*2016 Year in Review*

# Houston Ship Channel Security District

# 2017 HSCSD Board of Directors

**Security Zone 1**

Brian Blanchard - Southwest Shipyard
*Treasurer*

Jarrod Boehme - ExxonMobil

**Security Zone 2**

Craig Nelson - Albemarle Corp.

Chris Bennett - Intercontinental Terminals Company

**Security Zone 3**

Gary Scheibe - Shell Deer Park
*Chairman*

Duane Campbell - Vopak Americas

**Security Zone 4**

Todd Adamec - The Lubrizol Corporation
*Secretary*

Eric Bass - Kuraray America, Inc.
*Assistant Secretary*

**Harris County**

Steve Stewart - Gulf Winds International

**Harris County Mayors and Councils Association**

Jimmy Burke

**Port of Houston Authority**

Marcus Woodring - Port of Houston Authority
*Vice Chairman*


**HSCSD Administration**

Al Cusick
713-671-0947
alcusick@hscsd.org

CAPT Bill Diehl, USCG (Ret.), P.E.
713-678-4300
bdiehl@txgulf.org

Houston Ship Channel Security District board meetings are held on the second Tuesday of each month at 2:00 PM at the Shell Deer Park Learning Center.

Shell Deer Park Learning Center
Mustang Building, 2nd Floor
4400 Highway 225
Deer Park, TX 77536

# From the Chairman's Desk

## The District's Year in Review

District Members, Partners, and Community:

2016 was a productive year for the Houston Ship Channel Security District. With our federal, state, regional, and local partners, we have made great progress and ensured that dedicated professionals have the tools necessary to keep our supply chain safe. You can read more about what all the agencies are doing as well as what we're helping our members with later in the publication, but on behalf of the Board of Directors, I want to talk a bit about why we're doing what we're doing.

It's been a hard year for most of us in the security business, law enforcement, or anybody with friends and family who serve their communities as protectors. There have been shootings, stabbings, civil unrest, demonstrations, and other challenges that have threatened our freedoms, but the men and women who stand at the tip of the spear are a big part of the reason we can enjoy the liberties that are so dear to all of us.

At the District, we all have a common goal: go home every night, safe, sound, and secure in the knowledge that our communities are as ready for what comes as possible. Because of that, we're focused on making sure that everybody working to protect us has the tools to do the job right. To our waterside law enforcement partners, we're looking to make sure you not only have the equipment, but the training and experience to keep the waterways in our District open. To our landside partners, we want you to have the situational awareness to be able to respond to an event, and the lines of communication to industry as well as the communities. Finally, we want to make sure that our Members have quality training that adds value to their work.

Training is something that's important to me, and something that our Board focuses on. Every one of us has sat in a class where we thought "well, I think I already know some of this", but speaking for myself, I know that every time I hear something at a refresher course or something that I think I'm pretty good at, I think about something in a new way. I want to encourage every one of our FSOs to attend one of our MTSA, CFATS or cyber trainings in the new year. We'll not only find new ways to think about the threats and challenges facing our facilities, but we'll be doing it together. I've found it's a lot better to meet your neighbor when you're talking about shared issues than when you're loaning him your hose in the middle of the night for a house fire.

District FSOs listen to Major William Skeen at the 2016 HSCSD Annual Luncheon, held November 8th at the Pasadena Convention Center

Representatives from the Harris County Sheriff's Office listen to the District Board at a Board of Directors Meeting

The District is a Partnership. We're successful because we have great partners. More than that, we have a single-minded direction. From our federal friends at the Coast Guard to each individual Facility Security Officer, we are here to protect the maritime system and everything it touches. That includes every facility in the District and the communities where we all live and work. We're constantly engaging to make sure we're being good stewards, and if you have any comments, questions, or concerns, contact me directly at gary.scheibe@shell.com or go to your zone representative. We represent you and look forward to a safe, productive 2017.

Sincerely,

Gary

# *Houston Ship Channel Security District Member Companies*

Air Liquide USA LP
Air Products and Chemicals, Inc
Akzo Nobel Polumar Chemistry
Albemarle Corp
All Trans Port Services, Inc
Altivia Specialty Chemicals
American Acryl
American Commercial Lines (ACL)
AMPAC Fine Chemicals
Ardent Mills, LLC
Arkema
Athlon Solutions
Baker Petrolite Corp.
BASF Corporation
Battleground Oil Specialty Terminal Company
Bayport Rail Terminal
Bealine Service Company, Inc.
Boasso America Corporation
Boone Towing, Inc.
Braskem America, Inc.
Brenner Tank Services LLC
Brenntag Southwest, Inc.
Buffalo Marine Service, Inc
Cargill, Inc.
CB&I
CBSL Transportation Services
Celanese Chemical
Cemex USA
Ceres Gulf Inc
Channel Biorefinery & Terminals, LLC
Channel Shipyard Co., Inc.
Chemquest Chemicals, LLC
Cheryl K Marine, LLC
Chevron Phillips Chemical Company
Chevron Products
Clean Harbors Environmental Services
Cletex Trucking, Inc
Clorox Products Manufacturing Company
Coastal Cargo-Texas, Inc
Colonial Pipeline
Contanda Terminals, LLC
Contanda Steel, LLC
Cooper/Ports America, LLC
Cronimet USA
Curtis Kelly
Delta Companies Group
Derichebourg Recycling USA, Inc.
Dianal America
Dixie Chemical Company, Inc.
Dow Chemical
DXI Industries, Inc.
E.I. Du Pont de Nemours & Co.
E.R. Carpenter, L.P.
Eco Services Operations LLC
Empire Stevedoring Inc
Enterprise Products
Eurecat US
Evonik Oil Additives USA Inc.
Excalibar Minerals, LLC
Exel, Inc.
ExxonMobil
Flint Hill Resources Houston Chemical, LLC
Foothills Texas, Inc.
G & H Towing Company
GB Biosciences (a Syngenta company)
General Electric Energy
GEO Specialty Chemicals, Inc.
Glendale Boat Works, Inc.
Global ICS
Goodyear Tire & Rubber Company - Houston Chemical
Greens Bayou Pipe Mill
Gulbrandsen Technologies, Inc.
Gulf Bayport Chemicals, L.P.
Gulf Winds International
Haldor Topsoe Inc.
Hansen-Mueller Company
Harley Marine Gulf
Hexion Inc.
Higman Marine Services
Holcim (US) Inc
Houston Ammonia Terminal, L.P.
Houston Cement Company, L.P.
Houston Fuel Oil Terminal Company
Houston Mooring Company
HOYER Global (USA), Inc
Huntsman International, LLC
Industrial Terminals, L.P.
INEOS Olefins and Polymers USA
Inert Gas Services, Inc.
Ingenia Polymers, Inc.
Intercontinental Terminals Company LLC
Intergulf Corp.
Invista
Jacintoport International LLC
Jacob Stern and Sons, Inc.

JX Nippon Chemical Texas, Inc.
Kaneka North America LLC
Katoen Natie
Kinder Morgan Gulf Bulk Region Terminals
Kinder Morgan Liquid Terminals
Kirby Inland Marine
K-Solv, LP
Kuraray America Inc.
LBC Houston
LCY Elastomers
Linde Gas North America LLC
Louis Dryfuss Corporation
Lubrizol Corporation
LyondellBasell
Magellan Midstream Partners, L.P.
Manchester Terminal, LLC
Marathon Pipeline
Martin Midstream Partners, L.P.
Mc Kenzie Tank Lines
McDonough Marine Service
Monument Chemical Baytown, LLC
Monument Chemical Houston, Ltd.
Mosaic Corp Nutrition LLC
Motiva Enterprises, LLC, Pasadena Terminal I
New Market
Newpark Drilling Fluids (Qualitex)
Nissan Chemical America
Noltex, LLC
Nova Molecular Technologies, Inc.
NRG Energy LLC
Nu Star Energy
O'Neal Steel, Inc
O'Rourke Petroleum
Odfjell Terminals
Oil States International
Old River Shipbuilding and Repair LTD
Oxy Vinyls, L.P.
Pasadena Refining System, Inc.
Patterson Tubular Services
PCI Nitrogen, L.L.C.
Pelican Asphalt Company, LLC
PeroxyChem, LLC
Phillips Texas Pipeline Company
Port Packaging
Powell Industries
Praxair, Inc.
Reagens USA, Inc.

Reagent Chemical and Research
Reichhold LLC 2
Richardson Companies
S.I Enterprises, L.L.C.
Sasol Chemicals (USA) LLC
Schneider Resources Inc
Sekisui Specialty Chemicals America
Shell Deer Park Complex
Shell Lubricants
Sneed Shipbuilding
Solar Turbines Incorporated - Turbo Fab Facility
Solvay Chemicals, Inc.
South Atlantic Services, Inc.
South Central Cement
South Coast Terminals, LP
Southern Ionics Inc.
Southwest Shipyard L.P.
Stolthaven Houston Inc.
Storage and Processors
Sun Edison
Sundbeck Inc.
Superior Carriers, Inc.
Targa Resources
Technip USA
Texas Mooring, Inc.
Texas Port Recycling, Inc.
Texas Terminals LP
Texmark Chemicals, Inc.
TM Chemicals Limited Partnership
TMC Engineering
TOTAL Petrochemicals USA, Inc.
TPC Group LLC
Trecora Chemical, Inc
T-Rex Engineering & Construction
United States Gypsum
Univar Environmental Sciences
USA Environment, LP
Valero Energy
Volkswagen Group of America
Vopak Terminals, North America
Vulcan Materials Company
W.R. Grace & Co.
Walton Barge Terminal
WATCO Companies
Web Fleeting LP
Womble Company, Inc
Zeon Chemicals L.P.
ZXP Technologies, LTD

# *From the District Administrator:* The Assessment & Appeals Process

Among the first tasks in the assessment process is to determine the amount of funds necessary for the coming year. Project requests are received from Harris County, City of Houston, and other municipalities for the funding of 1) the development of security projects, and 2) ongoing operating and maintenance (O&M) of the completed security projects. These projects are reviewed and presented in open session to the Board of Directors for action. If approved, budgets are prepared for each project and O&M along with District administration and operation budgets. An Assessment Plan is developed that will be able to provide the funds necessary to support the budget that is developed.

The Assessment Plan identifies the administrative costs; the security projects total cost, and the O&M cost to the District. It also puts forward the method for assessing the companies within the District. An effort is made to allocate the cost to the companies on the basis of benefit derived from the security projects. Headcount and/or acreage have been selected as matrixes that are obtainable and allow, in some measure, for this distribution of cost. A public Hearing on the Assessment Plan is then held to give everyone an opportunity to comment of the current year's assessments.

Each year in the Fall, the Billing for Assessment is sent to the member companies of the District. The assessments are payable by January 31 of the following year. Any assessment not paid by the January 31st deadline accrues penalty and interest in the same manner as ad valorem taxes. Unpaid assessments may result in a lien being placed on the property of the offending company.

If a company disagrees with the matrices that were used to arrive at their assessment they may appeal. The appeal must be in writing and must be received within 30-days of the adoption of the Assessment Plan. A company failing to file the appeal in a timely manner loses the right to appeal.

It has been the practice of the District to have all appeals first heard by a subcommittee. This allows the company to present their case in an informal setting. It also gives everyone an opportunity to be sure that all necessary documentation can be gathered prior to presenting the appeal to the Board for action. The subcommittee then presents their recommendations to approve or deny each appeal to the Board. Each company is given an opportunity to present their case before the Board if they so desire.

If an appeal is approved by the Board, a new assessment bill with a new due date is sent to the company. The new due date will be no earlier than 30-days from the date of the Boards decision. If the appeal is denied, the original assessment bill and due date remain in effect. Therefore, some companies have paid their assessment prior to the appeal decision in order to avoid the possibility of incurring penalties and interest.


## *District Training Opportunities in 2017*

Following positive feedback in 2016, the District has secured the Chemical Security Group to provide ten trainings in 2017 free of charge to District Members. Course dates can be found on the Districts website at www.hscsd.org and the District will send notification prior to each opportunity. The following course types will be held in 2017:

Maritime Transportation Security Act FSO Refresher Training
Chemical Facility Anti-Terrorism Standards Refresher Training
TWIC Class for MTSA Facilities Unregulated
TWIC Class for Non-MTSA Regulated Facilities
U.S. Coast Guard Approved Facility Security Officer (FSO) Certification Classes
Introduction to CFATs
Internet Profiling and Intelligence Gathering


**Above: Steve Roberts, of the Chemical Security Group discusses cybersecurity with District FSOs during a June 2016 training.**

For more information regarding District-supported training opportunities, please contact Al Cusick at alcusick@hscsd.org or call the administrative office at 713-671-0947.

# Bringing Tools to the Fight

With a mission to protect the supply chain running through the vast Harris County manufacturing and transportation base, the Houston Ship Channel Security District has sponsored a wide range of programs and initiatives in 2016.

The Houston Ship Channel Security District has played a vital role in supporting the Harris County Ship Channel Surveillance System since its inception in 2010. With a network of cameras and sensors covering waterside and landside facilities and critical infrastructure points, the System provides critical situational awareness to HSCSD partners such as the United States Coast Guard, the Harris County Sheriff's Office, and the Port Houston Police.

Not content to allow the five-year old system to simply weather the harsh conditions on the Houston Ship Channel and surrounding environs, the District has supported efforts by the Harris County Central Technology Services (CTS) to refresh the technology at over 40 camera, sensor, and communications nodes that comprise this state-of-the-art system.

In addition, the District has provided the City of Baytown, the City of Houston, and Harris County with funds to ensure that their law-enforcement air and marine units are spending valuable hours training, patrolling, and conducting joint operations. In addition, the colocation of assets at places like US Coast Guard Station Houston ensures that regional first-response units are familiar enough with each others' requirements and practices to ensure smooth operations during a response scenario.

**HCSO deputies work in conjunction with Coast Guard partners at the Sector Houston-Galveston Interagency Operations Center.**

**HSC Surveillance System cameras capture the M/V Aframax River aflame during a September incident on the channel.**


**A Houston Police Department Bell 412 helicopter conducts a fast-rope training exercise on a mobile platform adjacent to the Houston Ship Channel.**

# Cyber Security & Business Vitality

*What Every Houston-Area Business Leader Needs to Know, from the Greater Houston Partnership*

## Protecting Your Business: General Guidelines

Protecting any business should follow a logical, deliberate method. Begin with an honest assessment of the organization's current security posture. This assessment should include an inventory of all critical systems, services and processes, as well as business priorities. This assessment will result in the institution's current security profile.

Once a baseline security profile is created, the next step is to assess the risks that businesses face to understand the specific threats and potential impact of those threats. With this information the organization can determine which risks can be reasonably mitigated and how long it will take. The outcomes of the risk mitigation strategy can be called the target security profile, or the desired profile. Then, a business can create a deliberate implementation plan comprised of actions required to move from the current security profile to the target security profile.

This implementation plan can include the following steps:

### 1. Provide security awareness training

All employees should understand your organizational policies around security: why you have them, how you enforce them and the penalties for violations. Training should also include any federal and state regulations and industry specific requirements.

### 2. Encrypted data at rest and in motion

All sensitive data should be encrypted for transmission. This entails:

• Using secure socket layers (https or the padlock symbol on a web browser) or transport layer security with a password protected digital certificate either installed on both the sending and receiving side or over a virtual private network set up between two organizations.

• Encrypting data at rest by using built in tools to encrypt the entire hard drive (e.g. Bitlocker on Windows and FileVault on Mac).

• Password protect databases, and physically secure them behind a firewall, thus protecting them from the Internet while ensuring limited access based on business need.

### 3. Use firewalls

Firewalls block inbound internet traffic and protect your internal network from external access. Use a firewall to block all inbound ports and services except for the ones your hardened services need for inbound access.

### 4. Intrusion prevention services

Intrusion prevention services (internal/external) automatically detect external threats to your network and provide notification before they damage your business.

### 5. Web security-restriction/monitoring/reporting

Filter and restrict websites, services and content that can be accessed from your business. Use this to block your employees from accessing inappropriate content and sites that are known to present a security risk to your business.

### 6. Data loss prevention

Monitor and block the sending of unencrypted confidential information by e-mail or file upload. Data loss prevention software reviews your outbound content for words and patterns that should be sent securely and automatically sends them encrypted.

### 7. Lock down desktops

Only certain individuals in your organization should be able to download and install software. Computers should be kept patched and virus scanning software should always be current.

### 8. Use strong passwords and force changes every 60-90 days

Set the required standard to at least a minimum of eight characters including at least one upper case letter, lower case letter, numeric and special characters. Also, advise employees to never write down or share passwords.

### 9. Classify data

Perform an assessment and determine what data is public, private and protected. Insure that your policies and systems treat data types appropriately, using the highest protection for the most sensitive data.

### 10. Data separation based on content

Use two internet services or a virtual local area network and isolate the systems that you use for secure data from those that access other internet services, such as e-mail and web browsing. This helps protect your data by reducing its exposure to internet threats that are initiated internally, whether by accident or on purpose.

### 11. Restrict access

Limit access to need to know/need to do. Limit user roles to only access data and systems that are essential for performing their duties. Also be sure to change their access when their re-

sponsibilities change, especially in the case where they no longer need access to specific data.

### 12. Whitelist applications if possible

This is an approach to only allow software that is verified (malware free) to run on your computers. This is a good strategy to include with your lockdown strategy, which only allows certain individuals in your organization to download and install software.

### 13. Wireless networks

• Change your default SSID (Name of the wireless network). The default name tells someone the brand of router (and any associated vulnerabilities).

• Do not broadcast your SSID if possible.

This is an option on the wireless router. It requires someone trying to connect to your wireless network to know the name, as well as the password.

• Change your admin password immediately.

The admin passwords for routers are available on the internet, making it very easy for someone to connect directly to your wireless network.

• Create a "public" and "private" Wi-Fi network. You may want to offer wireless access to your customers or clients. Do this through a separate guest wireless router that is on a different virtual network that only has access to the internet and does not have access to your internal network. The same SSID and password requirements apply to this guest wireless network.

• Encryption should be turned on.

### 14. Mobile device management

Require your employees to use a pin to lock their mobile device, have device tracking, have encryption turned on and set

## The Five Core Functions of the NIST Framework: A Practical Guide

- **Identify**
  Identify information assets (data) and risks associated with these assets, including business' own data as well as data of clients and other third parties. Classify assets by sensitivity, criticality, value, shelf life, ownership, and custodial responsibilities. Assess risks to each asset in terms of likelihood, business impact, and loss expectancy.

- **Protect**
  Protect identified assets through implementing policies, standards, guidelines and controls to:
  - Authenticate, authorize, and audit asset access. All access should be recorded or logged
  - Only those with a need to know or need to do are identified and given only necessary permissions.
  - Promote information security awareness within the business.
  - Insure the confidentiality, integrity, and availability of data at rest and in motion.
  - Protect data from unauthorized disclosure by, when permissible, safely destroying obsolete data in all forms.
  - Implement incident recovery and business continuity plans to protect its interests and those of its clients.

- **Detect**
  Detect threats in real-time through implementing policies, processes, procedures, and controls to:
  - Recognize malicious activity in a timely manner.
  - Maintain continuous internal and independent vulnerability and penetration assessments.

- **Respond**
  Respond to incidents by implementing, testing, and maintaining a pro-active response plan that includes:
  - Defined response team roles and responsibilities.
  - A predefined notification list of stakeholders, first responders, service providers, and public relations/media.
  - Contingencies for communicating directly with clients and other external entities.
  - Isolate an incident, prevent expansion, and mitigate effects.
  - Perform incident post-mortems to review and improve processes.

- **Recover**
  Recover from an incident and return to normal operations by:
  - Predefining recovery time objectives, as well as the maximum tolerable time that data, services, and operations can be unavailable. These objectives prioritize recovery operations.
  - Predefining recovery point objectives, the maximum acceptable data loss as the result of an incident.
  - Recovery time and point objectives determine if the business's key systems (e-mail, internet, document management) will be recovered at existing data centers, service providers, or failover/alternate sites.

data boundaries.

### 15. Network monitoring tools

These tools are more for performance than security.

### 16. Vulnerability assessment

You should perform an internal assessment of your security risks and make sound business decisions based on risks, vulnerabilities and costs. Network routers and firewalls generate large amounts of log data that can provide the basic reports necessary for assessing vulnerability, including the number of connected devices, how much traffic those devices are generating, the amount of traffic traversing the border and what applications are sending the data as well. This data can be correlated and patterns can be established, showing what is normal for different times during the day. By creating this baseline, businesses can flag and investigate anomalies to mitigate cyber-attacks.

### 17. Security policy

Communicate the security policy to all personnel. Have detailed security policies that are reviewed and approved by your Board. Educate all employees on these policies (based on their role and access to data classification type). Review policy understanding at intervals and document training and reviews. Monitor adherence to policies and correct any violations appropriately.

### 18. Avoid free/public cloud storage and email accounts

These are not secure and should not be used for sensitive data.

### 19. Improve controls for payment systems

Cyber-threats often target your financial systems, particularly payments and wire transfers. Several best practices include implementing positive pay and wire transfer verification with your financial institutions, reconciling payments daily, and segregating accounts for different payment methods and types.

### 20. Understand your liability for financial losses

In some cases monetary losses from payment fraud are the responsibility of the financial institution as there are rules and regulations for banks to prevent fraud. However, some cases have resulted in the courts siding with financial institutions provided that reasonable controls exist and the customers had to absorb the loss, which can be severe and cause bankruptcy.

### 21. Guard Against Social Engineering

Networks and computer systems are not the only area of vulnerability in your company. Hackers often utilize social engineering – or psychological manipulation – to manipulate employees into providing confidential information that can be later used in cyber-attacks or other crimes against the company. Educate employees on social engineering tactics and insure that company policies include means for verifying identity.

## 2016 Annual Meeting

The 2016 Annual Meeting for the Houston Ship Channel Security District was held on November 8th with attendees from a wide representation of District facilities, as well as regional governmental officials and District partners.

At the meeting, each partner, listed below, gave a brief presentation on the District-Supported operations and initiatives that they have engaged in this year.

- City of Baytown
- City of Houston
- Harris County
- Harris County Sheriff's Office
- Texas Parks and Wildlife
- US Coast Guard Sector Houston-Galveston

In addition, the Texas Department of Public Safety gave a presentation on the State Fusion Center and a position being created to focus on the maritime domain and intelligence produced for companies who depend on Texas Waterways.

# CyberSecurity Assessment Tool

| NIST Priority | | Negligible | Low Risk | Moderate Risk | High Risk | Extreme Risk |
|---|---|---|---|---|---|---|
| Access Control | Do you have an organization password strength policy? | | Multi factor authentication | 8 characters or more, special characters required. Required change every 3 or 6 months | Less than 8 characters, no special characters | |
| Access Control | Do individuals or third party organizations have access to your network? | | Over a virtual private network, restricted access vendor accounts, business associates agreement with vendor | Remote access tools to access secure network from outside | Physical access to hardware | |
| Awareness & Training | Do you perform Security/Awareness training? | | Mandatory for all employees periodically with assessment of understanding. Third parties understand roles and responsibilities | For new hires only | None | |
| Data Security | Do you manage assets? | | Formally managed through acquisition, update, transfer, removal and disposal | Network, servers, devices and software documented | Purchased inventory only documented | No device or network management |
| Data Security | Do your employees travel with laptops or other removable devices? | No | Encrypted and no local data storage | Hard drive encryption | File encryption | Unencrypted; e.g. via email |
| Data Security | Do you have remote backup? | No | Zero recovery encrypted | Encrypted | Unencrypted | Physically unsecured |
| Data Security | Do you have wireless networks? | | No SSID, broadcast, complex password, air defense system. User account and/or computer address access control. No public access | Separate isolated guest wireless with no access to internal network | Published SSID, weak password | |
| Data Security | Do you store personally identifiable information on your network? | | No | Yes, encrypted at rest and in transmission | Yes, unenvrypted at rest and/or in transmission | |
| Processes & Procedures | Do you have organizational security policies? | | Board approved, trained, monitored and enforced | On shelf | No | |
| Processes & Procedures | Contracts with vendors | | Have copies of vendor security policies. Vendor has adequate cyber protection and insurance. Liability defined in contract | Liability defined in contract | No cybersecurity in contract | |

**Cybersecurity Tool Developed by the Greater Houston Partnership Cyber-Security Task Force**
**Photo Credit:** *www.bluecoat.com*

| NIST Priority | | Negligible | Low Risk | Moderate Risk | High Risk | Extreme Risk |
|---|---|---|---|---|---|---|
| Processes & Procedures | Do you perform personnel security and background checks | | All employees have background checks. Physical access control to physical network and servers. Accounts disabled as soon as employee is no longer hired | Background checks, but no physical access controls | No security or background checks | |
| Processes & Procedures | How do you transmit personally identifiable information to third parties? | | Using mutual transport layer security with a BAA in place | Over a virtual private network (VPN) | Via secure/encrypted email to unvalidated recipient | Unencrypted; e.g. via email |
| Processes & Procedures | Do you have a security function in your organization? | | Dedicated Security team. Reports to Senior leadership | Security functions shared within technical teams | No security function | |
| Processes & Procedures | Do you have an incident response team and plan and recovery plan? | | 24/7 response by multiple teams. | Business hours response by some teams. | None | |
| Maintenance | Do you perform logging and monitoring? | | Network and host base alerts responded in real time | Network only/Host only (no real time alerting) | None | |
| Protective Technology | Do you have anti virus and malware software? | | All computers and servers, monitored | Computers with access to PHI only, not monitored | No | |
| Protective Technology | Do you have Phishing protection? | | Monitored, no email/unrestricted internet browser access on network containing secure information | Yes, users trained | No | |
| Protective Technology | Do you protect your network with a firewall? | | Monitored | Commercial class router, complex password, ports open to the internet restricted to only those required for business applications | Residential class router, default password | No |

| Negligible: | _____ | Low: | _____ | Moderate: | _____ | High: | _____ | Extreme: | _____ |
|---|---|---|---|---|---|---|---|---|---|
| x0: | _____ | x1: | _____ | x2: | _____ | x3: | _____ | x4: | _____ |
| Subtotal: | _____ | Subtotal: | _____ | Subtotal: | _____ | Subtotal: | _____ | Subtotal: | _____ |
| Total Score: | | _____ | | <20: Good Measures in Place | | 20-40: Perform risk/benefit analysis of enhanced security | | <40: High risk. At minimum, invest in basic protection. | |

## About the Houston Ship Channel Security District

The Houston Ship Channel Security District (the "District") is a political subdivision of the State of Texas created by the Harris County Commissioners Court in 2009. The District is governed by an 11 member Board of Directors, 8 of whom are nominated and employed by private industry facilities located within the boundaries of the District. The other three Board members are appointed by (one each) and represent The Port of Houston Authority, Harris County, and the Harris County Mayors and Councils Association (representing the various municipalities located within the District).

The ultimate purpose of the District is to enable a greater degree of security and safety for facilities, employees and communities located within its boundaries. The District seeks to accomplish this function by supporting projects and initiatives to enhance the capabilities, communications, and joint operational readiness of existing first response, law enforcement, and regional organizations.

Houston Ship Channel Security District
111 East Loop North
Houston, TX 77029
www.hscsd.org
(t) 713-671-0947
(f) 713-678-4839