all."

—C-TPAT Director Bradd Skinner



OVERVIEW OF SUPPLY CHAIN SECURITY BEST PRACTICES

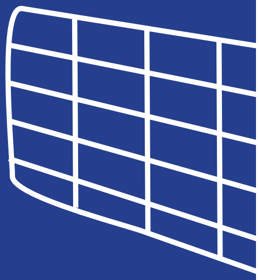
Applicable to C-TPAT members as well as all supply chain partner companies.

Security Criteria

- 🟥 Business Partner
- 🟦 Conveyance Security
- 🟫 Physical Access Control
- 🟩 Personnel Security
- 🟨 Procedural Security
- ◼ Physical Security
- 🟧 Security Training /Threat Awareness
- 🟪 Information Technology Security

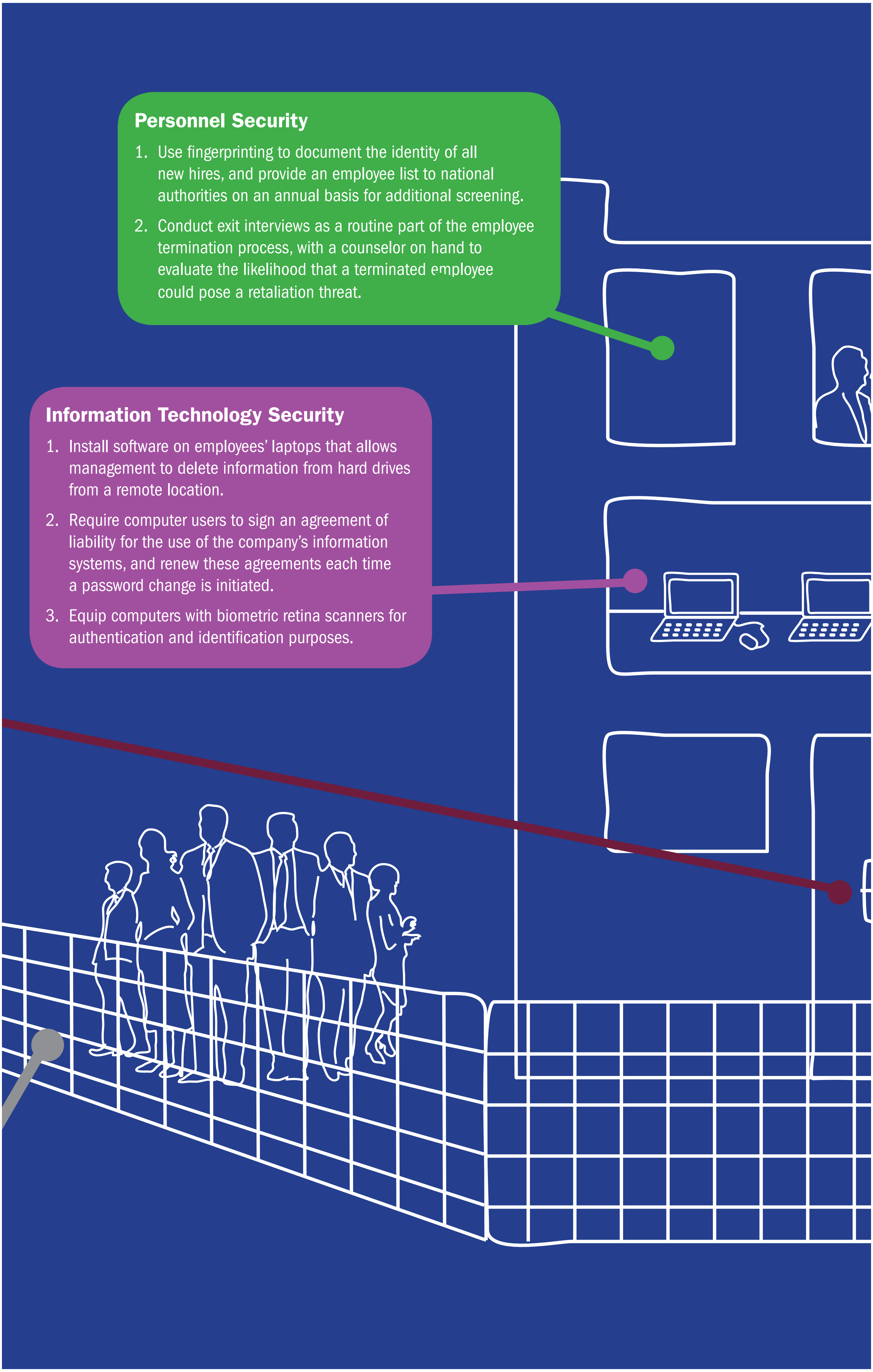
Physical Access Control

1. Ensure that as employees enter the facility, their photos are displayed on an electronic access system monitor so that the security guard in the area can verify that the individual entering matches the photo displayed on the monitor.
2. Issue all visitors thermal-activated visitor ID badges featuring expiration marking/coloring that appears after eight hours.
3. Ensure that the exterior doors of buildings are equipped with two-person key systems that require a company manager and security guard to unlock the facility.



Physical Security

1. Install a double-layered perimeter fence, creating a secure zone between the two fence lines. Ensure that both fences are equipped with electronic monitoring capabilities, and that the outer fence incorporates underground concrete to deter tunneling.
2. Maintain multiple alarm systems that include door contacts, heat and vibration sensors, and seismic movement detectors.



Personnel Security

1. Use fingerprinting to document the identity of all new hires, and provide an employee list to national authorities on an annual basis for additional screening.
2. Conduct exit interviews as a routine part of the employee termination process, with a counselor on hand to evaluate the likelihood that a terminated employee could pose a retaliation threat.

Information Technology Security

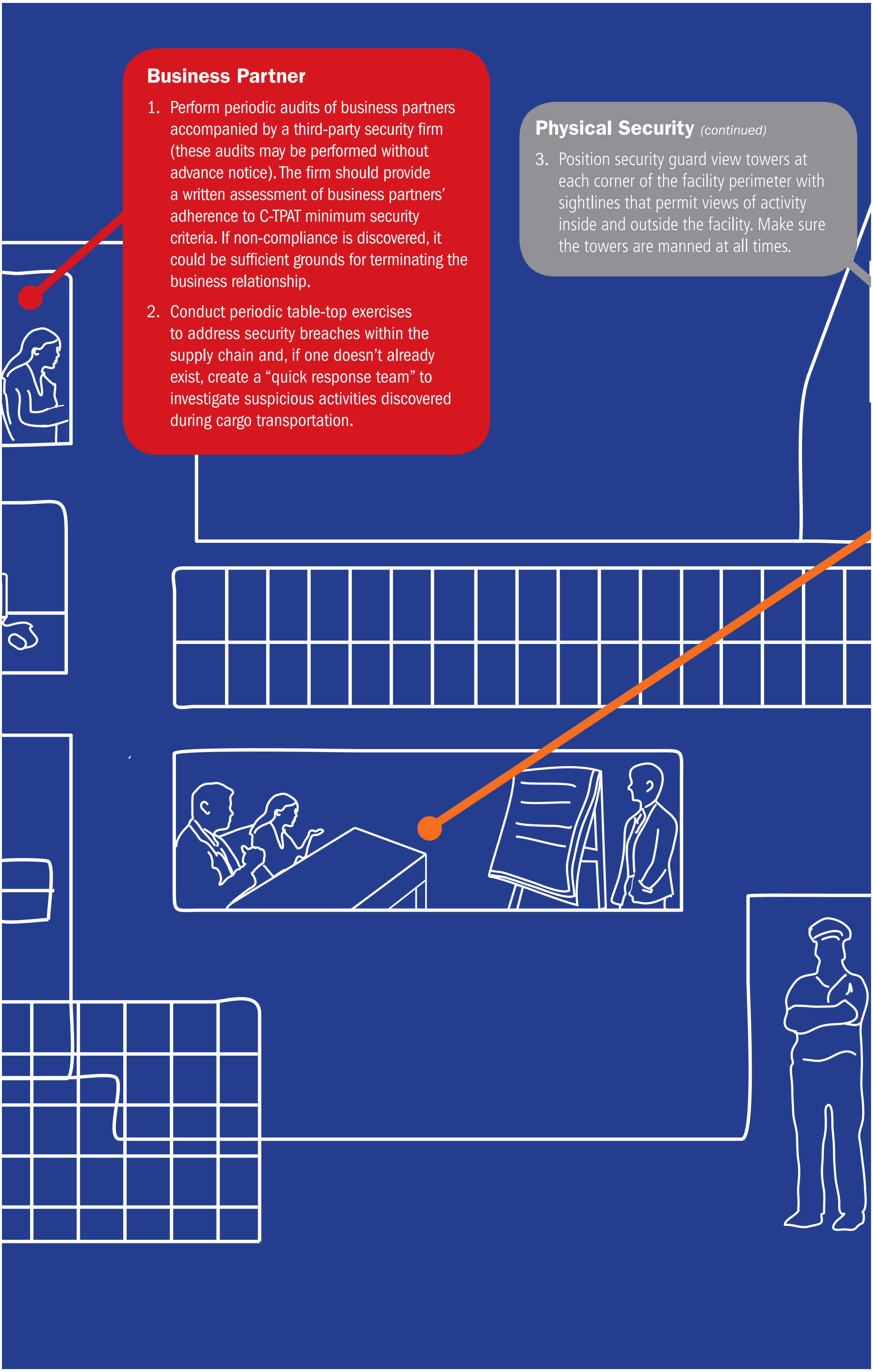
1. Install software on employees' laptops that allows management to delete information from hard drives from a remote location.
2. Require computer users to sign an agreement of liability for the use of the company's information systems, and renew these agreements each time a password change is initiated.
3. Equip computers with biometric retina scanners for authentication and identification purposes.

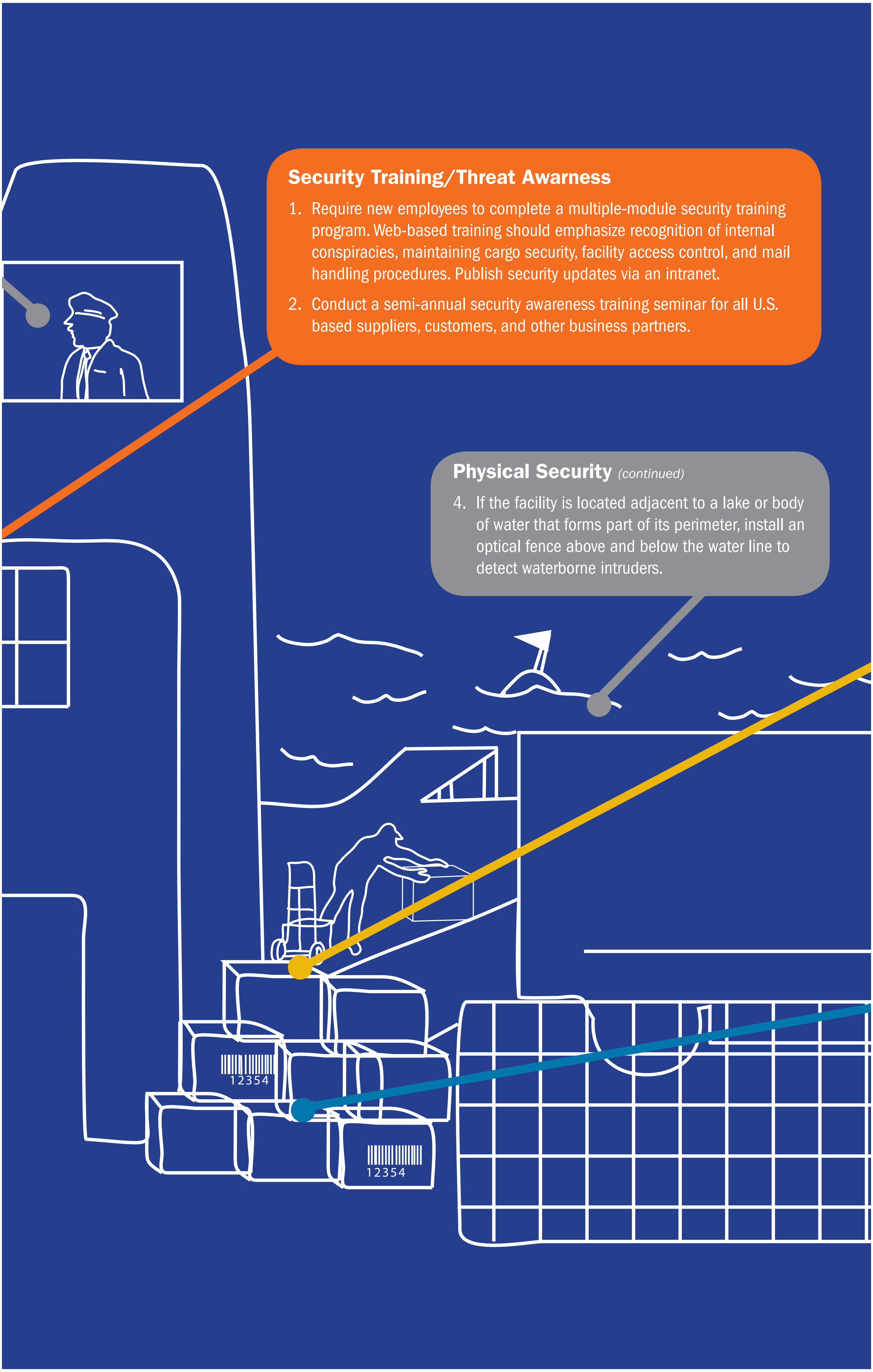
Business Partner

1. Perform periodic audits of business partners accompanied by a third-party security firm (these audits may be performed without advance notice). The firm should provide a written assessment of business partners' adherence to C-TPAT minimum security criteria. If non-compliance is discovered, it could be sufficient grounds for terminating the business relationship.
2. Conduct periodic table-top exercises to address security breaches within the supply chain and, if one doesn't already exist, create a "quick response team" to investigate suspicious activities discovered during cargo transportation.

Physical Security *(continued)*

3. Position security guard view towers at each corner of the facility perimeter with sightlines that permit views of activity inside and outside the facility. Make sure the towers are manned at all times.





Security Training/Threat Awarness

1. Require new employees to complete a multiple-module security training program. Web-based training should emphasize recognition of internal conspiracies, maintaining cargo security, facility access control, and mail handling procedures. Publish security updates via an intranet.
2. Conduct a semi-annual security awareness training seminar for all U.S. based suppliers, customers, and other business partners.

Physical Security *(continued)*

4. If the facility is located adjacent to a lake or body of water that forms part of its perimeter, install an optical fence above and below the water line to detect waterborne intruders.

Procedural Security

1. Use tamper-evident tape with serial numbers to seal cartons, and verify the serial numbers against the packing list when loading and at the final destination.
2. Schedule all deliveries at distribution centers in advance using an online automated tool, and ensure that upon arrival, drivers provide security guards with shipment-linked delivery numbers for verification.

Conveyance Security

1. Use tamper-indicative security labels bearing an actual photo of the seal and a serial number, attached to the hinges and between the two doors of the vehicles.
2. Use multiple ISO/PAS 17712 certified high security seals on all shipments bound to the U.S.
3. Use a dock locking arm to anchor the container chassis to the loading dock.
4. In addition to using a bolt seal, attach a cast iron J-bar device to the locking bar that requires a specialized tool for removal.