

EMERGING THREATS TO CARGO AND PORT SECURITY

A Practical, Risk-Based Approach
to Prioritizing Resources to Detect, Deter, and Mitigate
Drug Trafficking Operations



Team Members:

Anna Cizek, United Airlines
Brogan Ingstad, The Chertoff Group
Channing Mavrellis, Global Financial Integrity
Douglas Brown, Transportation Security Administration (TSA)
Joseph "Kenny" Sobek, FBI Office of Private Sector (Contractor)

Team Champions:

CDR David Gates, U.S. Coast Guard
LT Ryan Coffin, U.S. Coast Guard



2021
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

DISCLAIMER STATEMENT: This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.

Table of Contents

Executive Summary	3
Key Intelligence Question	4
Risk-Based Assessment Factors	4
Maritime Port Classification Factors	5
Maritime Port Threat Factors	6
Maritime Port Vulnerability Factors	9
Risk-Based Assessment Weighting Methodology	12
Key Findings	13
Indicators of Criminal Activity and Infiltration at Ports	16
Mitigating the Risk of Organized Crime Presence in Ports	19
Areas for Future Study	20
Acknowledgements	22
Bibliography	23
Appendix A: Overview of Complete Port Assessment	26
Appendix B: Slicksheet	36

Executive Summary

The 2021 Public-Private Analytic Exchange Program (AEP) Emerging Threats to Cargo and Port Security Team (hereafter referred to as “the team”) conducted research and analysis in an effort to identify critical risk areas within the cargo and port security sector. The team incorporated both government and private industry perspectives in developing and refining its assessment. Given the widely dispersed geographic nature of the cargo and port security realm, and the broad regional diversity of cargo and port security needs, the team chose to focus its efforts on a single, nationally significant subcomponent of the cargo and port security topic: drug trafficking.

During the team’s exploratory research, drug trafficking organization (DTO) activities and maritime port security continually emerged as key areas of concern for most community stakeholders. Consequently, the following study is focused on threats posed by DTOs and their use of maritime ports to facilitate smuggling activities. Additionally, rather than focus on individual DTOs or specific drugs, the team chose to pursue a holistic approach aimed at analyzing DTO activities as a national level threat vector in order to provide a practical risk assessment to identify those United States ports at greater risk of criminal exploitation.

In an effort to address the lack of an extensive, national-level assessment regarding DTO activities at maritime ports, the team formulated a comprehensive, purpose-built, risk-based prioritization tool, which can be used to inform the allocation of critical security resources to U.S. maritime port facilities across the country. Additionally, the team developed an informational *Slicksheet*¹ product to complement its risk assessment and be a resource for port security personnel and managers. Combined, this practical approach provides maritime port security stakeholders with a data-driven and actionable methodology for identifying risk and prioritizing resources to detect, deter, and mitigate DTO threats to their specific facilities.

¹ *Slicksheets* are informative documents used amongst industry stakeholders such as the Federal Bureau of Investigation, that use facts, statistics, and graphics to succinctly describe intelligence issues of interest.

Key Intelligence Question

In 1997, the U.S. Department of Transportation released a report outlining the essential aspects of maritime port security, including the following objectives of port security:

The goal of port security is to establish an environment in which trade may be conducted with reasonably high assurance of being unencumbered by criminal activity and without becoming a conduit for such activity. A port security department should strive to constrict the opportunities for criminal exploitation of the maritime transportation system, its providers and users.²

With this goal in mind, and after speaking with maritime security professionals representing both the government and the private sector, the team formulated the following key intelligence questions, which guided the development of the assessment:

1. How can the federal government, law enforcement, and industry port operators use a risk-based approach to resource prioritization aimed at better detecting, deterring, and mitigating the smuggling operations of DTOs in a maritime port environment?
2. What are the key threats and vulnerabilities that may indicate a port is at greater risk of infiltration and exploitation by organized crime and that a port presents a more favorable environment/target for drug smuggling operations?

Risk-Based Assessment Factors

To develop and refine its assessment of the threats DTOs pose to maritime port facilities, the team considered a variety of risk factors, which could be utilized as part of a universally applicable risk-based assessment tool. The team also evaluated a variety of information sources to drive its analysis. This process involved open-source literature reviews of numerous public and private sector holdings, multiple in-depth interviews with a broad cross-section of community experts, and several lengthy group discussions.

Ultimately, the team's research efforts yielded a set of risk factors, which the team assesses represents the most reliable, consistent, and nationally-available metrics for determining the risk for DTO activities within maritime port facilities. These factors can be categorized as either vulnerabilities of or threats to the port.

These factors place a notable emphasis on the environment that exists around the ports themselves and how those may lead to greater risk of infiltration and exploitation by criminal actors. As such the factors focus on passenger volume, corruption, crime, local economy, and the volume of foreign containerized trade. These together are meant to capture the overall picture of a port's risk environment, which in turn may indicate a greater risk of drug smuggling and other criminal activities.

² U.S. Department of Transportation, *Port Security: A National Planning Guide* (Washington, D.C.: U.S. Department of Transportation, 1997), 2, <https://www.hsdl.org/?abstract&did=437492>.

This report recognizes the importance for DTOs to identify and exploit access points to a port whether by physical entry points, cyber intrusion, or insider threat. It is [notable] that four of these factors relate to insider threats and the potential susceptibility of employees to bribery, co-option, or coercion. Numerous studies, expert interviews, and criminal investigations have shown that insiders – both public and private sector port employees – can play pivotal roles in actively (e.g. bypassing security checks for containers) and/or passively (e.g. providing access cards) assisting organized criminal groups, making the recruitment or placement of complicit employees “highly sought.”³

The following is a discussion of how the maritime ports were classified as well as the factors selected when evaluating port threats and vulnerabilities.

Maritime Port Classification Factors

An initial challenge the team faced in evaluating the broad topic of emerging threats to cargo and port security was the fact that the United States maintains 360 commercial maritime ports of varying size, type, specialty, and location. Therefore, after the team elected to evaluate threats associated with DTO smuggling activities, additional preliminary research led the team to narrow its focus on only United States ports that facilitate containerized trade. This refinement enabled the team to reduce its initial port dataset by approximately 88%. In so doing, the team was able to not only maximize the efficiency of its further research, but it was also able to refine port classification factors. Combined, these factors offered the team a richer and more relevant dataset than attempting to evaluate the full array of ports in the United States.⁴ Listed below, are the factors that the team used to identify and classify ports.

- **Port Type.** First, each port was classified based on its designation as a deepwater port. Taking into consideration channel depth, ports were categorized into either *deepwater* port or *other*. Second, taking into consideration coastal proximity, ports were categorized further into either the *seaport* or the *river port* categories.
- **Port Size.** Each port was classified by its overall size, which was derived as a combination of total trade volume and physical area.
- **Passenger Cruise Terminal Status.** Each port was classified by the presence of a passenger cruise terminal. For the purposes of this study, a port was only considered positive for a cruise terminal when it contained a dedicated terminal for large, oceangoing, commercial cruise vessels.
- **Cruise Passenger Volume.** Each applicable port’s total annual volume of cruise ship passengers was collected in an effort to evaluate the potential risk associated with

³ Robby Roks, Lieselot Bisschop, and Richard Staring, “Getting a foot in the door. Spaces of cocaine trafficking in the Port of Rotterdam,” *Trends in Organized Crime* 24, no. 2 (2021): 184, <https://link.springer.com/content/pdf/10.1007/s12117-020-09394-8.pdf>; Leonid Lantsman, “Seaport Vulnerability to Criminal Networks: A Mixed Method Approach to Measuring Criminological Vulnerability in the Top 30 U.S. Container Ports,” PhD diss., (City University of New York, 2017), 25, https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=3018&context=gc_etds.

⁴ The dataset for port classification factors was obtained from the following sources: “USA Ports by State,” World Port Source, accessed May 2021, <http://www.worldportsource.com/index.php>; “Ports Compared,” US Trade Numbers, accessed May 2021, <https://www.ustradenumbers.com>; and individual port authority websites.

significant volumes of civilians transiting the port facility. The team focused on total passenger volume for calendar year 2019, as the COVID-19 pandemic drastically skewed cruise passenger trends throughout 2020. Utilization of this factor was strongly supported by interviews with Senior Intelligence Officers at the United States Customs and Border Protection's (CBP) National Targeting Center, as well as multiple federal government studies. Collectively, these resources highlight that cruise ship passengers and crew members account for a notable volume of drug smuggling incidents each year.⁵

- ***Historical Imports and Exports.*** The team collected the top three imports and exports for each port as of March 2020, listed by commodity description.

Maritime Port Threat Factors

According to the DHS Lexicon Terms and Definitions, 2017 Edition Revision 2, a threat may be defined as an “indication of potential harm to life, information, operations, the environment and/or property.” Additionally, a threat “may be a natural or human-created occurrence and includes capabilities, intentions, and attack methods of adversaries used to exploit circumstances or occurrences with the intent to cause harm.”⁶ The team utilized this definition when identifying potential threats to be incorporated into the assessment. Given the wide degree of variability in how local and regional criminal activities are cataloged, the team chose to consider only threat factors with data that could be obtained via a national-level or otherwise nationally comprehensive repository. Although this approach may potentially result in minor loss of fidelity for data held solely at the local level, it ensures data consistency in the team's effort to develop a reliable risk assessment tool that can be applied to any United States port.

The team determined that the following threat factors combine to provide the most reliable forecast of DTO threat intensity that a port facility will likely experience.

Prevalence of Public Corruption

Public corruption was included as a factor because it opens a potential door for criminal actors to access public officials, infiltrate port environments, and ensure greater success of smuggling activities. Public corruption can be defined as a “breach of public trust and/or abuse of position by federal, state, or local officials and their private sector accomplices,” and can involve the

⁵ “Cruise Ship Employee Sentenced To 10 Years For Drug Smuggling,” U.S. Department of Justice, March 11, 2016, <https://www.justice.gov/usao-mdfl/pr/cruise-ship-employee-sentenced-10-years-drug-smuggling>; Drug Enforcement Administration, U.S. Department of Justice, *2018 National Drug Threat Assessment* (Washington, D.C.: Drug Enforcement Administration, October 2018), 55, 132, <https://www.dea.gov/sites/default/files/2018-11/DIR-032-18%202018%20NDTA%20final%20low%20resolution.pdf>; U.S. Congress, Senate, Committee on the Judiciary, Subcommittee on Criminal Justice Oversight, *Caribbean Drug Trafficking: Return of the Caribbean Connection*, 106th Cong., 2nd sess., 2000, <https://www.govinfo.gov/content/pkg/CHRG-106shrg73139/html/CHRG-106shrg73139.htm>; “Virginia man sentenced to federal prison in conspiracy to import heroin and cocaine using cruise ship employees,” U.S. Immigration and Customs Enforcement, March 5, 2012, <https://www.ice.gov/news/releases/virginia-man-sentenced-federal-prison-conspiracy-import-heroin-and-cocaine-using>;

⁶ U.S. Department of Homeland Security, *DHS Lexicon Terms and Definitions 2017 Edition – Revision 2*. Washington, D.C.: U.S. Department of Homeland Security, October 16, 2021. https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

demand, solicitation, acceptance, or agreement by a public official for anything of value in return for influence over their official duties.⁷

Based on conversations with maritime domain professionals, both in the government and the private sector, the team identified public corruption as a possible threat factor, which could impact the security of the port and act as a potential enabler or catalyst for criminal activity in the port environment. During one such discussion, a representative from the Intelligence Community with extensive experience in maritime and port security explained that ports are often very different from one another and that the same can be said for their cargo facilities and operations. Port environments often experience economic disparity and in many cases are located in areas that are economically disadvantaged. Taking into account the potential for public corruption where these facilities are located, corruption opens opportunities for insider threats and criminal actors because of the unique, insular environment around ports. DTOs may seek to infiltrate these areas and port facilities that are especially isolated from other federal or law enforcement presence, as monitoring at these areas may be less effective.⁸

SafeSeas, a network of researchers studying maritime security and ocean governance, notes that while there may be a lack of empirical work on corruption in the maritime sector, it is undeniable that “for the shipping industry corruption at ports have (sic) been a reality for decades,” and that maritime corruption affects, among other things, “transnational organized crime and other illegal activities, such as smuggling of people and drugs, piracy and terrorism.”⁹

To assess the level of corruption in the port environment, the team used as an indicator the number of federal public corruption convictions per district over the decade 2010-2019. The data comes from the U.S. Department of Justice’s *Report to Congress on the Activities and Operations of the Public Integrity Section for 2019*.¹⁰ The team considered ports located in districts with higher numbers of federal public corruption convictions to be at a higher risk of corruption within the port environment.

Prevalence of Crime

The purpose of including this factor is to incorporate data that may provide insight into the state of the organized crime environment around ports. In an interview with the United States National Targeting Center, one representative pointed out that “one thing that does not get enough attention is the influence of organized crime in the ports” and that it is possible that some ports in the U.S. may have significant organized crime influence. As an indicator for crime prevalence, the team gathered crime rate data for each port’s surrounding metropolitan statistical area (MSA), as defined

⁷ “Public corruption,” Legal Information Institute, Cornell Law School, accessed May 2021, https://www.law.cornell.edu/wex/public_corruption#:~:text=Public%20corruption%20involves%20a%20breach,and%20their%20private%20sector%20accomplices.

⁸ Team interview with Sharon Halstead, Office of the Director of National Intelligence and Federal Bureau of Investigation, [25 Feb 2021].

⁹ Morten Koch Andersen, “What we know about corruption in the maritime sector,” SafeSeas, 25 July 2020, <http://www.safeseas.net/what-we-know-about-corruption-in-the-maritime-sector/>.

¹⁰ Public Integrity Section, Criminal Division, US Department of Justice, *Report to Congress on the Activities and Operations of the Public Integrity Section for 2019* (Washington, D.C.: US Department of Justice, 2019), 25-28, <https://www.justice.gov/criminal-pin/file/1346061/download>.

by the Federal Bureau of Investigation's (FBI) Uniform Crime Reporting (UCR) Program and the Crime in the United States statistics for the year 2018.¹¹

For the purposes of this study, the crime rate factor includes both violent crimes and property crimes. In cases where MSA data was unavailable, city data was utilized. The UCR Program as well as the Crime in the United States report were selected as data sources because they provide harmonized, comprehensive, and complete reporting of U.S. crime statistics as submitted by relevant law enforcement agencies. The FBI advises that any comparisons of crime among different locales should take into consideration relevant factors in addition to the area's crime statistics. However, the rates used in this risk assessment were not for the purposes of ranking, but to ensure criminal activity was incorporated into the final score for each port. In this case, the higher the crime rate in a particular MSA, the higher risk for potential infiltrations and prevalence of organized crime in that port.

Drug Seizure Events

The number of drug seizure events in a given area is a strong indication of the level of drug trafficking, and therefore, whether a particular port environment may be at greater risk to smuggling activities. The team collected the cumulative totals of all United States Customs and Border Protection (CBP) drug seizure events from January 2018 through April 2021, categorized by CBP Field Office, as an indicator. Rather than evaluate this metric from a drug volume-centric perspective, the team chose to focus on the raw number of individual seizure events. This approach is more representative of the relative frequency of seizure events within any given region.¹² The amount of known drug seizure events is considered a key indicator of threat. The greater the number of seizure events, the greater the threat level to the port environment.

Proximity to A Drug Trafficking Area

A vast majority of illegal narcotics that arrive in the United States each year – cocaine, heroin, amphetamine-type stimulants, synthetic opioids, cannabis, etc. – are produced in or transit through Latin America and the Caribbean (LAC). Drugs can either pass through drug smuggling corridors, or be loaded into container ships bound for United States ports.

Proximity to these corridors is considered an important risk factor in this analysis. Each port was classified on a scale of Low, Medium, or High for its geographic proximity to an historical drug trafficking area.¹³ High-risk is denoted if the port falls in southern California or the Texas coastline. Medium-Risk is donated for Northern California or the rest of the Gulf of Mexico. Low-Risk is reserved for the eastern or northwestern seaboard.

¹¹ "Crime Data Explorer," Federal Bureau of Investigation, accessed May 2021, <https://crime-data-explorer.app.cloud.gov/pages/home>.

¹² "Drug Seizure Statistics," U.S. Customs and Border Protection, accessed May 2021, <https://www.cbp.gov/newsroom/stats/drug-seizure-statistics>.

¹³ Drug Enforcement Administration, US Department of Justice, *2020 National Drug Threat Assessment* (Washington, D.C.: Drug Enforcement Administration, March 2021), 33-35, 58, 65-76, [https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment WEB.pdf](https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment%20WEB.pdf).

Maritime Port Vulnerability Factors

The team defines port vulnerability as flaws, weaknesses, or areas in the port environment, which expose a port to harm; among other things, vulnerabilities can be physical, cyber, and/or human. The vulnerability factors that contribute to a port's overall risk for DTO activities, like the threat factors above, were chosen after consultation with community experts and after thorough review of available unclassified data sources. The team assesses that the following vulnerabilities represent the broadest cross-section of data which is both reliable and also consistently available on a national level: Economic Inequality, Debt-to-Income Ratio, and Foreign Containerized Trade.

Vulnerabilities can also be understood in the literature to be technical flaws in systems that could enable threat actor exploit. For the purposes of this research, the decision was made to focus on more high-level structural factors rather than specific technical vulnerabilities for a few reasons. First, the cyber threat landscape is vast in nature, and a number of technical vulnerabilities or Common Vulnerability Exploits (CVEs) will be specific to the devices used at each port and their patching cadence. Second, from a broader policy perspective, the community cannot legislate against future vulnerabilities because they have not been disclosed yet and are ever changing and evolving. For these reasons, and the intricate factors that construct each port's technical vulnerability threat landscape, the team decided to focus the research away from technical flaws.

It is worthwhile to highlight that three of the non-technical vulnerability factors take into consideration local demographics. The demographic of the local population surrounding the port is an important factor as the majority of the public and private sector employees at the port will come from the community.

Economic Inequality

Evaluating the possibility of an insider threat at ports requires, in part, scrutinizing the demographics and norms of the population from which public and private sector employees are drawn. One component of this is economic inequality, which refers to the disparity in income and wealth between the wealthiest and poorest in a population. Research has shown a positive correlation between the levels of income inequality and corruption as well as crime.

According to a Harvard University study, as income inequality increases, the wealthy have "both greater motivation and opportunity to engage in corruption, while the poor are more vulnerable to extortion and less able to monitor and hold the rich and powerful accountable... Inequality also adversely affects people's social norms about corruption and beliefs about the legitimacy of rules and institutions, and thereby makes it easier to tolerate corruption as acceptable behavior."¹⁴ Additionally, a study of organized crime in Italy found a positive correlation between inequality and organized crime development.

The above suggests that with higher levels of inequality, those most affected by it are potentially more likely to be co-opted into accepting or engaging in corrupt and/or criminal activities. The income distribution across a population can be represented by the Gini coefficient, which shows

¹⁴ Jong-Sung You and Sanjeev Khagram, "A Comparative Study of Inequality and Corruption," Faculty Research Working Paper Series RWP04-001 (Cambridge, MA: Harvard University, 2004), 2, <https://www.hks.harvard.edu/publications/inequality-and-corruption>.

the difference between what the top one percent makes in comparison to the bottom 99 percent. A Gini score of 10, for example, would signify that the top one percent makes 10 times more than the bottom 99 percent. Data was obtained from the Economic Policy Institute for the most recent year available, 2015.¹⁵ Leveraging Gini Coefficients, a port's surrounding area with a Gini Coefficient closer to 1 (more unequal) received a higher weighted risk score than ports with surrounding areas closer to 0 (more equal).

Debt-to-Income Ratio

Another important consideration is the motivations of those individuals who act intentionally. Some malicious actors may be disgruntled employees acting out of revenge, whereas others are motivated by financial reasons: greed or need. To take into account those who might be motivated by need – specifically debt – and might be susceptible to bribery, we compiled the debt-to-income ratio for the county in which each port is located. Financial stressors are “one of the key risk factors that can lead to malicious insider threats.”¹⁶

Eric Shaw and Laura Sellers developed the Critical-Path Method, a framework that evaluates the factors that increase the likelihood of individuals becoming a malicious insider. They noted that financial stressors, such as debt, “especially place pressure on those who possess vulnerable predispositions and can lead such individuals down the next step on the critical path.”¹⁷ The data for this indicator was obtained from the Federal Reserve’s county-level debt-to-income ratio for the year 2019.¹⁸ Areas surrounding a port with a higher debt-to-income ratio received a higher weighted risk score than surrounding areas that were in aggregate less in debt.

Foreign Containerized Trade

The team identified three sub-categories that highlight potential trade-based vulnerabilities that a port may face, based on historic DTO tactics, techniques, and procedures. The following three sub-factors were evaluated:

- Total raw containerized volume in metric tons;
- Containerized cargo percentage with respect to total port volume; and
- Percentage of containerized cargo originating in LAC region.

The decision to factor in the percentage of containerized cargo specifically coming from the LAC region is due to the fact that the overwhelming majority of narcotics that are trafficked into or through the United States are moved by Mexican DTOs and are produced in Mexico or South America.¹⁹ Data were obtained from the U.S. Census Bureau’s USA Trade Online database.

¹⁵ “Income inequality in the United States,” Economic Policy Institute, accessed 27 May 2021, <https://www.epi.org/multimedia/unequal-states-of-america/>.

¹⁶ Bryan Denson, “How financial triggers can help spot insider threats,” GCN, August 5, 2020, <https://gcn.com/articles/2020/08/05/financial-triggers-insider-threat.aspx>.

¹⁷ Eric Shaw and Laura Sellers, “Application of the Critical-Path Method to Evaluate Insider Risks,” *Studies in Intelligence* 59, no. 2 (June 2015): 4, <https://www.cia.gov/static/2cb216188d28738a6adc6f2b35da7357/Application-of-Critical-Path.pdf>.

¹⁸ “County-Level Debt-to-Income Ratio, 1999-2020,” Board of Governors of the Federal Reserve System, accessed May 2021, https://www.federalreserve.gov/releases/z1/dataviz/household_debt/county/map/#state:all;year:2019.

¹⁹ Drug Enforcement Administration, *2020 National Drug Threat Assessment* (Washington, D.C.: Drug

Summary

The above classification, threat and vulnerability factors provide a multi-dimensional view of any given port's potential risk with regard to DTO smuggling activities. The quantitative and qualitative data elements that feed these risk factors can be continually updated based on the ever-changing port environment, and will, thereby, enable port security stakeholders to continually reassess their facilities' risks and prioritize resources accordingly. After gathering an exhaustive breadth of data for each of the above factors, the team relied on its research and interviews to analyze and weight the factors' correlations, associations, and interactions to develop an overarching risk-based assessment model.

Enforcement Administration, 2021), 9,13-15,21,24-25,33-34,57, https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf.

Risk-Based Assessment Weighting Methodology

Risk is a function of threat, vulnerability, and consequence (TxVxC). As part of this analysis, the AEP team endeavored to create a risk weighting that allowed for a proper understanding of risk between different port environments. For this analysis, consequence is assumed to be static - the introduction of drugs into the United States is the single outcome of concern, and it affects the country the same regardless of where they are introduced. Thus, our risk score was developed as a function of a threat score and a vulnerability score only, with equal weightings (50 and 50) adding up to a maximum possible risk score of 100. A wide variety of factors contribute to threat and vulnerability viewed through the lens of drug trafficking. The relative weighting for the factors outlined above are highlighted below.

Table 1. Risk scoring matrix

Risk Scoring (100 Points Total)			
Threat Score (50/100)		Vulnerability Score (50/100)	
Threat Factor	Threat Weighting	Vulnerability Factor	Vulnerability Weighting
Total Federal Public Corruption Convictions by District from 2010-2019	25%	Economic Inequality (Gini Coefficient)	25%
Crime Rate per 100,000 Inhabitants*	25%	Debt-to-Income Ratio	25%
Drug Seizure Events (2018-2021 YTD)	25%	Percent of containerized trade from LAC	50%
Proximity Risk	25%		

Threat and vulnerability factors were assessed in quartiles based on the minimum and maximum of the sample size. For instance, drug seizure incidents range from 114 to 8,471 depending on the port. If the number of drug seizure incidents landed in the first quartile, the port would be assigned 25 points. The second most quartile would be 50 points, the third 75 points, and the fourth 100 points. All threat and vulnerability factors were assessed by quartiles with the exception of proximity risk. Proximity Risk was assessed as High, Medium, and Low, with point totals of 75, 50, and 25 allocated respectively.

In addition to these weightings, this analysis recognizes the unique risk considerations of cruise liners in a commercial port environment. It assumes the presence of a large number of annual cruise passengers expands the risk profile of a port beyond containerized cargo. As such, cruise passenger volumes were assessed by quartiles, with values of 0, 2, 4, 6, and 8 added to the overall risk score after threat and vulnerability scores were finalized. 0 means the port has no cruise terminal. 8 means the port has the highest number of cruise passengers.

Key Findings

The AEP team applied its risk assessment methodology to all U.S. container ports, creating a risk score for each port to help gauge variance of risk levels between ports. The below represents the top ten ports by this risk score.

Port	City & County	Type	Size	Cruise Passenger Volume	Cruise Passenger Volume Sub Score	Threat Score	Vulnerability Score	Risk Score
Port of Los Angeles	Los Angeles, CA Los Angeles County	Deepwater Seaport	Very Large	650,010	2	87.5	62.5	77
Port Everglades	Fort Lauderdale, FL Broward County	Seaport	Medium	1,931,000	6	62.5	75	74.75
Port of Miami	Miami, FL Miami-Dade County	Seaport	Medium	3,403,000	8	62.5	68.75	73.625

Port of Newark	Newark, NJ Essex County	Deepwater Seaport	Very Large	348,000	2		62.5		75		70.75
Port of Houston	Houston, TX Harris County	Seaport	Very Large	NA	0		62.5		68.75		65.625
Port of Long Beach	Long Beach, CA Los Angeles County	Deepwater Seaport	Very Large	696,000	2		87.5		37.5		64.5
Port of Hueneme	Oxnard, CA Ventura County	Deepwater Seaport	Medium	NA	0		81.25		37.5		59.375

Port of New York	Brooklyn, NY Staten Island, NY	Deepwater Seaport	Very Large	550,085	2		62.5		50		58.25
Port of Palm Beach	Palm Beach, FL Palm Beach County	Seaport	Medium	NA	0		62.5		50		56.25
Port of Jacksonville	Jacksonville, FL Duval County	Seaport	Large	195,000	2		56.25		50		55.125

Port Risk Scores Table Summary

The team's risk assessment tool yielded risk scores for the nation's 43 largest containerized cargo ports. Each risk score was derived by the application of the risk assessment methodology outlined above, based on analysis of the classification, vulnerability and threat factors described in the Risk-Based Assessment Factors section. The table above illustrates the ten highest scoring ports, which are:

Port of Los Angeles, 77; Port Everglades, 74.75; Port of Miami, 73.63; Port of Newark, 70.75; Port of Houston, 68.63; Port of Long Beach, 64.5; Port of Hueneme, 59.38; Port of New York, 58.25; Port of Palm Beach, 56.25; Port of Jacksonville, 55.125.

Indicators of Criminal Activity and Infiltration at Ports

To provide port and maritime security partners with additional resources to help potentially identify the presence of criminal and smuggling activities at their facilities, the team identified a list of indicators categorized by the threats included in the assessment. These indicators are primarily categorized by insider threat/corruption, criminal activity, and cyber, and are derived from a combination of FBI, open source, and private sector reporting.

This is not an exhaustive list, and there may be other behavioral indicators or conduct that should be reported to law enforcement for potential investigation. A totality of behavioral indicators and other relevant circumstances must be evaluated when considering law enforcement notification or response

Insider Threat and Corruption:

TSA defines Insider Threat as the threat that an individual with authorized access to sensitive areas and/or information will wittingly or unwittingly misuse or allow others to misuse this access in an effort to exploit vulnerabilities to compromise security, facilitate criminal activity, terrorism, or other illicit actions that inflict harm to people, organizations, the transportation system, or national security (2020 TSA Insider Threat Roadmap).

U.S. ports may vary in terms of insider threat risk as a result of the factors presented in this assessment. As noted earlier in the assessment, trusted insiders and port employees who are susceptible to corruption may be targeted by criminal organizations to gain critical access that would help facilitate smuggling activities.

- Increased reports of employees engaging in illicit activities
- Port personnel reporting suspicious contacts either at work or outside of the port
- Increase in employment applications or hiring of temporary workers with criminal histories or little prior experience working in ports or incomplete background checks on temporary employees
- Unsolicited employment attempts by foreign nationals or individuals not associated with port operations
- Reporting of suspicious behavior by employees with authority to manipulate access or schedules
- Employees working unusual hours or accessing the site without authorization
- Increased reporting of lost credentials or access badges used to access the port or maritime facility
- Reports of security or other personnel bypassing routine protocols to gain access, introduce equipment, or remove items in or near restricted zones or areas outside their responsibility
- Atypical employee requests to work with a specific company, vendor, or with specific cargo; unauthorized attempts or accesses by employees or others to transfer areas
- Increase in reports of cargo not inspected according to routine or expected policies and procedures

Criminal Activity:

Port Environment

- Increased regional drug supply or other criminal activity in proximity to port or intermodal facilities
- Observed increase in theft of containers or trailers on port grounds or in proximity to the port
- Atypical or increased reporting of suspicious activity, citations, warnings, tickets around railcars and rail yards, motor carrier terminals, air parks or correlated activity at organizations or entities with access (e.g., vendors, suppliers, etc.)

Port Access

- Increased reports of attempts to enter the port, maritime, or intermodal facility with fraudulent identification or credentials (e.g., Transportation Worker Identification Credential (TWIC), access card, or license)
- Increased reports or occurrences of unauthorized people successfully gaining access to the port or maritime facility or being granted access privileges beyond required use
- Reports or occurrences of inappropriate or suspicious behavior during site visits

Surveillance and Elicitation

- Individuals monitoring or conducting surveillance of port entry and exit points, vehicles, vessels, port operations, parking areas, or personnel
- Reports or occurrences of unauthorized individuals observed near port or maritime facilities or intermodal connection points after normal hours of operation or at times of secured access
- Suspicious questions about the security, technology, products, or cyber processes of a port or maritime facility by persons with no authorized purpose or need to know

Vessel Activity, Traffic, and Crew

- Observed increase in unusual, atypical, or suspicious maritime traffic in or near the port
- Unusual crew size or composition, increased reports of missing or absent crew from vessels, or crewmembers disembarking or making atypical personal contacts at the port
- Suspicious signaling or transmissions between personnel, devices, or other devices from vessels, individuals, or equipment
- Suspicious transfer of items between vessels, shore, or port

Other Suspicious Activity

- Persons arriving or departing the port with unusual items, luggage, or packages
- Disturbed or sabotaged fencing, security equipment, or lighting on port or facility
- Reports of tempered or disturbed cases or unusual modifications to shipping container scanning equipment
- Interruptions of RFID reading processes or unauthorized tracking of containers

- A pattern of reduced or unusual interception rates for contraband and unauthorized cargo in other channels or modes of transportation
- Increased reporting of extra or missing inventory in cargo or shipments or atypical discrepancies on manifests and bills of lading

Cyber:

Though not directly incorporated into the assessment, the cyber realm is increasingly becoming a potential vector for criminals to exploit port and maritime facilities to facilitate smuggling and other illegal activity. In one case from 2013, a Dutch-based DTO hid drugs among legitimate cargo shipped in containers from South America, and employed hackers based in Belgium to “infiltrate computer networks in at least two companies operating in the port of Antwerp.” The hackers were then able to access data necessary to identify the location and security details of containers, thereby allowing the criminal group to steal the cargo before the legitimate owner arrived.²⁰

- Suspicious scanning of the port’s Internet Technology (IT) and operational systems such as prior intrusion attempts to test IT security strength
- Reporting or indications of GPS jamming, Distributed Denial of Service attacks (DDOS) disruption, or malfunction at the port or in the area
- Increase in Advanced Persistent Threat (APT), hacktivist, or cybercriminal attacks across port networks or related verticals
- Irregular or unusual login times by port personnel to port networks in addition to suspicious login locations as demarcated by Internet Protocol (IP) addresses
- Weaponization of Common Vulnerability Exploits (CVEs) impacting systems leveraged in the port environment
- Illicit exposure or sale of port employee credentials across dark market forums including but not limited to the Raid and Exploit forums
- Third-Party data exposures impacting the port environment via Application Program Interface (API) connectivity, shared systems, or Personally Identifiable Information (PII) belonging to shared customers or travelers
- Cyberattacks targeting intellectual property leveraged in the port environment for purposes of intelligence collection, replication, or exploitation
- Typo-squatted domains mimicking port authorities for economic gain, credential harvesting, and fraud
- Adversarial trends and Tactics, Techniques, and Procedures (TTPs) intended to spread malware and gain a foothold on the port network including but not limited to social engineering threats such as phishing and vishing

²⁰ Bateman, Tom. “Police Warning after Drug Traffickers’ Cyber-Attack.” BBC News. BBC, October 16, 2013. <https://www.bbc.com/news/world-europe-24539417>.

Mitigating the Risk of Organized Crime Presence in Ports

Based on the above indicators, the team developed a series of potential mitigation strategies that may be employed within a port environment to combat drug smuggling operations carried out by organized crime. This does not represent an exhaustive list, but rather a starting point for ports and maritime security professionals to consider when confronting criminal and DTO influence at their facilities. These are meant to reflect established industry best practices, recommendations from DHS and other critical infrastructure partners, and not require extensive commitment of resources.

All port employees, security personnel, and managers can contribute towards port security and safety. Most smuggling operations require some degree of involvement from individuals with routine access to sensitive import/export processes. A robust insider threat program by port operators can help monitor anomalous behavior of employees and screen against insider-based risk factors. Additionally, port and maritime security professionals may consider the following:

- Monitor international reporting to help identify criminal trends and incorporate into risk posture
- Leverage automatic exchange of custom declarations between country partners, particularly those countries that are high-risk as source and transit countries for narcotics and other illicit goods
- Ensure employee vetting processes are in place, including a financial triggers program that monitors employees' credit risks; for example, employers could have a credit bureau notify them if an employee's overall debt reaches a particular threshold
- Emphasize importance of controlling the physical access to the port facility (TWIC)
- If permitted by law, consider requiring valid ID from all employees, customers, and visitors to any port or maritime facility
- Develop clear reporting guidelines for suspicious activities
- Keep a lookout for and document suspicious activities or things considered to be outside the norm for port operations
- Ask questions, listen to answers, and document responses in case they warrant notification to law enforcement or security personnel
- Establish close working relationship with local, state, and federal law enforcement partners
- Engage in public-private partnerships between public sector actors (e.g., CBP, US Coast Guard, etc.) and private sector actors (e.g., port operators, unions, freight forwarders, shipping companies, etc.) at ports to improve both formal and informal communication as well as detect, prevent, and disrupt illicit activity
- Implement cyber hygiene practices, including those recommended by DHS, CISA, FBI, and other government partners

Areas for Future Study

The team sought to present the most broadly accessible and impactful risk assessment tool for the maritime port security community. This approach was driven by our research and the availability of relevant data and was also guided by our effort to efficiently utilize available time and resources as part of the AEP. As the Emerging Threats to Cargo and Port Security topic continues to evolve, future study into various subtopics or approaching the topic from differing perspectives may yield additional relevant findings that could supplement the team's existing research and analysis. Specifically, the team identified three areas for potential future study.

First, it may be worthwhile to approach the same DTO smuggling topic but analyzed from the perspective of threats associated with specific drug types. The team chose not to parse drug smuggling events or DTO activities according to drug type. However, additional research into this aspect of the broader issue may indeed result in further refinement of the team's existing risk assessment tool. One potential challenge in this regard is obtaining nationally available and consistently formatted reporting data at an unclassified level. Another challenge is that current CBP seizure data is aggregated at the regional level; there is not publicly-available seizure data disaggregated at the port level. Such data granularity would likely be required in order to develop a drug-specific risk assessment tool. Additionally, regarding other areas for potential further study, sourcing reliable and consistent data may pose a challenge. The team found this to be true with our research areas and we expect future researchers may face similar difficulties. However, if such data can be gathered, it would certainly aid in refining existing DTO-based risk assessments for the cargo and port security industry.

Second, the team's research and interviews strongly indicated that threats posed by DTO smuggling activities at land ports of entry and airports were relatively well understood and accounted for by current security practices. The same body of research and interviews indicated that the maritime ports realm has a greater perceived gap in DTO threat awareness. Consequently, the maritime ports sector is where the team chose to focus its work. However, with additional time and resources, future researchers may find that exploring existing DTO-based threat assessment methodologies for both land ports of entry and airports may advance community-wide DTO threat awareness. Such research and analysis would depend on robust coordination with a broad array of government and industry stakeholders across numerous modes of transportation and multiple industries. This may pose a challenge due to divergent interests, geography, terminology and policy considerations. Nevertheless, such an expanded research initiative may further enhance DTO threat awareness across the entire cargo and port security sector.

Third, future groups may utilize a broader array of vulnerabilities, which, if properly sourced, could add additional insight into the overall risk assessment process. Additional vulnerabilities, which could be incorporated into future iterations of the risk assessment may include:

- Port security funding (Port Security Grant Program)
- Presence and reports of small vessels
- Concentration of high-value cargo
- Vehicle traffic in the port environment
- Intermodal connections

- Port divergence - dispersion of container traffic across ports
- Port automation
- Presence of freight forwarding and peripheral companies
- Relationships between certain labor organizations and organized crime
- Other forms of corruption, in addition to public corruption
- Export cargo vulnerability

While each of these potential vulnerabilities would require additional metrics to effectively incorporate them into the risk assessment, each could be valuable factors for further study and analysis to strengthen future assessments.²¹

²¹ Lantsman, "Seaport Vulnerability to Criminal Networks," 193-196.

Acknowledgements

The team would like to thank those experts who took the time to speak with us during the research phase of this project as well as those who took the time to review the report and provide feedback.

The team members would also like to thank their employers for allowing us to participate in the Public-Private Analytic Exchange Program:



DISCLAIMER STATEMENT: The views and opinions expressed in this document do not necessarily state or reflect those of The Chertoff Group, United Airlines, Global Financial Integrity, the Transportation Security Administration, the U.S. Coast Guard, or the Federal Bureau of Investigation.

Bibliography

- Bateman, Tom. "Police Warning after Drug Traffickers' Cyber-Attack." BBC News. BBC, October 16, 2013. <https://www.bbc.com/news/world-europe-24539417>.
- "County-Level Debt-to-Income Ratio, 1999-2020." Board of Governors of the Federal Reserve System, accessed May 2021. https://www.federalreserve.gov/releases/z1/dataviz/household_debt/county/map/#state:all;year:2019.
- "Crime Data Explorer." Federal Bureau of Investigation, accessed May 2021. <https://crime-data-explorer.app.cloud.gov/pages/home>.
- "Cruise Ship Employee Sentenced To 10 Years For Drug Smuggling." U.S. Department of Justice, March 11, 2016. <https://www.justice.gov/usao-mdfl/pr/cruise-ship-employee-sentenced-10-years-drug-smuggling>.
- Denson, Bryan. "How financial triggers can help spot insider threats." GCN, August 5, 2020, <https://gcn.com/articles/2020/08/05/financial-triggers-insider-threat.aspx>.
- Drug Enforcement Administration, U.S. Department of Justice. *2018 National Drug Threat Assessment*. Washington, D.C.: Drug Enforcement Administration, October 2018. <https://www.dea.gov/sites/default/files/2018-11/DIR-032-18%202018%20NDTA%20final%20low%20resolution.pdf>.
- Drug Enforcement Administration, U.S. Department of Justice. *2020 National Drug Threat Assessment*. Washington, D.C.: Drug Enforcement Administration, March 2021. https://www.dea.gov/sites/default/files/2021-02/DIR-008-21%202020%20National%20Drug%20Threat%20Assessment_WEB.pdf.
- "Drug Seizure Statistics." U.S. Customs and Border Protection, accessed May 2021. <https://www.cbp.gov/newsroom/stats/drug-seizure-statistics>.
- "Income inequality in the United States." Economic Policy Institute, accessed 27 May 2021. <https://www.epi.org/multimedia/unequal-states-of-america/>.
- Koch Andersen, Morten. "What we know about corruption in the maritime sector." SafeSeas, 25 July 2020. <http://www.safeseas.net/what-we-know-about-corruption-in-the-maritime-sector/>.
- Lantsman, Leonid. "Seaport Vulnerability to Criminal Networks: A Mixed Method Approach to Measuring Criminological Vulnerability in the Top 30 U.S. Container Ports." PhD diss. City University of New York, 2017. https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=3018&context=gc_etds.

- “Personal Income by County and Metropolitan Area, 2019.” Bureau of Economic Analysis, U.S. Department of Commerce, November 17, 2020. https://www.bea.gov/sites/default/files/2020-11/lapi1120_1.pdf.
- “Ports Compared.” US Trade Numbers, accessed May 2021. <https://www.ustradenumbers.com>.
- “Public corruption.” Legal Information Institute, Cornell Law School, accessed May 2021. https://www.law.cornell.edu/wex/public_corruption#:~:text=Public%20corruption%20involves%20a%20breach,and%20their%20private%20sector%20accomplices.
- Public Integrity Section, Criminal Division, US Department of Justice. *Report to Congress on the Activities and Operations of the Public Integrity Section for 2019*. Washington, D.C.: U.S. Department of Justice, 2019. <https://www.justice.gov/criminal-pin/file/1346061/download>.
- Roks, Robby, Lieselot Bisschop, and Richard Staring. “Getting a foot in the door. Spaces of cocaine trafficking in the Port of Rotterdam.” *Trends in Organized Crime* 24, no. 2 (2021): 171-188. <https://link.springer.com/content/pdf/10.1007/s12117-020-09394-8.pdf>.
- Shaw, Eric, and Laura Sellers. “Application of the Critical-Path Method to Evaluate Insider Risks,” *Studies in Intelligence* 59, no. 2 (June 2015): 1-8. <https://www.cia.gov/static/2cb216188d28738a6adc6f2b35da7357/Application-of-Critical-Path.pdf>.
- U.S. Congress, Senate, Committee on the Judiciary, Subcommittee on Criminal Justice Oversight. *Caribbean Drug Trafficking: Return of the Caribbean Connection*. 106th Cong., 2nd sess., 2000. <https://www.govinfo.gov/content/pkg/CHRG-106shrg73139/html/CHRG-106shrg73139.htm>.
- U.S. Department of Homeland Security, *DHS Lexicon Terms and Definitions 2017 Edition – Revision 2*. Washington, D.C.: U.S. Department of Homeland Security, October 16, 2021. https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf
- U.S. Department of Transportation. *Port Security: A National Planning Guide*. Washington, D.C.: U.S. Department of Transportation, 1997. <https://www.hsdl.org/?abstract&did=437492>.
- “USA Ports by State.” World Port Source, accessed May 2021. <http://www.worldportsource.com/index.php>.
- “Virginia man sentenced to federal prison in conspiracy to import heroin and cocaine using cruise ship employees.” U.S. Immigration and Customs Enforcement, March 5, 2012. <https://www.ice.gov/news/releases/virginia-man-sentenced-federal-prison-conspiracy-import-heroin-and-cocaine-using>.
- You, Jong-Sung, and Sanjeev Khagram. “A Comparative Study of Inequality and Corruption,” Faculty Research Working Paper Series RWP04-001. Cambridge, MA: Harvard University, 2004. <https://www.hks.harvard.edu/publications/inequality-and-corruption>.

DISCLAIMER STATEMENT: This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.

Appendix A: Overview of Complete Port Assessment

Port	City & County	Type	Size	Cruise Passenger Volume	Cruise Passenger Volume Sub Score		Threat Score		Vulnerability Score		Risk Score
Port of Los Angeles	Los Angeles, CA Los Angeles County	Deepwater Seaport	Very Large	650,010	2		87.5		62.5		77
Port Everglades	Fort Lauderdale, FL Broward County	Seaport	Medium	1,931,000	6		62.5		75		74.75
Port of Miami	Miami, FL Miami-Dade County	Seaport	Medium	3,403,000	8		62.5		68.75		73.625

Port of Newark	Newark, NJ Essex County	Deepwater Seaport	Very Large	348,000	2		62.5		75		70.75
Port of Houston	Houston, TX Harris County	Seaport	Very Large	NA	0		62.5		68.75		65.625
Port of Long Beach	Long Beach, CA Los Angeles County	Deepwater Seaport	Very Large	696,000	2		87.5		37.5		64.5
Port of Hueneme	Oxnard, CA Ventura County	Deepwater Seaport	Medium	NA	0		81.25		37.5		59.375

Port of New York	Brooklyn, NY Staten Island, NY	Deepwater Seaport	Very Large	550,085	2		62.5		50		58.25
Port of Palm Beach	Palm Beach, FL Palm Beach County	Seaport	Medium	NA	0		62.5		50		56.25
Port of Jacksonville	Jacksonville, FL Duval County	Seaport	Large	195,000	2		56.25		50		55.125
Port of Galveston	Galveston, TX Galveston County	Seaport	Medium	1,092,000	4		62.5		37.5		54

Port of Philadelphia	Philadelphia, PA Philadelphia County	River Port	Large	NA	0		43.75		62.5		53.125
Port of Oakland	Oakland, CA Alameda County	Deepwater Seaport	Very Large	NA	0		56.25		43.75		50
Port of Fernandina	Fernandina Beach, FL Nassau County	Seaport	Small	NA	0		56.25		43.75		50
Port of San Diego	San Diego, CA San Diego County	Deepwater Seaport	Very Large	242,000	2		50		43.75		48.875

Port of Baltimore	Baltimore, MD Baltimore County	Deepwater Seaport	Very Large	224,000	2		56.25		37.5		48.875
Port Tampa Bay	Tampa, FL Hillsborough County	Seaport	Large	514,000	2		50		39.75		46.875
Port of Gulfport	Gulfport, MS Harrison County	Seaport	Small	NA	0		50		43.75		46.875
Port Freeport	Freeport, TX Brazoria County	Seaport	Medium	NA	0		62.5		31.25		46.875

Port of Canaveral	Cape Canaveral, FL Brevard County	Seaport	Medium	2,243,000	6		50		31.25		46.625
Port of New Orleans	New Orleans, LA Orleans Parish	River Port	Very Large	586,000	2		43.75		43.75		45.75
Port Charleston	Charleston, SC Charleston County	Deepwater Seaport	Very Large	262,776	2		37.5		50		45.75
Port of Norfolk	Norfolk, VA Norfolk City County	Deepwater Seaport	Very Large	41,600	2		50		37.5		45.75

Port of Seattle	Seattle, WA King County	Seaport	Very Large	596,127	2		43.75		43.75		45.75
Port of Wilmington	Wilmington, DE New Castle County	Seaport	Medium	NA	0		31.25		56.25		43.75
Port of Richmond	Richmond, VA Richmond County	River Port	Small	NA	0		50		37.5		43.75
Port of Savannah	Savannah, GA Chatham County	Seaport	Medium	NA	0		37.5		43.75		40.625

Port of Brownsville	Brownsville, TX Cameron County	Seaport	Medium	NA	0		56.25		25		40.625
Port of Tacoma	Tacoma, WA Pierce County	Seaport	Very Large	NA	0		43.75		37.5		40.625
Port of Everett	Everett, WA Snohomish County	Seaport	Medium	NA	0		43.75		37.5		40.625
Port of Mobile	Mobile, AL Mobile County	Deepwater Seaport	Large	114,000	2		50		25		39.5

Port of Boston	Boston, MA Suffolk County	Deepwater Seaport	Very Large	402,346	2		31.25		37.5		36.375
Port of Portland	Portland, ME Cumberland County	Seaport	Medium	NA	0		37.5		31.25		34.375
Port of Chester	Chester, PA Delaware County	River Port	Medium	NA	0		37.5		31.25		34.375
Port of Longview	Longview, WA Cowlitz County	River Port	Small	NA	0		31.25		37.5		34.375

Port of Wilmington	Wilmington, NC New Hanover County	Seaport	Medium	NA	0		31.25		31.25		31.25
Port of Portland	Portland, OR Multnomah County	River Port	Medium	NA	0		37.5		25		31.25
Port of Portsmouth	Portsmouth, NH Rockingham County	Seaport	Medium	NA	0		25		31.25		28.125
Port of Eastport	Eastport, ME Washington County	Pier, Jetty or Wharf	Very Small	NA	0		37.5		12.5		25



ASSESSING U.S. PORT RISK FOR CRIMINAL ACTIVITY

The 2021 AEP Emerging Threats to Cargo and Port Security Team developed a risk assessment for the 40 largest U.S. ports to aid resource prioritization and allocation across U.S. ports to better detect, deter, and mitigate Drug Trafficking Organization (DTO) operations. The risk score was a function of equally-weighted threat and vulnerability sub-scores, along with cruise passenger volume, and is meant to incorporate critical factors of the ports and their surrounding areas that could place them at higher risk for exploitation by DTOs.

Cruise Passenger Volume

- Each port's total volume of cruise ship passengers for 2019
- Potential risk associated with significant volumes of civilians transiting the port facility

Threat Factors

- Public Corruption
- Regional Crime Rate
- Drug Seizure Events
- Proximity to a Drug Trafficking Area

Vulnerability Factors

- Foreign Containerized Trade and Cargo Volume
- Economic Inequality (Gini Coefficient)
- Debt-to-Income Ratio

Top 10 Ports at Greatest Risk of DTO Exploitation and Activity

Port	City	Threat Score	Vulnerability Score	Overall Risk Score
Port of Los Angeles	Los Angeles, CA	87.5	62.5	77
Port of Everglades	Fort Lauderdale, FL	62.5	75	74.75
Port of Miami	Miami, FL	62.5	68.75	73.625
Port of Newark	Newark, NJ	62.5	75	70.75
Port of Houston	Houston, TX	62.5	68.75	65.625
Port of Long Beach	Long Beach, CA	87.5	37.5	64.5
Port of Hueneme	Oxnard, CA	81.25	37.5	59.375
Port of New York	Brooklyn, NY Staten Island, NY	62.5	50	58.25
Port of Palm Beach	Palm Beach, FL	62.5	50	56.25
Port of Jacksonville	Jacksonville, FL	56.25	50	55.125

This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.



Disclosure Is Not Limited

TLP:WHITE



GLOBAL FINANCIAL INTEGRITY



UNITED



RISK INDICATORS AND MITIGATION OVERVIEW

The following suspicious activities/indicators include but are not limited to any individual, group, or activity (these indicators should be observed in context and not individually). This list is not exhaustive, and a totality of indicators and relevant circumstances should be evaluated when reporting to law enforcement or security.

Criminal Operations

- Increased regional drug supply, theft of containers, or other criminal activity in proximity to the port
- Atypical reporting of suspicious activity, citations, warnings, or tickets around port/intermodal facilities
- Increased reports of attempts or successful entry of the port, maritime, or intermodal facility with fraudulent identification or credentials
- Individuals monitoring or conducting surveillance of port entry and exit points, vehicles, vessels, port operations, parking areas, or personnel
- Suspicious questions about the security, technology, products, or cyber processes of a port or maritime facility by persons with no authorized purpose or need to know
- Suspicious transfer of items between vessels, shore, port
- A pattern of reduced or unusual interception rates for contraband and unauthorized cargo

Insider Threat and Corruption

- Increased reports of employees engaging in illicit activities or suspicious contacts
- Increased employment or applications for workers with criminal histories or little prior experience working in ports
- Suspicious behavior by employees with authority to manipulate access or schedules
- Employees working unusual hours or accessing sites without authorization
- Increased reports of lost credentials or access badges
- Reports of security or other personnel bypassing routine protocols
- Atypical employee requests to work with a specific company, vendor, or with specific cargo
- Increased reporting of cargo not being inspected according to routine or expected policies and procedures

Considerations for Mitigating Risk to Port, Vessel, and Intermodal Security

Local

- Maintain robust insider threat training program
- Implement and educate workforce regarding cyber hygiene practices
- Develop clear reporting guidelines for suspicious activities
- Ensure employee vetting processes are in place, including a financial triggers program
- Emphasize importance of controlling the physical access to the port facility (TWIC)

National

- Establish close working relationship with local, state, and federal law enforcement partners
- Engage in public-private partnerships to share information and best practices

International

- Implement automatic exchange of custom declarations between country partners
- Monitor international reporting to help identify criminal trends and develop risk posture

The 2021 DHS AEP facilitates teams of government analysts, including from the Intelligence Community (IC), and private sector analysts to better understand emerging threats by collaborating on topics of mutual interest. For more information and to access deliverables from previous years, please visit <https://www.dhs.gov/private-sector-engagement>.



Disclosure Is Not Limited

TLP:WHITE



GLOBAL FINANCIAL INTEGRITY



UNITED