

Protective Measures Against Theft and Diversion

<p>Know Your Environment</p> 	<p>In order to identify potential theft and diversion, you should be able to answer the following questions about your typical customers as well as your products, inventory, or raw materials:</p> <ul style="list-style-type: none"> • Customers <ul style="list-style-type: none"> ○ Who are your typical customers? ○ How do they normally operate? ○ What do you need to know or verify about new customers? • Products, inventory, or raw materials <ul style="list-style-type: none"> ○ What in your inventory or facility might be stolen or redirected? ○ Who are the authorized buyers for monitored items? 	<p>Protect Against Internal Threats</p> 	<p>Protect against internal threats by screening your employees, ensuring access is restricted where needed and terminated if an employee is dismissed or laid off. Screen employees by:</p> <ul style="list-style-type: none"> • Establishing a smart hiring process (personal interviews, background checks, credit checks, etc.). • Conducting criminal/background checks on personnel with access to items of interest or the systems that control them.
<p>Monitor Inventory and Sales</p> 	<p>Monitor the following activities, implementing improved accounting practices, sales/ordering process controls, and recordkeeping as necessary:</p> <ul style="list-style-type: none"> • Sales, for exceptionally high or unusual orders. • Shipments and deliveries, to ensure they match expected methods (e.g., pick up, express shipments) and destinations, and arrive intact. • Payments and terms, to identify unusual transactions (e.g., cash, personal credit card or check, third party invoicing). 	<p>Train Employees</p> 	<p>Ensure that employees recognize the signs associated with theft and diversion and know what actions to take.</p> <ul style="list-style-type: none"> • Conduct theft and diversion awareness and identification training based on your risks. • Emphasize the importance of reporting and describe your reporting mechanisms. • Regularly review what to report and reporting procedures with employees. • Follow up reports of suspicious encounters or incidents in a team meeting. • If an incident occurs, update training as necessary.
<p>Restrict Physical and Cyber Access</p> 	<p>Protect physical and cyber access through the following:</p> <ul style="list-style-type: none"> • Establish a system to regularly monitor inventory and identify tampering. • Restrict and control access to high-risk or monitored information or inventory using physical measures, such as by using security personnel and inspections, locks, and other access controls as warranted. • Institute supply chain security initiatives. • Institute cybersecurity initiatives. 	<p>Document Actual & Suspicious Activities</p> 	<p>Documenting actual and suspicious activities may allow security and law enforcement personnel to identify trends and related incidents that are possible indicators of a larger conspiracy. To accomplish this:</p> <ul style="list-style-type: none"> • Implement internal reporting procedures. • Provide a reporting mechanism. • Encourage employees to report suspicious activities and security incidents.
		<p>Join or Form Partnerships</p> 	<p>Join existing partnerships or form new ones for critical infrastructure protection, including:</p> <ul style="list-style-type: none"> • Law enforcement partnerships, such as local and regional theft task forces. • Homeland security and other partnerships that focus on: <ul style="list-style-type: none"> ○ Strengthening the supply chain. ○ Physical and cyber security. • Industry partnerships that provide theft and diversion information relevant to your own business or industry.