Protected Critical Infrastructure Information (PCII) Submission Confirmation and Submitter Information

For the submitter

Thank you for your submission!

Your submission identification number is **PCII-IST-WI-009007**.

Please use this number to identify your submission for all communications with the PCII Program.

Your submission was received, validated, and marked as Protected Critical Infrastructure Information and is protected as PCII in accordance with the Critical Infrastructure Information Act of 2002 (CII Act) and 6 Code of Federal Regulations Part 29, "Procedures for Handling Critical Infrastructure Information." The Department of Homeland Security will retain your submission. The PCII markings, protections and access requirements apply to the submission held by the Government.

Handling of PCII:

- Only Federal, State, local, tribal, and territorial government employees and their contractors who are approved PCII Authorized Users with a valid need-to-know may access PCII. Penalties exist for the improper handling and unauthorized disclosure of PCII.
- The CII Act and 6 CFR Part 29 do not establish handling requirements for PCII submitters. However, PCII submitters are strongly encouraged to follow best practices for handling sensitive proprietary information.
- The protections of the CII Act apply specifically to critical infrastructure information received, validated, and marked by the DHS PCII Program as PCII.

Suggested Best Practices for Submitter Copies:

- Keep this sheet with the copy of your PCII submission and retain the PCII tracking number.
- Password-protect your digital copy of the PCII, and store your hardcopy or digital copy of the PCII submission in a manner that prevents unauthorized access or viewing.
- Exercise caution in how the copy of your submission is stored, protected, and shared. Keep your copy of the submission as a separate document or file and do not commingle it with other information.

Please note the following:

- The copy of the submission retained by the submitter is not protected as PCII.
- Submitters are free to assert the protections described in 6 CFR Part 29 with regard to the submitter's copy.
- A Federal, State, or local agency that receives PCII may utilize the PCII only for purposes appropriate under the CII Act.
- PCII may not be utilized for any other collateral regulatory purposes without the written consent of the PCII Program Manager and of the submitting person or entity. 6 CFR Part 29 Section 29.3(b).
- PCII is exempt from disclosure under the Freedom of Information Act and any State or local law requiring disclosure of records or information. 6 CFR Part 29 Section 29.8(g).
- PCII cannot be used by third parties in civil actions without the submitter's express written consent. 6 CFR Part Section 29.8(c).
- Your submission may lose PCII protections if the information becomes "customarily accessible in the public domain." 6 CFR Part 29 Section 29.5(a)(4).

For more information on the PCII program, please refer to 6 CFR Part 29 or read more at https://www.cisa.gov/pcii-program

This page intentionally left blank.

Homeland Security

INFRASTRUCTURE SURVEY
SECURITY & RESILIENCE REPORT

Port of Milwaukee
Milwaukee, WI 53207

This page intentionally left blank.

Table of Contents

Figures

Infrastructure Survey Tool Overview

On behalf of the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), Infrastructure Security Division, thank you for your participation in the Infrastructure Survey Tool (IST) process. We appreciate the opportunity to work with you through this process to assist your organization in improving its physical and operational security and overall resilience.

The IST is a risk-informed assessment applied to facilities, complexes, buffer areas, and systems. The IST methodology is aligned to support the 2013 National Infrastructure Protection Plan, *Partnering for Critical Infrastructure Security and Resilience,* which guides the national effort to manage risk to the Nation's critical infrastructure using an integrated approach to:

- Identify, deter, detect, disrupt, and prepare for threats and hazards;
- Reduce vulnerabilities of critical assets, systems, and networks; and
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

This report provides a list of identified significant assets or areas (SAAs) and lists commendable actions (what the facility is doing well), vulnerabilities (what the facility could improve), and options for consideration (potential security or resilience enhancements). This information is based on a Protective Security Advisor's (PSA's) observations and discussions with key site personnel.

IST Process and Products

During the visit, a PSA assists a critical infrastructure owner or operator in accomplishing the following objectives:

- Identify and document critical infrastructure on which the facility depends, security measures in place, and resilience factors (preparedness, mitigation measures, response capabilities, recovery mechanisms);
- Evaluate the facility's security and resilience posture; identify all-hazards vulnerabilities; and provide options for consideration to increase security and resilience planning and to support potential resource allocation to mitigate those vulnerabilities; and
- Facilitate information sharing among public and private-sector partners.

DHS uses the Protected Critical Infrastructure Information Program to protect the confidentiality and integrity of the information collected and the resultant IST products. IST products include this report and two Dashboards - the Protective Measures Index (PMI) and the Resilience Measures Index (RMI) - that compare the security and resilience of the facility to other like facilities across the Nation. The Dashboards can be used as a benefit-analysis tool, allowing an owner or operator to experiment with changes to his or her facility's security and resilience measures and instantly see the impact of those changes in various scenarios. Experience has proven the Dashboards to be valuable tools for visually presenting proposals for security and resilience changes to C-Level corporate leaders. NOTE: This report represents a snapshot of the comparison of the facility's current security and resilience

posture to like facilities, as of January 28, 2022. The Dashboards provide near real-time comparison data.

DHS conducted a visit the week of August 11, 2021, at Port of Milwaukee.

Site Representative(s)

- Adam Tindall-Schlicht
  Email: adam.tindall.schlicht@milwaukee.gov
  Office: 414-708-4956
  Cell: 414-708-4956
  24-hour Contact: 414-286-3511

Visit Participants

- Eric Polzin
  Email: epolzin@milwaukee.gov
- John Dermyer
  Email: jdermy@milwaukee.gov
  Office: 414-286-3610
  Cell: 414-708-9891
- Brian Kasprzyk
  Email: bkaspr@milwaukee.gov
  Office: 414-286-8141
  Cell: 414-708-4213
- Matthew Schwister
  Email: mschwister@gmail.com
  Office: 414-722-2640
- John Luckey
  Office: 414-507-3578
- Judy Siettmann
  Email: jsiett@milwaukee.gov
  Office: 414-232-4955
  Cell: 414-286-2677

Facility Description

Port of Milwaukee is a major economic driver for not only the City of Milwaukee and the State of Wisconsin; it also provides a critical supply chain option for myriad of critical manufacturing and other key business partners throughout Wisconsin and surrounding states in the Midwest. The port provides direct access to the St. Lawrence Seaway system, the Mississippi River inland system, the North American rail system, and other multi-modal supply chains that facilitate regional, national, and global trade options for businesses in the region. Port of Milwaukee generates more than $100 million in business revenue for partners using the port and facilitates the shipment of 2-3 million tons of goods and various cargo with more than $3 billion in added value annually. Port of Milwaukee also serves as the government administrator and grantee of Foreign Trade Zone (FTZ) No. 41, which includes the 12 counties of Southeastern Wisconsin. The FTZ enhances the competitiveness of local manufacturers and distributors via deferrals, reductions or complete elimination of tariffs. Port of Milwaukee is also the sole Lake Michigan port approved to serve the Mississippi River inland waterway system with direct river barge access from the Port of Illinois River. In addition, the Port of Milwaukee has recently expanded operations to facilitate and host cruise ships servicing the Great Lakes and beyond. Both Viking Cruises and Pearl Seas cruise lines have announced they will use the Port of Milwaukee as a port of call, and Pearl Seas has stated that its vessel, “the Pearl Mist,” will use Milwaukee as its home port. Port of Milwaukee is a municipal entity under the jurisdiction of the City of Milwaukee. Oversight is provided by a seven-member Board of Harbor Commissioners.

Port of Milwaukee is located on Jones Island, due South of downtown Milwaukee, and directly adjacent to the Henry Maier Festival Park. The port encompasses 467 acres of commercial and industrial space and has more than 330,000 square feet of covered space, including more than 30,000 square feet of climate-controlled warehousing for storage use. The port also has approximately 300,000 barrels of bulk liquid storage capacity onsite, with servicing capabilities via vessel, pipeline, rail, and/or truck. The port contains 16 berths, each capable of handling vessels with a Seaway maximum draft of 26.5 feet at normal water conditions and a length of 1000 feet. The port also has two dedicated barge berths with drafts in excess of 18 feet. On the north end of the port is Milwaukee Metropolitan Sewerage District (MMSD) Jones Island Wastewater Treatment Facility as well as the termination point for the MMSD deep water tunnel. An elevated section of Interstate (I)-794 also traverses along the eastern edge of the port and crosses over the Milwaukee River via the Hoan Bridge. The port owns and operates a number of heavy lift cranes which have the capability to load/unload cargo up to 300 tons via the City Heavy Lift Dock (CHLD). The port also owns approximately 14 miles of railroad track and is serviced by two Class I railroads, Union Pacific (UP) and Canadian Pacific (CP). Both UP and CP provide direct pier delivery at all Port facilities, as well as necessary switching services, on a daily basis at the port. The port also includes a new Dredged Material Management Facility on the southeastern corner of Jones Island which will be used to contain approximately 1.9 million cubic yards of sediment from the Milwaukee estuary and will eventually facilitate expansion of the port. The facility occupies 467 acres.

Figure 1 shows Port of Milwaukee.

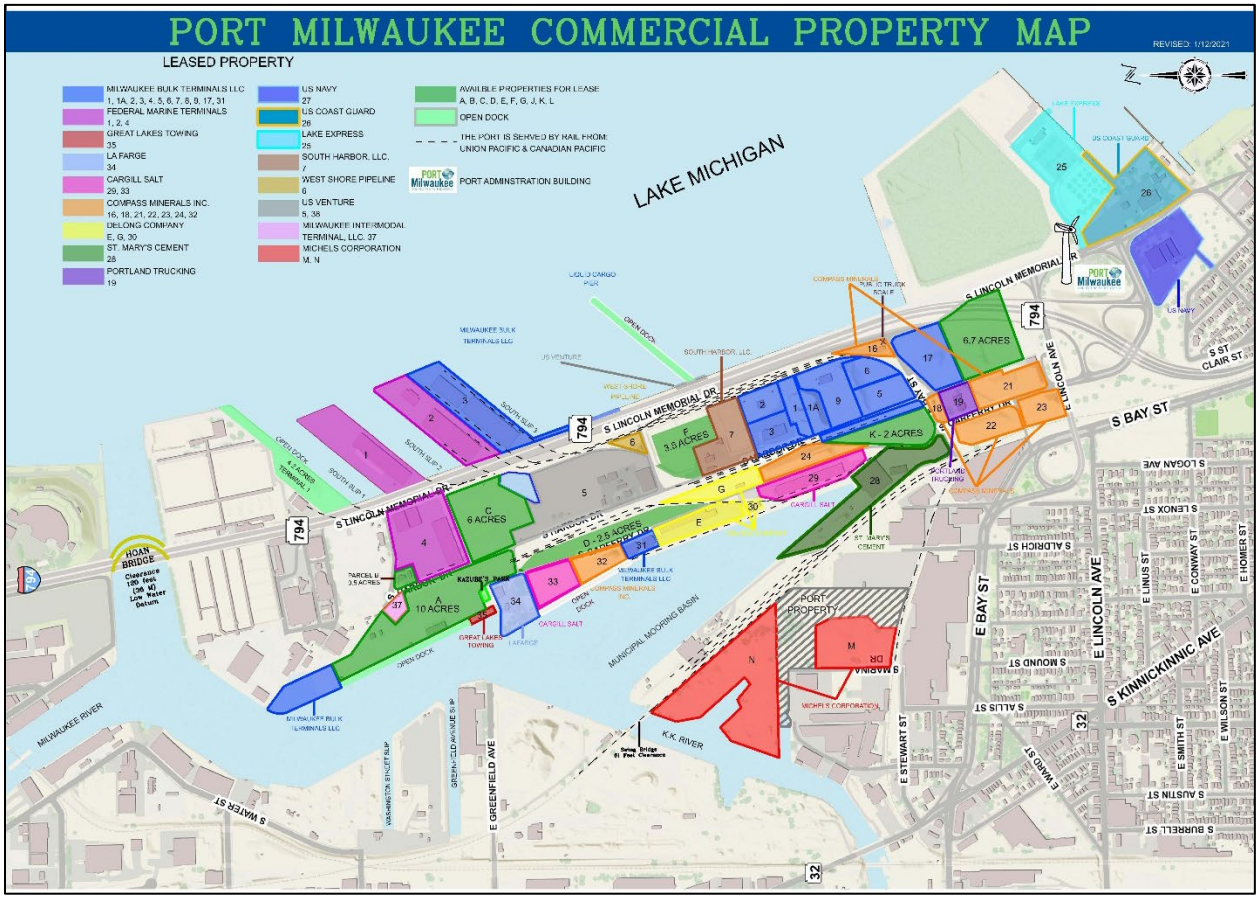

FIGURE 1.—Commercial Property Map - 31 JAN 21.

Facility Function/Purpose

Port of Milwaukee facilitates maritime loading and transport of bulk goods, such as salt, cement, ash, limestone, slag, and fertilizer, as well as various agricultural products, large machinery and equipment, and liquid cargo, such as fuel and other petroleum products. The port also provides direct access to multimodal transportation nodes, such as rail, truck and barge transportation.

Key Products and Services

Port of Milwaukee provides maritime loading/offloading capabilities of goods and cargo as well as facilitates the use of, and direct access to, multimodal supply chain options, including rail and ground transportation. It also provides both open and covered storage space for staging of various bulk goods and materials.

Primary Customers/Users

Port of Milwaukee currently consists of more than 20 resident tenant businesses. However, a wide range of local/regional businesses use these tenants in order to operate through them to facilitate the maritime transport of goods and equipment to both domestic and global markets.

Significant Assets and Areas

A facility SAA is defined as:

- Something critical to operation or function of the facility,
- Something critical to the physical vulnerability of the facility,
- An aspect about the facility that may be important to intelligence or risk assessment analysis for this type of facility, or
- Something that is important in describing the character of the facility.

During the visit, Port of Milwaukee representatives and the PSA identified the following SAAs that are critical to the facility's operations:

- SAA 1 - Liquid Cargo Dock
- SAA 2 - Federal Marine Terminals
- SAA 3 - CHLD
- SAA 4 - Agricultural Maritime Export Facility / DeLong Terminal

Protective Measures Index

The PMI is a quantitative value using a 0-100 scale that is an aggregate measure of the following five operational dimensions of protection, as they relate to the security posture at this facility:

- **Physical Security** refers to measures and features that protect a facility and its buildings, perimeter, and occupants from intrusion. This component is influenced by the presence or absence of fences, gates, barriers, electronic surveillance, parking controls, illumination, and entry control procedures.
- **Security Management** refers to plans and procedures that a facility has in place to deal with security issues. This component is influenced by the presence or absence of a designated security manager, security plans and communications, procedures for handling suspicious packages and sensitive information, security working groups, and background checks.
- **Security Force** refers to a designated group of employees or contractors with security duties. This component is influenced by the presence or absence of staffing, equipment, training, post orders, and a command and control center.
- **Information Sharing** refers to the exchange of hazard and threat information with private industry and local, state, and federal agencies. This component is influenced by the presence or absence of threat sources, employees with a national security clearance, coordination of security plans with local law enforcement, participation in security working groups, and written memorandums of understanding (MOUs) and memorandums of agreement (MOAs) with agencies and personnel other than emergency responders.
- **Security Activity History/Background** refers to previous vulnerability assessments and new protective measures that a facility may have implemented to improve its security posture. This component is influenced by the presence or absence of prior vulnerability assessments, new and additional protective measures, threat levels in the security plan, and protective measures associated with each threat level.

The overall PMI for Port of Milwaukee of 43 is below the average of 53 when compared to 70 other assessed ports. Figure 2 shows the overall PMI summary for Port of Milwaukee. NOTE: This summary represents a snapshot of the comparison of the facility's current security posture to like facilities as of January 28, 2022. The Dashboards provide near real-time comparison data that are updated continuously as ISTs for like facilities are added to the nationwide comparison group.

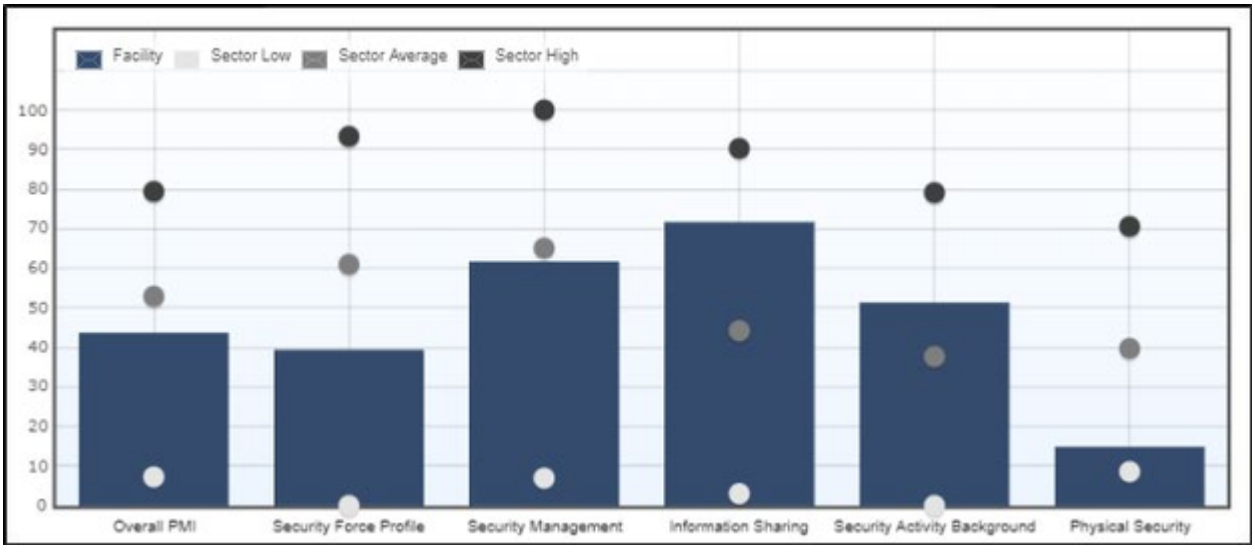

FIGURE 2.—Overall PMI Summary.

Resilience Measurement Index

The RMI is a quantitative value using a 0-100 scale that is an aggregate measure of the following four operational dimensions of resilience, as they relate to the resilience posture at this facility:

- **Preparedness** refers to activities that a facility has taken to define its hazard environment. This component is influenced by the presence or absence of external agencies with whom physical or cyber threat information is exchanged; business continuity, emergency, and cyber plans and designated managers; and additional training, exercises, and planning activities.
- **Mitigation Measures** refer to activities that a facility has taken prior to an event to reduce the severity or consequences of a hazard or incident. This component is influenced by the presence or absence of hazard-mitigating construction enhancements or infrastructure upgrades, alternate sites for continuity of business, and backup capabilities for SAAs and external utilities/services.
- **Response Capabilities** refer to immediate and ongoing activities, tasks, programs, and systems developed or undertaken to manage the adverse effect of an event. This component is influenced by the presence or absence of onsite response capabilities, new communications and incident response enhancements; contingency plans, MOUs/MOAs, and visits with offsite first responder agencies; contingency plans with external utility/service providers; and an incident management and command center.
- **Recovery Mechanisms** refer to activities and programs that a facility has in place to help return conditions to a level that is acceptable for operations. This component is influenced by the presence or absence of restoration agreements with external utility/service providers; written MOUs/MOAs with agencies and personnel other than emergency responders; SAA recovery time duration and resources; and external utility/service recovery times.

The overall RMI for Port of Milwaukee of 37 is above the average of 36 when compared to 65 other assessed ports. Figure 3 shows the overall RMI summary for Port of Milwaukee. NOTE: This summary represents a snapshot of the comparison of the facility's current resilience posture to like facilities as of January 28, 2022. The Dashboards provide near real-time comparison data that are updated continuously as ISTs for like facilities are added to the nationwide comparison group.

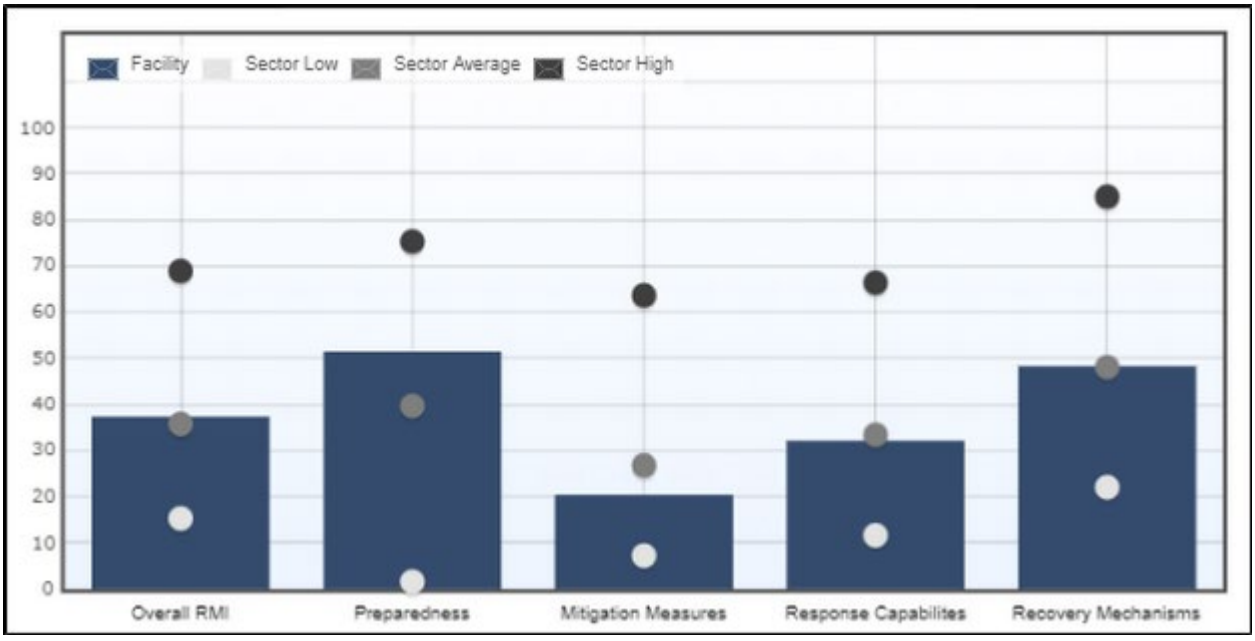

FIGURE 3.—Overall RMI Summary.

Facility and SAA Vulnerabilities and Options for Consideration (VOFCs)

The PSA identified potential vulnerabilities and suggested options for consideration the facility may consider to reduce them.

The IST process and options for consideration provide an opportunity for the facility to mitigate vulnerabilities, increase resilience, and implement protective measures. This process involves an assessment of risk tailored to the facility that takes into consideration the threat, assets to be protected, facility characteristics, and capital expenditures planning. The options for consideration are not prescriptive endorsements of specific protective measures to be installed and/or used at the facility. The critical infrastructure owner or operator determines for the facility whether the options for consideration provide the desired enhancements in light of the facility's current security and resilience posture, anticipated growth or organizational changes, budgetary outlook, etc.

The options for consideration provide actions that may help improve physical security, operational security, and resilience. Appendix D contains references for the options for consideration provided in this report.

Introduction

Port of Milwaukee is unique in that it encompasses portions of publicly owned and managed land that thus requires it remain open to the public for recreational use. This is unusual in the fact that most major maritime ports across the nation are fully secured and maintain restricted access to only those individuals conducting official maritime operations and have vetted/authorized access to port facilities. This security posture poses significant risk to not only the Port of Milwaukee's operations, but to the economic security of the greater Milwaukee Metropolitan Area as a whole

VOFCs

First Preventers/Responders

The facility does not have a written MOU/MOA with the primary law enforcement agency. Formal agreements with first responders expedite assistance and the provision of special services as necessary.

- Establish a liaison with the agency. Explore the option of creating a formal agreement for assistance and special services.[1]

The facility does not have interoperable communications with the primary law enforcement agency. Without interoperable communications, the facility cannot communicate with first responders in order to coordinate security and response activities.

- Collaborate with the agency on potential solutions to achieve cost-effective interoperable communications onsite.[2]

The primary fire response agency has not conducted an onsite visit of the facility. Onsite visits can familiarize first responders with the facility, key personnel, site layout, and other issues that would enhance incident response.

- Invite the agency to visit the facility. Provide a tour to familiarize first responders with the site layout.[3]
- Establish annual onsite visits for first responders to maintain their familiarity with the facility.[4]

The primary emergency medical response agency has not conducted an onsite visit of the facility. Onsite visits can familiarize first responders with the facility, key personnel, site layout, and other issues that would enhance incident response.

- Invite the agency to visit the facility. Provide a tour to familiarize first responders with the site layout.[5]
- Establish annual onsite visits for first responders to maintain their familiarity with the facility.[6]

Natural Hazards

The facility has no plans or procedures to implement long-term mitigation measures for flooding.

- Establish specific plans and procedures to protect the facility and its critical assets from flooding damage. Contact the state/local emergency management office and/or the regional Federal Emergency Management Agency (FEMA) office for available flood planning resources.

- Establish a flood response checklist that can be provided to employees ahead of a flood watch and/or warning.[7]
- Consult the Ready.gov Website, at http://www.ready.gov/floods, for more information.

Information Sharing

None of the facility's employees have U.S. government security clearance. Without clearances, facility personnel cannot review classified material related to pertinent threats.

- Consult your local PSA for more information about the DHS Private Sector Clearance Program, which sponsors security clearances for certain private-sector officials, including critical infrastructure owners/operators, sector leadership, and subject matter experts.

No port staff have access to the DHS Homeland Security Information Network (HSIN). HSIN is a valuable information sharing tool that critical infrastructure owners and operators can use for a myriad of uses and benefits. This resource can also be used to assist in collaborating with other critical infrastructure owners and operators via the HSIN Connect platform.

- At a minimum, designate a few key personnel to pursue getting access to HSIN. To learn more about HSIN, go to https://www.dhs.gov/homeland-security-information-network-hsin#; to join HSIN, go to https://www.dhs.gov/how-join-hsin; ensure when you request access to HSIN that you request access to the "Critical Infrastructure" Community Of Interest and cc your local DHS PSA on the access request.

Security Management Profile

The facility does not review the security plan annually with local law enforcement.

- Review the security plan annually with local law enforcement and other first responders as necessary, to ensure these agencies are familiar with the facility and its security plans, policies, and procedures.
- Consult *Developing and Maintaining Emergency Operations Plans*, available at http://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf, for more information.

The facility's security plan is missing key elements.

Update the security plan to include the following:

- Key control program
- Physical security inspection program
- A security awareness training program

The facility lacks procedures for handling suspicious packages.

- Incorporate procedures on how to handle suspicious packages into initial and annual security training programs.[8]
- Prominently display informational materials on suspicious package indicators in the mailroom.[9]
- Refer to the Ready.gov Website for information about suspicious packages and letters, at http://www.ready.gov/explosions.

While reviewing routing contract security logs, it was noted that unauthorized personnel commit often dozens of security incidents/incursions in any given week. While most of these are mundane trespassing incidents with no damage to property, it does illustrate that the wide-open nature of the port facility and limited security presence is widely known to personnel beyond just the port. This fact is concerning as a nefarious actor could use this to conduct criminal activity or exploited by someone attempting to target the port itself. See figures 4, 5, 6, and 7.

FIGURE 4.—Alternate View Looking North on Carferry Drive Showing Open Vehicle Access Gates.

FIGURE 5.—Memorial Drive Primary Entrance.

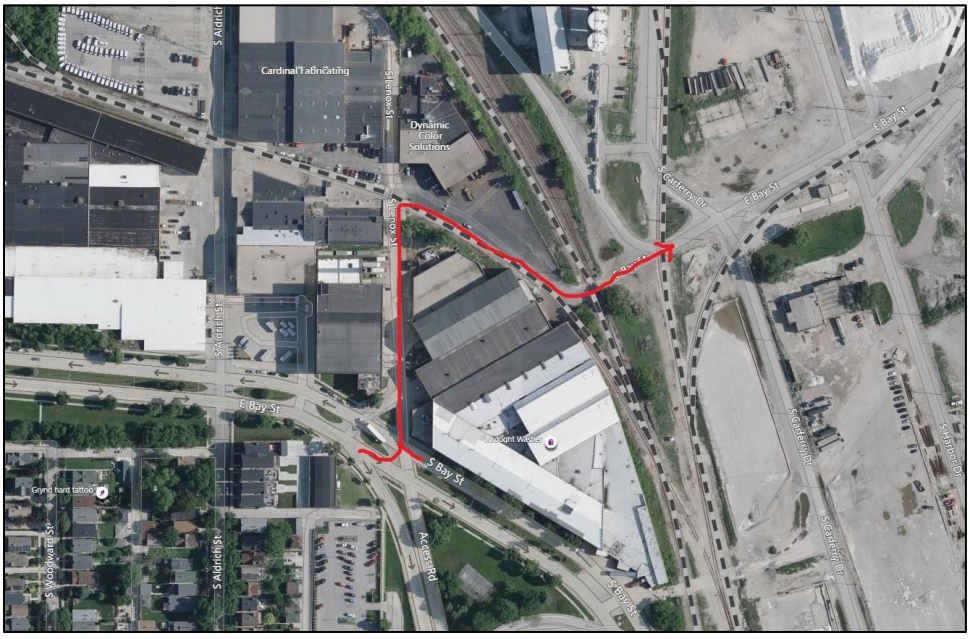

FIGURE 6.—Unrestricted Vehicular Pathway from Bay St to Lenox St.

FIGURE 7.—View Looking North on Carferry Drive Showing Open Vehicle Access Gates and Signage Stating to Use Alternate Route when Closed.

- Coordinate with Milwaukee Police Department (MPD) and Milwaukee County Sheriff's Office to explore whether they can conduct additional security patrols through the port area, especially at night and times when onsite port staff is limited.

- Coordinate with security contractor to request that Random Anti-Terrorism Measures be implemented to limit the ability of nefarious actors from identifying potential patterns for the security staff working at the port.
- Fully enclose the port within a perimeter fence and secure the port during non-operational hours.

Resilience Management Profile

The facility's business continuity plan identifies critical processes and assets necessary for core operations; however, the facility's impact evaluation for these processes and assets does not address some key impacts.

Update the impact evaluation, or, business impact analysis, to consider the following:

- Work backlog[10]
- Regional, national and international considerations (i.e., the analysis shall evaluate the potential effects of regional, national, or international incidents that could have cascading impacts)[11]
- Health and safety of persons in the affected area[12]

The facility's business continuity plan is missing key elements.

Update the business continuity plan to include the following:

- Alert and notification procedures for communications with employees[13]
- Identification of personnel with special skills, education, or training

The facility does not have a written emergency operation/emergency action plan.

- Develop a comprehensive emergency operation/emergency action plan specific to the facility. The emergency operation/action plan should assign responsibilities for carrying out specific actions to protect people (including those with special needs), property, operations, and the environment in an emergency, and to provide incident stabilization. Train personnel on the plan, and exercise the plan at least once a year. For more information, visit the Ready.gov Website at http://www.ready.gov/business/implementation/emergency, and consult *Developing and Maintaining Emergency Operations Plans*, available at http://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf.[14]

The facility does not have an incident management and command center (IMCC). Without an IMCC, the facility lacks a dedicated area to direct and oversee emergency management activities.

- Establish an IMCC dedicated to facilitating the coordination and support of emergency management activities.[15]
- Implement access control measures for the IMCC. Provide members of all teams who staff the IMCC with 24/7 access.[16]
- Ensure the IMCC has an uninterruptible power supply; essential computer, telecommunications, heating/ventilating/air-conditioning systems; and other support systems to continue operations for at least 72 hours. In addition, identify and store emergency supplies in the IMCC.[17]

Security Force Profile

The security force does not receive continuous/in-service training. Refresher training helps security force personnel maintain continued proficiency and current knowledge of security issues, trends, and technologies.

- Provide or contract refresher training for the security force, at least annually. Document refresher training and retain training records.[18]

The security force does not receive training on cardiopulmonary resuscitation (CPR) or First Aid.

- Ensure the security force receives training on CPR and First Aid.
- Review the training materials available from the Red Cross at http://www.redcross.org/take-a-class.

The facility does not have comprehensive post orders for the security force, which may result in situations where security personnel do not fulfill their duties and/or perform outside the scope of their duties.

- Develop post orders that describe in detail the duties and responsibilities of the security force. After comprehensive post orders are developed, ensure that they are kept current and accessible. Comprehensive post orders may serve to express the policies of the protected enterprise, summarize required officer duties, avoid problems associated with of word-of-mouth instructions, and provide a basis for site-specific training. They are the vital link between the requirements of the facility and the ability of security personnel to effectively meet those requirements.[19]

The security force does not have a dedicated command and control/operation center. Without a dedicated security center, the security force lacks a control point for coordination, monitoring and dispatch, and other critical activities.

- Establish a command and control post/operation center for the security force.[20]

The facility was uncertain whether all port personnel, and port tenant staff, have taken security awareness training. Given the current security posture of the port, it is imperative that everyone understand the importance of safety and security of the port and be provided the tools and resources to become effective contributors to the security of the port.

- Provide additional security awareness training to all port staff and tenant organizations, stressing the importance of ensuring the safety and security of the port.
- Use or share the following free training resources: CISA Office for Bombing Prevention Virtual Instructor-Led Training https://cdp.dhs.gov/obp; DHS See Something, Say Something Challenge Videos: https://www.dhs.gov/see-something-say-something/take-challenge; DHS National Suspicious Activity Reporting Initiative (NSI/SAR) Resources: https://www.dhs.gov/nationwide-sar-initiative-nsi/nsi-resources; DHS NSI/SAR online training: https://www.dhs.gov/nationwide-sar-initiative-nsi/online-sar-training.
- Explore the FEMA Emergency Management Institute Independent Study website for additional training opportunities and resources available at https://training.fema.gov/is/crslist.aspx.
- Connect with the U.S. Coast Guard (USCG) for additional training opportunities that may be available locally and through USCG Homeport, go to https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Port-and-Facility-Compliance-CG-FAC/Homeport-20/.

- Conduct outreach with MPD Southeastern Threat Analysis Center for additional training and collaboration opportunities related to NSI/SAR and other resources; visit https://www.milwaukee.gov/WiWATCH/stac.

Perimeter Security

Less than 100% of the facility is enclosed, and less than 100% of SAAs are enclosed. The lack of fencing may allow unrestricted access to critical areas of the facility.

- Design the fence line to maximize natural surveillance from the street to the facility and from the facility to the street, and minimize opportunities for intruders to hide.[21]
- Install fencing appropriate for the facility type. Determine the appropriate role of the fencing either to demarcate the boundary of the site to protect against trespassing; provide access control by channeling individuals through authorized access points.[22]
- Consult *Site and Urban Design for Security: Guidance against Potential Terrorist Attacks (FEMA 430)*, available at https://www.fema.gov/sites/default/files/2020-08/fema430.pdf, for more information.
- Consult *UFC 4-022-03, Security Fences and Gates*, available at https://www.wbdg.org/FFC/DOD/UFC/ufc_4_022_03_2013.pdf, for more information.[23]

The base of the fence at the facility is not anchored, which may allow access under the fence line.

- Anchor the base of the fence to protect against access by crawling under or raising lower portion of fence. The fence should also be installed to preclude access made possible by ground erosion.[24]

Objects and/or structures are adjacent to the fence that may aid traversing the fence.

- Remove all objects near the fence that would aid traversing it. Keep a clear zone free of any item that could aid an intruder in breeching or circumventing the perimeter fence.[25]
- Ensure security force roving patrols include surveillance of the perimeter fence and objects/structures that remain near the fence line.[26]

The fence is not clearly marked or identified with warning signs.

- Post visible, well-placed warning signs on the fence. Signs may act as a deterrent and/or provide safety information for unauthorized personnel. Signs are usually placed on boundary fences, typically at 50-foot intervals, to indicate ownership and to warn of possible danger within. In areas where two or more languages are commonly spoken, the warning signs must use both (or more) languages.[27]

Port of Milwaukee is not fully enclosed within a perimeter fence. Further, although the port is technically closed to visitors after normal duty hours, no way exists to fully secure and lock down the port after hours to prevent unauthorized personnel from accessing the property. (Vehicular access from S Bay St. to S Lenox St. cannot be secured at this time) This condition enhances the ability for nefarious actors to easily gain access to the facility during non-duty hours when port operations are typically limited and only minimal onsite security staffing is present. See figures 8, 9, 10, and 11.

FIGURE 8.—Alternate View Looking North on Carferry Drive Showing Open Vehicle Access Gates.

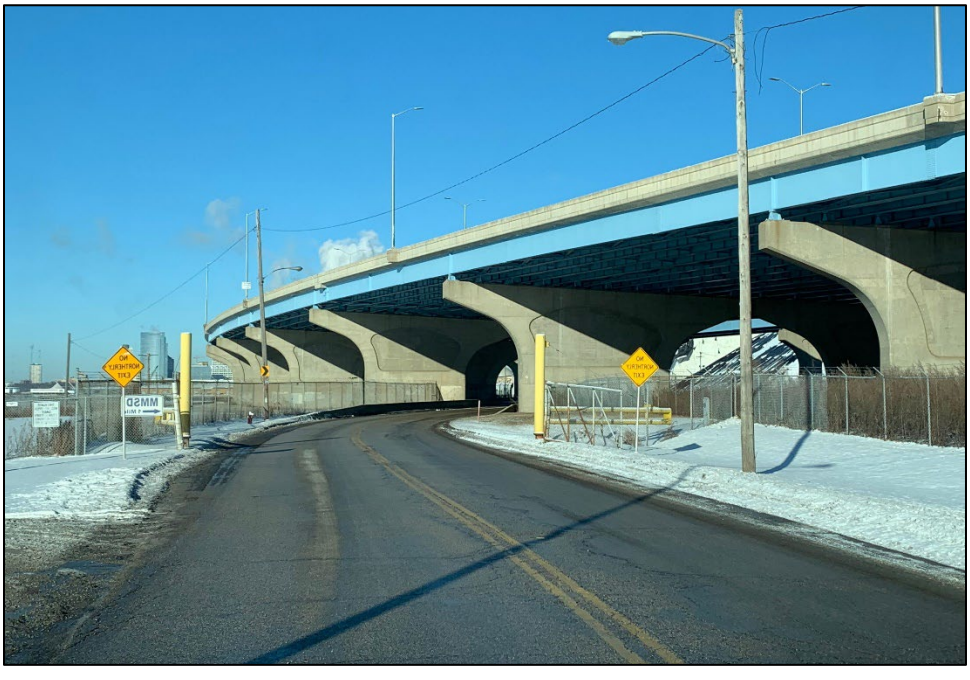

FIGURE 9.—Memorial Drive Primary Entrance.

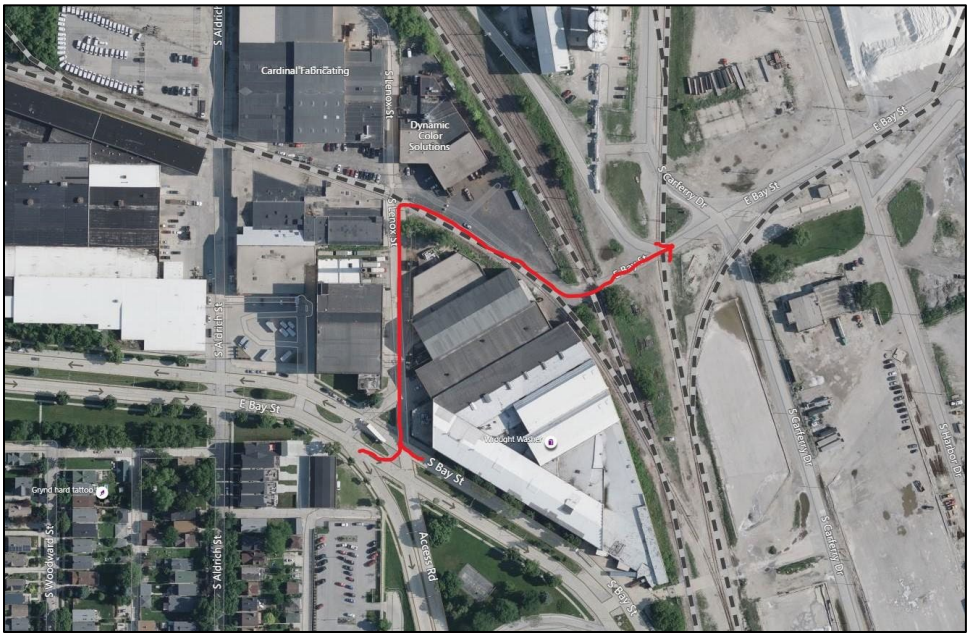

FIGURE 10.—Unrestricted Vehicular Pathway from Bay St to Lenox St.

FIGURE 11.—View Looking North on Carferry Drive Showing Open Vehicle Access Gates and Signage Stating to Use Alternate Route when Closed.

- Fully enclose the entire port facility within a secure perimeter fence. Ideally this fence line should have a well-maintained clear zone, proper signage, and be anchored/secured to minimize the potential for gaps due to soil erosion.
- Add outriggers with barbed wire for additional protection.
- Explore the feasibility of using USCG Port Security Grant Funding to assist with covering the cost of this (and other) security enhancements/upgrades. To find out more about the Port Security Grant Program, go to https://www.fema.gov/grants/preparedness/port-security or discuss with USCG Sector Lake Michigan grants team.

A number sections of the existing perimeter fence are in serious disrepair or have significant issues due to soil erosion. A number of sections of fencing beneath the I-794 bridge have holes cut in the fencing, unstable fence posts, and large gaps underneath the fence due to erosion. See figures 12 and 13.

FIGURE 12.—Example of Fencing in Poor Condition.

FIGURE 13.—Example of Perimeter Fence Compromise.

- Coordinate with a fencing contractor to conduct a full perimeter fence assessment to identify and address gaps and issues with the existing fence line as necessary.

The facility has no gates at openings in the fence line. The lack of gates provides individuals and vehicles with unrestricted access to the facility.

- Install gates, providing appropriate levels of access control and/or penetration delay against individuals, at identified gaps in perimeter fencing. Install barriers/systems at gates to provide vehicle access control and/or vehicle penetration delay, as appropriate.[28]
- Consult *UFC 4-022-03, Security Fences and Gates*, available at https://www.wbdg.org/FFC/DOD/UFC/ufc_4_022_03_2013.pdf, for more information.[29]

The railroad demarcation points on the southern end of Jones Island have no fencing/gates, are wide open, and cannot be secured. This prevents the port from being able to create a fully secure perimeter as any unauthorized individual could simply walk onto the property via the existing rail lines. See figure 14.

FIGURE 14.—View of Rail Spur Demarcation Points Looking South on Access Road Illustrating No Rail Gates.

- Explore the feasibility of installing rail gates at the point where these rail lines enter port property. Coordinate these rail gates with overall perimeter fence expansion as well. Ideally these gates would be automated and could be remotely operated from the Port Administration Building.

Entry Controls

Kaszube's Park is a public space that is located in the center of the Port of Milwaukee and therefore forces the port to remain wide open and left unsecured to enable residents of Milwaukee the ability to access this public land. In addition, other critical areas of the port property have been authorized for public use for picnicking, fishing and other activities. This creates an extreme vulnerability and exposes the Port of Milwaukee, and the greater Milwaukee economy, to unnecessary risk. While the history and importance of this public park is well understood, the risk it poses to this vital piece of maritime critical infrastructure and the greater regional economy cannot be understated. See figures 15 and 16.

FIGURE 15.—Kaszube's Park.

FIGURE 16.—Typical Signage Providing Access to Critical Areas beneath I-794 Bridge Structural Columns.

- Work with the City of Milwaukee to relocate the park to more accessible and less vulnerable location (e.g., in front of the Administrative Building). Historical items of interest from the park could be relocated to this area with a rededication ceremony to honor the historic significance of the village. This area would be outside of the port's perimeter fence (but within the building's fence line and could still be secured), could be well-monitored by both security staff and port administrative staff due to its open space, and would greatly reduce potential risk to port operations.
- Eliminate the ability for the general public to use any port property for recreational use (i.e., fishing, picnicking) due to liability and security concerns. Work with the city to re-write/adjust Milwaukee Code of Ordinances Section 118-66 pertaining to access of Jones Island so that it states that public access to the port and island is prohibited as no public lands will exist on the island once the park is relocated.
- If the port is unable to negotiate the movement of park, significant additional security protocols need to be put in place, such as a staffed and monitored primary access/entry control point that can provide security overview of all vehicles/personnel accessing the port property.
- Remove or relocate the park from the island; this would be the most secure course of action. If doing so is not achievable, use measures from Crime Prevention Through Environmental Design (CPTED). Specific measures follow the idea of territoriality and can be implemented by manipulating the environment to identify proper and improper uses of designated spaces.
- Use signs to communicate which areas are off limits and which areas may be used by patrons. This can be done by prohibiting anyone from exiting a vehicle in non-public areas.

- Create a parking lot and use fences or highly visible paint that designates areas public patrons must stay within. Use signs to reinforce this principle. Train all employees to know the designated areas, and empower employees to challenge patrons when they are outside of such areas.
- Use signs at the entrance to identify the rules, and use painted lines that show the path from the entrance area to the designated park area. Use signs, fencing and/or barriers along the path to reinforce proper use of spaces.
- Work with historical societies in the area, and use social media such as the Jones Island Milwaukee Kaszube Park Wisconsin Facebook page organizers and others to ask patrons to respect the port property and stay in designated areas when visiting.
- Ask local societies to post the rules on their websites and ensure those who may give tours understand and respect the rules.
- Host or support an annual event and ask patrons to respect the rules and participate in the protection of the site. Use this principle to create a sense of "ownership."

Parking / Delivery / Standoff

Vehicles can park within 400 feet of the facility. Access to the parking area is uncontrolled. The lack of rigorous vehicle access control procedures increases the vulnerability of the facility to a vehicle-borne attack.

- Explore options to implement vehicle access control procedures within 400 feet of the facility. Options to consider include vehicle screening and locked vehicle access points.[30]
- (1) Determine the facility's susceptibility to blast. Consult *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06)*, available at http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, for more information, especially Chapters 2 and 3: Chapter 2 discusses blast design concerns and protective measures for areas surrounding buildings. Chapter 3 discusses the nature of explosive blasts, their effects on buildings and occupants, and the concept of levels of protection. In addition, review the DHS Bomb Threat Stand-off Chart, available through the Lessons Learned Information Sharing national, online network, at https://www.hsdl.org/?abstract&did=4506. (2) Based on the facility's potential vulnerabilities, explore the feasibility of conducting a preliminary blast analysis using simple, commercially available building modeling and software designed to support the ability to address blast mitigation and potential vehicle-borne improvised explosive device threats, such as A.T.-BLAST by ARA Applied Research Associates. (3) Based on the results from the preliminary blast analysis, explore the feasibility of consulting with an engineering firm that specializes in structural fragility to procure a professional blast assessment to inform capital investments intended to protect personnel and the facility against blast.[31]

Parking in the uncontrolled parking area is not monitored in any way.

- Explore the feasibility of providing 24/7 CCTV monitoring for the parking area. Although CCTV coverage may need to be limited in its scope, it can still provide satisfactory coverage.[32]
- Install cameras in areas such as the main entrance, at all vehicle access control points, guard booths, cashier booths, and elevator lobbies on every floor. This will ensure more than adequate security.[33]
- Ensure lighting adequately illuminates activity in the parking area for viewing and videotaping.[34]

- Ensure that the parking area is covered by roving patrols conducted by the security force. Routes and times for patrols should also be varied at frequent intervals to preclude establishing a routine that may be observed by potential intruders.[35]
- Provide suspicious activity awareness training to facility employees, including topics related to uncontrolled parking areas. Provide options (e.g., hotline, direct phone or radio communications with security operations) for employees to report suspicious activity, potential threats, and incidents.

The facility has no procedures or policies to identify and act on unauthorized vehicles parked in the uncontrolled parking area for an extended period.

- Implement standard operating procedures to address unauthorized, suspicious, and extended-stay vehicles. Processes to consider include reporting vehicles to security and/or local law enforcement, and contracting with an area towing company for vehicle removal.[36]
- Train security personnel on the standard operating procedures to address unauthorized, suspicious, and extended-stay vehicles.[37]
- Ensure that the parking area is covered by roving patrols conducted by the security force to ensure early identification of unauthorized parked vehicles.[38]

During the visit, a number of vehicles, bulk chemical storage drums, and other equipment and materials were being stored directly beneath the I-794 bridge and directly adjacent to many critical support columns. Also, the access gates to these areas were unsecured, open, and unmanned during daytime hours. Allowing third-party contractors to store and stage equipment and materials in this area poses a significant vulnerability to the port and to critical transportation infrastructure supporting the port and the Greater Milwaukee Metro Area. See figures 17, 18, 19, and 20.

FIGURE 17.—Example of Bulk Liquid Chemicals Stored under I-794 Bridge.

FIGURE 18.—Example of Large Vehicles Parked under I-794 + Hoan Bridge.

FIGURE 19.—Example of Non-port Equipment Being Stored underneath I-794 Bridge.

FIGURE 20.—View of Random Bulk Chemicals Staged adjacent I-794 Support Columns.

- Remove all third-party equipment and materials from beneath the I-794 bridge being staged for long-term storage in this area. Minimize or completely eliminate the storage of any equipment and materials in this area.
- If storage of equipment in this area is absolutely necessary, establish additional security protocols to minimize potential risk, such as searching or screening all equipment and material before staging; prevent any equipment and material from being directly staged adjacent to critical I-794 support columns; providing additional security sweeps/patrols in this area; and adding CCTV camera coverage in these areas.

Barriers

The facility does not use barriers to mitigate high-speed avenues of approach. Barriers would reduce vehicle speeds and/or prevent vehicle penetration.

- Evaluate vehicle traffic patterns near the facility. Design and implement strategies to reduce vehicle speeds, improve pedestrian safety, and reduce the threat of vehicle approach velocities.[39]
- Install barriers to mitigate high-speed avenues of approach, deny vehicle entry, and provide perimeter protection. Options include, but are not limited to, fixed and retractable bollards, engineered planters, heavy objects and trees, walls and ha-ha barriers, water obstacles, and Jersey barriers.[40]
- Install fixed bollards, engineered planters, and/or heavy objects to mitigate high-speed avenues of approach.[41]
- Install heavy objects that can resist vehicle penetration, such as boulders, sculptures, and trees. Such objects need varying degrees of embedment and reinforcement, depending on their weight, footprint, and height/width ratio.[42]
- Explore the possibility of adding speed controls (e.g., serpentines or speed bumps) to limit vehicle speed at impact.[43]
- Explore the possibility of using CPTED principles, concepts, and strategies (e.g., water barriers, landscaping) to install barriers. Consult Appendix A of *Site and Urban Design for Security: Guidance against Potential Terrorist Attacks (FEMA 430)*, available at https://www.fema.gov/sites/default/files/2020-08/fema430.pdf, and Tables 2.4 and 2.5 of *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06)*, available at http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, for more information.[44]
- Use vehicles as temporary physical barriers to eliminate straight-line vehicular access to the facility during elevated threat conditions.[45]

The facility does not use barriers to enforce an effective standoff distance (i.e., the distance between the facility and the potential location for an explosive detonation).

- Install barriers to increase standoff distance and reduce damage from a potential explosive device. Options include, but are not limited to, fixed and retractable bollards, engineered planters, heavy objects and trees, walls and ha-ha barriers, water obstacles, and Jersey barriers.[46]
- Explore alternatives if it is not possible to create sufficient standoff distance through the use of barriers. Options may include hardening the building and minimizing hazardous flying debris during an explosive event (e.g., window protective measures such as anti-shatter film, bullet-resistant glass, and laminated glass).[47]

- Use vehicles as temporary physical barriers to increase standoff distance during elevated threat conditions.[48]

Electronic Security Systems

Port of Milwaukee has no CCTV camera coverage. This significantly degrades both port staff as well as security personnel from effectively monitoring potential nefarious activity that may occur onsite.

- Coordinate with a vetted security camera installation contractor to conduct an initial needs assessment. Conduct a lighting assessment concurrently to ensure maximum effectiveness of CCTV system during lowlight/nighttime hours.
- Explore funding options, to include UCSG Port Security Grant Funding, to assist in covering some or all of the cost of implementing a CCTV camera system to cover critical port areas.

Illumination

Lighting for fences, gates, and/or parking areas is uneven and dissimilar, causing glare and shadows, and resulting in inconsistent coverage, which can produce dark areas and shadows where intruders can go undetected.

- Update the lighting system to ensure illumination uniformity, so that security personnel can see ahead and to the sides with an absence of dark areas caused by shadows. Lighting should be brightest in secure areas, with the light gradually less in areas adjacent to high-illumination areas.[49]

Dependencies (Electric Power)

The facility does not have a contingency/business continuity plan with the electric power utility provider for rapid restoration in the event of a service disruption.

- Determine the electric power requirements to support facility core operations, and develop commensurate plans in collaboration with the utility provider to ensure service is restored with priority, or alternate service provisions are made. Ensure plans address legitimate hypothetical scenarios that would result in service loss and corresponding restoration timelines so the facility can address business continuity and interim workarounds.[50]

Facility and SAA Commendable Actions/Practices

As part of the onsite visit, the PSA noted several positive and commendable operations-related actions and security practices. Below are the commendable actions and practices that the PSA considers particularly noteworthy.

Security Management Profile

Despite limited security funding, Port of Milwaukee continues to seek creative ways to enhance the security and resilience of the port and its operations. It continues to actively establish relationships with key stakeholders and partners that can aid and assist them in establishing a more secure port.

Resilience Management Profile

Port of Milwaukee is fully committed to identifying, assessing, and mitigating all hazards risk to ensure continuity of business in any environment. This is clearly evident in the efforts the port has taken since post-flooding incident in January 2020.

Dependencies (Electric Power)

The port of Milwaukee has enhanced its energy resiliency by establishing a secondary, renewable power source via a 100-kilowatt (kW) wind turbine. This wind turbine provides more than 100% of the electric power needed to operate the Administration Building. Since it's installation, it has generated more than 1 million kW of electric power for the site, and surplus power has been provided back to the grid. The Administration Building is the first in the city of Milwaukee that is a "net zero" electric power user."

Conclusion

This report provides a summary of key findings of the IST at your facility and may be used as a guide for the consideration and implementation of future security and resilience enhancement measures. The report integrates with the Dashboards that visually depict the facility's security and resilience posture as compared to like facilities nationwide and can be used as a benefit-analysis tool during consideration of potential security and resilience changes.

The Dashboards are accessible through the Infrastructure Survey Dashboard application via the IP Gateway at https://gateway.cisa.gov/dashboard. The required username and password are provided in separate emails.

Please contact your PSA, John Busch, or DHS with any inquiries about the information contained in this report:

- John Busch, DHS PSA
  Email: John.Busch@hq.dhs.gov
  Phone: 414-369-8540

- DHS CISA, Infrastructure Security Division
  Email: IPassessments@dhs.gov

For technical support related to the Dashboards, please contact:

- Dashboard Comments
  Email: CISA-gatewayhelpdesk@cisa.dhs.gov

Appendix A: Commonly Used Acronyms and Abbreviations

AED	Automated External Defibrillator
ATAC	Anti-Terrorism Advisory Council
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BIA	Business Impact Analysis
BSI	British Standards Institution
CBR	Chemical, Biological, or Radiological
CCTV	Closed-circuit Television
CDC	Centers for Disease Control and Prevention
CHLD	City Heavy Lift Dock
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
COBIT	Control Objectives for Information and Related Technology
CoP	Community of Practice
CP	Canadian Pacific
CPR	Cardiopulmonary Resuscitation
CPTED	Crime Prevention Through Environmental Design
DHS	U.S. Department of Homeland Security
DOS	Denial of Service
EMA	Emergency Management Agency
EOC	Emergency Operations Center
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
FPS	Federal Protective Service
FTZ	Foreign Trade Zone
HAZMAT	Hazardous Material
HSA	Homeland Security Advisor
HSIN	Homeland Security Information Network
HVAC	Heating, Ventilating, and Air-conditioning
I	Interstate
ICE	U.S. Immigration and Customs Enforcement
ICS	Incident Command System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team

ID	Identification
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Improvised Explosive Device
IMCC	Incident Management and Command Center
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IST	Infrastructure Survey Tool
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JTTF	Joint Terrorism Task Force
kW	Kilowatt
LAN	Local Area Network
MARSEC	Maritime Security
MMSD	Milwaukee Metropolitan Sewerage District
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPD	Milwaukee Police Department
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NSI/SAR	National Suspicious Activity Reporting Initiative
NTAS	National Terrorism Advisory System
OPSEC	Operations Security
OSHA	Occupational Safety and Health Administration
PHIN	Public Health Information Network
PMI	Protective Measures Index
PS-Prep™	Voluntary Private Sector Preparedness Program
PSA	Protective Security Advisor
RMI	Resilience Measurement Index
SAA	Significant Asset or Area
SOP	Standard Operating Procedure
SP	Special Publication
TSA	Transportation Security Administration
UP	Union Pacific

US-CERT	U.S. Computer Emergency Readiness Team
USCG	U.S. Coast Guard
USGS	U.S. Geological Survey
VA	U.S. Department of Veterans Affairs
VBIED	Vehicle-borne Improvised Explosive Device
VLAN	Virtual Local Area Network
VOFC	Vulnerability and Option for Consideration
VPN	Virtual Private Network

This page intentionally left blank.

Appendix B: Common Terms and Definitions

Alternate Site
A location away and independent from a facility with the capability, technology, resources, and equipment to continue operations in the event that the primary location is unusable.

Business Continuity Plan
A plan that would help a facility recover or maintain its activities after a disruption to normal business operations.

Consequence Assessment
Process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence.

Countermeasure
Action, measure, process, or device that reduces an identified risk. A countermeasure can reduce any component of risk-threat, vulnerability, or, consequence.

Dependency
A utility or a service, often external to a facility, whose loss would adversely affect its operations, function, or mission.

Deterrent
A measure that discourages an action or prevents an occurrence by instilling fear, doubt, or anxiety. A deterrent reduces threat by decreasing the likelihood of an attempted attack.

Emergency Action Plan
A plan that outlines the roles of employers and employees and the actions they should take during an incident or emergency.

Entry Control
Processes and technology in place that control a person's access into a facility or certain areas of the facility. Entry control takes into consideration the individual (employee, visitor, contractor/vendor, or customer/patron/public), and time (during operating hours or off-business hours).

Human Consequence
Effect of an incident, event, or occurrence that results in injury, illness, or loss of life.

Incident Management and Command Center
Any room or area specifically designated by the facility as the central location from which the facility would manage emergency operations. It is the place where decision makers and key facility emergency personnel or business continuity personnel can gather during an emergency.

Information Sharing
The act of exchanging hazard and threat information with other agencies. "Exchange" can mean "receive from," "provide to," or both.

Integrated Risk Management
Incorporation and coordination of strategy, capability, and governance to enable risk-informed decision making.

Interoperable Communication
The ability of emergency responders to work seamlessly with other systems or products without any special effort, including capability communications equipment and bandwidth.

Mitigation
The capabilities necessary to reduce loss of life and property by lessening the impact of disasters.

Protective Measures
Procedures, policies, equipment, or personnel that help protect a facility.

Resilience
The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies. Elements of resilience include preparedness, mitigation, response, and recovery.

Response
Capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.

Risk
Potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence.

Risk Management
Process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost. The primary goal of risk management is to reduce or eliminate risk through mitigation measures (avoiding the risk or reducing the negative effect of the risk); however, risk management also includes the concepts of acceptance and/or transfer of responsibility for the risk as appropriate. Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to reduce risk.

Risk Mitigation
Application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences. Measures may be implemented prior to, during, or after an incident, event, or occurrence.

Risk Profile
Description and/or depiction of risks to an asset, system, network, geographic area, or other entity. A risk profile can be derived from a risk assessment; it is often used as a presentation tool to show how risks vary across comparable entities.

Security Force
A security force is a special group of employees or contractors with security duties. Security force does not include general employees who are trained in security awareness to observe and report in addition to their regular duties.

Security Plan

A plan that contains procedures for dealing with security issues such as active shooters, hostage taking, and terrorism.

Significant Asset or Area

Something critical to the operation/function of the facility; something critical to the physical vulnerability of the facility; an aspect about the facility that may be important to intelligence or risk assessment analysis for this type of facility; or something that is important in describing the character of the facility.

Standoff Distance

A measure that enforces a distance between a vehicle and a facility or building.

Vulnerability

Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

References:

DHS (U.S. Department of Homeland Security), Cybersecurity and Infrastructure Security Agency, 2013, *Infrastructure Survey Tool (IST) Version 4,* "Questions Set with Helps."

DHS, Cybersecurity and Infrastructure Security Agency, 2012, *Resilience Measurement Index Overview.*

DHS, 2011, *Presidential Policy Directive / PPD-8: National Preparedness*, March.

DHS, 2011, *National Preparedness Goal*, First edition, September.

DHS, 2011, *Infrastructure Survey Process User Guide*, "Module 4: Manage Visit Data," Version 1.0.

DHS, 2010, *DHS Risk Lexicon*, September.

This page intentionally left blank.

Appendix C: Images

The figures below illustrate points of interest or potential vulnerabilities identified at Port of Milwaukee during the August 11, 2021, onsite visit.

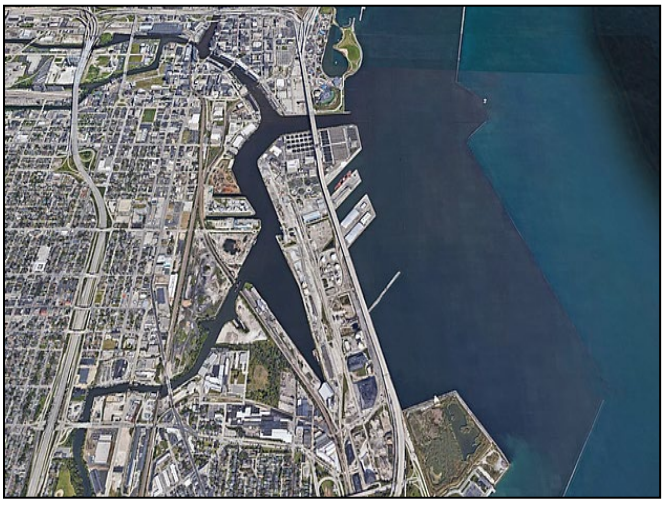

FIGURE C-1.—Port of MKE.

FIGURE C-2.—Alternate View Looking North on Carferry Drive Showing Open Vehicle Access Gates.

FIGURE C-3.—Alternate View of Rail Cars in Proximity of S Harbor Drive.

FIGURE C-4.—Example of Bulk Liquid Chemicals Stored under I-794 Bridge.

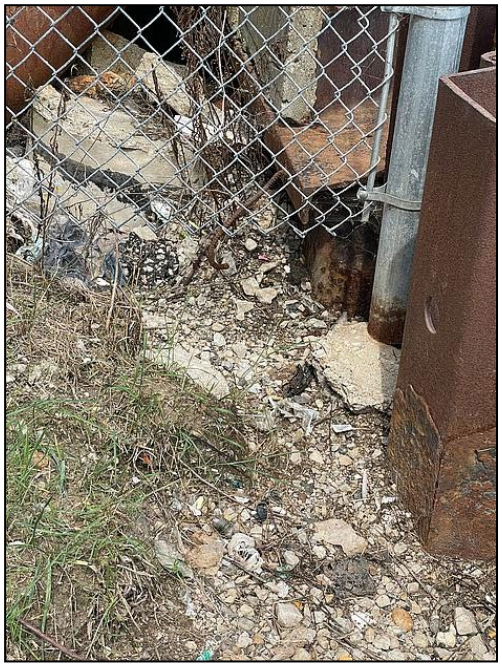

FIGURE C-5.—Example of Fencing in Poor Condition.

FIGURE C-6.—Example of Large Vehicles Parked under I-794 + Hoan Bridge.

FIGURE C-7.—Example of Non-port Equipment Being Stored underneath I-794 Bridge.

FIGURE C-8.—Example of Perimeter Fence Compromise.

FIGURE C-9.—Example of Salt Coverage Tarps Wrapped around Electrical Service Line.

FIGURE C-10.—Kaszube's Park.

FIGURE C-11.—Memorial Drive Primary Entrance.

FIGURE C-12.—Typical Signage Providing Access to Critical Areas beneath I-794 Bridge Structural Columns.

FIGURE C-13.—Unrestricted Vehicular Pathway from Bay St to Lenox St.

FIGURE C-14.—View Looking N on Carferry Drive Showing Open Vehicle Access Gates and Signage Stating to Use Alternate Route When Closed.

FIGURE C-15.—View Looking South on Carferry Drive at Port Facility Entrance.

FIGURE C-16.—View of Liquefied Petroleum Gas Rail Tankers Directly Adjacent to S Harbor Drive.

FIGURE C-17.—View of Conflicting Signage Stating no Public Access and Directions for Where Fisherman Should Access Facility.

FIGURE C-18.—View of Exposed I-794 Support Structures at Memorial Drive Entrance.

FIGURE C-19.—View of Rail Spur Demarcation Points Looking South on Access Road Illustrating no Rail Gates.

FIGURE C-20.—View of Random Bulk Chemicals Staged Adjacent I-794 Support Columns.

Appendix D: Options for Consideration References

[1] Walsh, T.J., and R.J. Healy, 2011, *Protection of Assets: Security Management*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 285-286.

[2] Walsh, T.J., and R.J. Healy, 2011, *Protection of Assets: Security Management*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 285-286.

[3] Walsh, T.J., and R.J. Healy, 2011, *Protection of Assets: Security Management*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 285-286.

[4] Walsh, T.J., and R.J. Healy, 2011, *Protection of Assets: Security Management*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 285-286.

[5] Walsh, T.J., and R.J. Healy, 2011, *Protection of Assets: Security Management*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 285-286.

[6] Walsh, T.J., and R.J. Healy, 2011, *Protection of Assets: Security Management*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 285-286.

[7] Nadel, B.A., 2004, *Building Security: Handbook for Architectural Planning and Design*, New York, NY: McGraw-Hill, ch. 12, p. 9.

[8] Walsh, T.J., and R.J. Healy, 2011, *Protection of Assets: Security Management*, M. Knoke, Ed., Alexandria, VA: ASIS International.

[9] Walsh, T.J., and R.J. Healy, 2011, *Protection of Assets: Security Management*, M. Knoke, Ed., Alexandria, VA: ASIS International.

[10] NPFA, 2013, *Standard on Disaster/Emergency Management and Business Continuity Programs (NPFA 1600)*, section A.5.3, p. 1600-16, http://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf, accessed June 17, 2014.

[11] NPFA, 2013, *Standard on Disaster/Emergency Management and Business Continuity Programs (NPFA 1600)*, section 5.2.4, p. 1600-7, http://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf, accessed June 17, 2014.

[12] BSI, 2006, *Business Continuity Management – Part 1: Code of Practice (BS 25999-1:2006)*, section 6.2.3, p. 17.

[13] BSI, 2006, *Business Continuity Management – Part 1: Code of Practice (BS 25999-1:2006)*, section 8.5.4, p. 30; ISO, 2012, *Societal Security – Business Continuity Management Systems – Requirements (ISO 22301)*, section 7.4, p. 13, section 8.4.4, p. 18.

[14] NPFA, 2013, *Standard on Disaster/Emergency Management and Business Continuity Programs (NPFA 1600)*, section 6.8, p. 1600-9, http://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf, accessed June 17, 2014.

[15] ASIS International, 2009, *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use (ASIS SPC.1-2009)*, section A.4.7, p. 33, http://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf, accessed June 16, 2014; NPFA, 2013, *Standard on Disaster/Emergency Management and Business Continuity Programs (NPFA 1600)*, section 6.7.1.1, p. 1600-9, http://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf, accessed June 17, 2014; Walsh, T.J., and R.J. Healy, 2011, *Protection of Assets: Crisis Management*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 20.

[16] ASIS International, 2009, *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use (ASIS SPC.1-2009)*, section A.4.7, p. 33, http://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf, accessed June 16, 2014.

[17] ASIS International, 2009, *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use (ASIS SPC.1-2009)*, section A.4.7, p. 33, http://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf, accessed June 16, 2014.

[18] Walsh, T.J., and R.J. Healy, 2011, *Protection of Assets: Security Officer Operations*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 92-93.

[19] Department of the Army, 2010, *ATTP 3-39.32 (FM 3-19.30) – Physical Security*, p. 3-8, http://fas.org/irp/doddir/army/attp3-39-32.pdf, accessed June 19, 2014.

[20] Department of the Army, 2010, *ATTP 3-39.32 (FM 3-19.30) – Physical Security*, p. 6-14, http://fas.org/irp/doddir/army/attp3-39-32.pdf, accessed June 19, 2014.

[21] Fischer, R.J., E.P. Halibozek, and D.C. Walters, 2013, *Introduction to Security*, 9th Edition, Waltham, MA: Elsevier Inc., p. 229-239; Walsh, T.J., and R.J. Healy, 2012, *Protection of Assets: Physical Security*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 39.

[22] DOD, 2013, *Unified Facilities Criteria (UFC) - Security Fences and Gates (UFC 4-022-03)*, section 2-12, p. 26-28, October, http://www.wbdg.org/ccb/DOD/UFC/ufc_4_022_03.pdf, accessed July 10, 2014.

[23] DOD, 2013, *Unified Facilities Criteria (UFC) - Security Fences and Gates (UFC 4-022-03)*, section 2-2, p. 15, October, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_022_03_2013.pdf, accessed April 3, 2018.

[24] Fennelly, L., 2013, *Effective Physical Security*,_4th Edition, Waltham, MA: Elsevier Inc., p. 271, p. 275.

[25] Fennelly, L., 2013, *Effective Physical Security*, 4th Edition, Waltham, MA: Elsevier Inc., p. 272.

[26] Department of the Army, 2010, *ATTP 3-39.32 (FM 3-19.30) – Physical Security*, p. 9-5, http://www.fas.org/irp/doddir/army/attp3-39-32.pdf, accessed June 19, 2014.

[27] FEMA, 2011, *Risk Management Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS 06)*, section 2.4.4, p. 2-70, October, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed June 17, 2014.

[28] Fennelly, L., 2013, *Effective Physical Security*, 4th Edition, Waltham, MA: Elsevier Inc., p. 112-113, p. 270; Walsh, T.J., and R.J. Healy, 2012, *Protection of Assets: Physical Security*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 47, p. 180, p. 263-265.

[29] DOD, 2013, *Unified Facilities Criteria (UFC) - Security Fences and Gates (UFC 4-022-03)*, section 2-2, p. 15, October, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_022_03_2013.pdf, accessed April 3, 2018.

[30] New York Police Department, 2009, *Engineering Security: Protective Design for High Risk Buildings*, ch. 5, http://www.nyc.gov/html/nypd/downloads/pdf/counterterrorism/nypd_engineeringsecurity_low_res.pdf, accessed May 20, 2014.

[31] FEMA, 2007, *Risk Management Series – Site and Urban Design for Security (FEMA 430)*, section 5.8, p. 5-24, December, http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed June 26, 2014.

[32] FEMA, 2007, *Risk Management Series – Site and Urban Design for Security (FEMA 430)*, section 5.8, p. 5-23 to 5-25, December, http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed June 26, 2014; Fischer, R.J., E.P. Halibozek, and D.C. Walters, 2013, *Introduction to Security*, 9th Edition, Waltham, MA: Elsevier Inc., p. 206; Walsh, T.J., and R.J. Healy, 2012, *Protection of Assets: Physical Security*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 166.

[33] FEMA, 2007, *Risk Management Series – Site and Urban Design for Security (FEMA 430)*, section 5.8, p. 5-23 to 5-25, December, http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed June 26, 2014; Fischer, R.J., E.P. Halibozek, and D.C. Walters, 2013, *Introduction to Security*, 9th Edition, Waltham, MA: Elsevier Inc., p. 206; Walsh, T.J., and R.J. Healy, 2012, *Protection of Assets: Physical Security*, M. Knoke, Ed., Alexandria, VA: ASIS International, p. 141-142.

[34] FEMA, 2007, *Risk Management Series – Site and Urban Design for Security (FEMA 430)*, section 5.8, p. 5-25, December, http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed June 26, 2014.

[35] Department of the Army, 2010, *ATTP 3-39.32 (FM 3-19.30) – Physical Security*, p. 9-5, http://www.fas.org/irp/doddir/army/attp3-39-32.pdf, accessed June 19, 2014; FEMA, 2007, *Risk Management Series – Site and Urban Design for Security (FEMA 430)*, Appendix A, p. A-2 to A-3, December, http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed June 26, 2014.

[36] FEMA, 2007, *Risk Management Series – Site and Urban Design for Security (FEMA 430)*, section 2.5, p. 2-30, section 3.3, p. 3-10 to 3-14, section 5.8, p. 5-23 to 5-25, December, http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed June 26, 2014.

[37] FEMA, 2007, *Risk Management Series – Site and Urban Design for Security (FEMA 430)*, section 2.5, p. 2-30, section 3.3, p. 3-10 to 3-14, section 5.8, p. 5-23 to 5-25, December, http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed June 26, 2014.

[38] Department of the Army, 2010, *ATTP 3-39.32 (FM 3-19.30) – Physical Security*, p. 9-5, http://www.fas.org/irp/doddir/army/attp3-39-32.pdf, accessed June 19, 2014; FEMA, 2007, *Risk Management Series – Site and Urban Design for Security (FEMA 430)*, Appendix A, p. A-2 to A-3, December, http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed June 26, 2014.

[39] FEMA, 2007, *Risk Management Series – Site and Urban Design for Security, Guidance Against Potential Terrorist Attacks (FEMA 430)*, section 3.5, p. 3-37, December, http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed May 20, 2014.

[40] FEMA, 2011, *Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06)*, section 2.3.4.4, p. 2-43 to 2-56, October, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed May 20, 2014.

[41] FEMA, 2011, *Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06)*, section 2.3.4.4, p. 2-43 to 2-56, October, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed May 20, 2014.

[42] FEMA, 2011, *Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06)*, section 2.3.4.4, p. 2-43 to 2-56, October, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed May 20, 2014.

[43] FEMA, 2007, *Risk Management Series – Site and Urban Design for Security, Guidance Against Potential Terrorist Attacks (FEMA 430),* Appendix A, p. A-5, December, http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pd, accessed May 20, 2014.

[44] FEMA, 2011, *Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06)*, section 2.3.4.4, p. 2-43 to 2-56, October, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed May 20, 2014; FEMA, 2007, *Risk Management Series – Site and Urban Design for Security, Guidance Against Potential Terrorist Attacks (FEMA 430)*, Appendix A, p. A-1 to A-6, December, http://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf, accessed May 20, 2014.

[45] FEMA, 2011, *Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06)*, section 1.8.3, p. 1-40, October, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed May 20, 2014.

[46] FEMA, 2011, *Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06)*, section 2.3.4.4, p. 2-43 to 2-56, October, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed May 20, 2014.

[47] FEMA, 2011, *Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06)*, section 3.3, p. 3-31 to 3-60, October, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed May 20, 2014.

[48] FEMA, 2011, *Buildings and Infrastructure Protection Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426/BIPS-06)*, section 1.8.3, p. 1-40, October, http://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf, accessed May 20, 2014.

[49] Department of the Army, 2010, *ATTP 3-39.32 (FM 3-19.30) – Physical Security*, p. 5-5, August, http://www.fas.org/irp/doddir/army/attp3-39-32.pdf, accessed June 13, 2014.

[50] FEMA, 2010, *Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide 101*, p. C-13 to C-14, November, http://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf, accessed June 17, 2014.