

# THE DIR CYBERSECURITY INSIGHT



October FY2017 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV



## Spooks, Spiders and Security Plans – Oh My!

October is a time for ghosts, ghouls and scary things. As we prepare for Halloween – buying candy, decorating the house and looking for costumes for our kids (or ourselves), security professionals in the state of Texas have another spooky task on their list: the agency security plan.

Under Senate Bill (SB) 1597 of the 83<sup>rd</sup> Legislature, each Texas state agency is required to submit a security plan to the Texas Department of Information Resources (DIR or Department) by October 15 of each even-numbered year. This means that the security plans are due THIS MONTH! The looming deadline can be enough to frighten even the steadiest ISO.

DIR is working to help make this deadline a little less scary. This year, agencies must submit their plans through the SPECTRIM portal, which allows inline editing, quick access to the controls and can provide reports on the progress of your security program. In addition, if you submitted a plan in 2014 using the Excel spreadsheet, that data has been imported into SPECTRIM allowing you to build on what has been done. SPECTRIM also provides the ability to export a copy of the data entered for offline review and/or agency approval. The detailed instructions for exporting your security plan can be found in the [July issue of Cybersecurity Insight](#).

There is online training available for the Security Plan module on the [DIR Information Security website](#). If you have any questions regarding security plan submission or using the SPECTRIM portal, please contact [GRC@dir.texas.gov](mailto:GRC@dir.texas.gov).

## CONTENTS

### Monthly Article

Spooks, Spiders and Security Plans  
P.1

### Program Updates

InfoSec Academy P.2  
NSOC Update P.2-3

### Interest Articles

Mobile protection P.3-4  
HHS Cybersecurity Fair P.4

### Our State ISO

### Spotlight

Frank Williams P.5

### Events

p.6

## Are You Aware of the Cybersecurity Awareness Events?

- **Threat Report Briefing by NTT Data**  
October 12, Austin, TX  
[REGISTER HERE](#)
- **Social Engineering by Denim Group**  
October 19, Austin, TX  
[REGISTER HERE](#)

# InfoSec Academy Update

---

The Texas InfoSec Academy is off to a great start! Approximately 75 people have already completed the Texas Security Policy & Assurance class, enabling them to enroll in certification prep and a variety of other courses.

**Upcoming instructor led Texas Security Policy & Assurance classes are scheduled from 8 a.m. to 4 p.m. on the following days:**

November 21, 2016

January TBD, 2017

This course, open to information security personnel of state agencies and higher education institutions, is provided so that they can become familiar with and can articulate their responsibilities under Texas Administrative Code (TAC) 202 and Texas Government Codes 2054 and 2059.

Upon completion students shall:

- Explain why agencies and higher education institutions have to comply with DIR rulemaking authority.
- Explain how new TAC 202 is structured.
- Understand and interpret the security control standards.
- Explain how Texas Government Code and TAC 202 work together.
- Describe the roles and responsibilities of agencies and higher education institutions under TAC 202.

Instruction will occur at the New Horizons Austin location at 300 E Highland Mall Blvd, Suite 100, Austin, TX 78752. An online anytime version of the Texas Security Policy and Assurance course is also available. If you would like to sign up for either of these classes, [VISIT THE INFOSEC ACADEMY website](#). If you have any questions about the InfoSec Academy send an email to [infosecacademy@dir.texas.gov](mailto:infosecacademy@dir.texas.gov).

# NSOC Update

---

The NSOC has been mandated to continually evaluate new technologies for viability of use not only for NSOC operations but also for applicability within the state and for DIR's customers. From August 2015—2016, DIR NSOC worked on a project to identify and evaluate Network Forensic Tools (NFT) to determine which, if any, would be successful in the NSOC environment and provide support to SOC operations.

The DIR NSOC acts as the internet service provider for its customers, meaning our main focus is to monitor network traffic to and from the internet. In order to enhance our ability and to minimize the time it takes to detect attacks, it is imperative that the NSOC has the most comprehensive view of the traffic that it inspects. NFTs allow the team the widest view for full packet capture and storage of metadata. Potential threats can then either be confirmed or denied more rapidly. This tool also gives the team the ability to conduct analysis on historical logs and connections when new threats are confirmed, which is a unique capability when compared to other NSOC tools.

Current NSOC systems create limited records of the events detected or prevented, they do not use that information to support any future activities and provide only the barest of context for the NSOC Security analyst. This results in the analyst spending time and effort trying to capture and correlate network data to assist in the understanding of the suspect activity.

NFTs are systems designed to capture or record, and analyze network traffic and events to identify security attacks or other suspicious activities. NFTs provide the ability to capture all network traffic and allow analysts to quickly query that data to

support any current investigation. Having the network data readily accessible speeds the triage process and allows our analysts to issue an alert or move on to the next item much faster. Additionally, NFT systems support the long-term storage of network data and metadata allowing analysts to look for patterns in the network traffic over long periods of time potentially identifying 'low and slow' attacks also known as Advanced Persistent Threats. Finally, many NFT systems provide their own ability to detect potential threats, utilizing the data they capture to identify attacks which are not detected by any other current security device.

The NSOC evaluated the NFT solution and confirmed it could provide visibility into events that our existing security stack had not previously identified. It also allows for better and faster correlation of events the existing security stack did identify. The greatest value we have seen in the evaluation of NFTs is their ability to support and enhance our daily operations. Having a tool that allows the NSOC analysts to more quickly triage a suspicious event and convert that into an actionable alert is critical. A tool that allows an analyst to gather additional data for context around a single event and determine that an alert needs to be issued is even more critical. In the end, NFTs provide greater context around events, help the NSOC to identify possible incidents more quickly and move the NSOC toward a more proactive state.

## Mobile Protection

---

As our dependence on mobile devices grows, so does the threat of cybercriminals targeting our devices. In 2014 alone, more than 1 billion records were breached and more than 5 million phones were reported lost or stolen. As of 2015, approximately 2/3 of the U.S. population owns a mobile smart device, 25 percent of which experience a threat each month.

Most of the communication that we do on these devices isn't verbal, but digital. We text, live-feed, tweet, check bank statements, watch videos, etc. In short, we live socially and professionally at the touch of a button or swipe of a bar. By doing so, we create a wealth of information stored – conveniently – in the palms of our hands.

Hackers and cybercriminals use a number of tools to acquire the information that resides in your device.

- **Scam Applications.** These apps mislead users into setting up payment for false services.
- **Madware.** These malicious applications act as advertising displays on popular mobile apps. Every time an app with in-app advertising is used, it generates an advertisement library registered to the cybercriminal which then filters advertising revenue directly to themselves.
- **Ransomware.** Some apps hold your data hostage until the owner pays a fee, or ransom.
- **Spamming.** Spam infects a device, and allow cybercriminals the opportunity to send massive amounts of spam with little chance of having their activities halted.
- **Intercepting Mobile Transactions.** For those that conduct online banking from their smart devices, users are generally provided an mTAN (mobile Transaction Authentication Number) as a means of verifying security credentials. These mTANs usually take the form of a one-time security code via text message sent directly to the customer. If a cybercriminal can intercept this type of information, they can circumvent the authentication process by using social engineering tactics and the one-time mTAN to gain access to bank account information.

To protect yourself and smart devices, there are some simple steps you can take.

- **Keep your device up-to-date.** Like any other computer; it occasionally needs updates. These updates are meant to patch bugs and security vulnerabilities that crop up from time-to-time.
- **Enable your lock screen.** Most phones allow you to setup a lock screen that protects it from unauthorized entry when not in use. Though you may have the option of setting up a PIN or pattern, it's best to use a passphrase or strong password to lock your device.
- **Enable remote lock and wipe.** If your device somehow becomes lost, you can remotely lock or even wipe your mobile device from a PC to keep unauthorized users from getting to your important data.
- **Enable location services.** Location services do more than just provide your mobile device's GPS with coordinates to determine the best routes. It also provides a near real-time location of your device. This is invaluable when using "Find

- my Phone” services because it will track your smart device’s location with incredible accuracy.
- **Install antivirus/antimalware.** Just like a PC, a smart device needs protection from viruses, trojans, rootkits and other exploits. Having a specific model phone or running the latest mobile OS doesn’t mean that your device is in the clear. With plenty of reputable programs out there that are either free or relatively affordable, it’s best to have added protection.
- **Enroll in a mobile device security plan.** Many big-name cellular services, like AT&T and Verizon have their own security plans available. Though these security plans primarily offer backup options for data and phone replacements, some provide monitoring services to track suspicious activity on your mobile device.
- **Refrain from jailbreaking.** Jailbreaking is the act of removing restrictions imposed by your smart device’s native OS. By jailbreaking, you’re essentially granted root control of your device. This allows users to install and remove applications at their discretion as well as run programs that usually are incompatible with restrictive OS environments. However, jailbreaking also circumvents security measures that are indigenous to your device. And in some cases, jailbreaking also voids warranty programs.
- **Turn off Wi-Fi and Bluetooth.** If you’re not at home or in familiar surroundings, disable your Wi-Fi and Bluetooth capabilities. These services are constantly pinging your environment in hopes of finding a connectable network or device. Not only does it eat your mobile device’s battery, it also leaves your device open to attack. With Wi-Fi/Bluetooth services on, hackers can see networks you’ve connected to in the past. They can then spoof those networks to trick your mobile device into connecting to them.
- **Become vigilant.** Just as you should check your credit report, so should you frequently monitor bank and phone account records for any suspicious activity.

# Health and Human Services 2016 Cybersecurity Awareness Fair

---

The HHS 2016 Cybersecurity Awareness Fair will be held Friday, Oct. 28, 2016, from 9 a.m. to 2 p.m. in the John Winters Building, Public Hearing Room located at 701 W 51st Street, Austin, Texas. All state agency employees are invited to attend. There will be multiple speakers as well as tables with information about security, privacy, identity protection, and business continuity.

Our event is primarily oriented towards training and awareness for our employees for work situations, however, we also recognize that security concerns come at us from all directions daily and we want to address those concerns as well. Therefore, you will find another objective of the event is to give our employees and attendees the capability to make educated decisions around security, privacy, and identity theft in their personal lives as well. We'll be providing employees and attendees informational materials so they can also protect and educate their family, children, their social networks and overall community.

For your convenience I have included an area map, as well as the google directions that can be provided for GPS location services. There is parking in the front of the building when you enter from 51st street.

Google Direction Mapping - <https://goo.gl/76lf7o>

If you have any questions, please feel free to contact me at [InfoSecurity@hhsc.state.tx.us](mailto:InfoSecurity@hhsc.state.tx.us)

# Information Security Officer Spotlight



**Frank Williams**  
Information Security Officer; CCISO, CISSP, CEH  
Teacher Retirement System

I was born and raised on Galveston Island until my family moved to Santa Fe, Texas, where I attended high school. I then followed in my father's footsteps and joined the Navy. I separated in 1996 after six years of service with the intention of using my GI Bill to pay for a degree in electronics. A wise man by the name of Peter Doak placed me on the path of computer networking which eventually got me where I am today. Along the way I met my beautiful wife Jennifer and have made several lifelong friends. Overall pretty darn happy how things have turned out so far.

## **Professional history**

After leaving the U.S. Navy "silent service" fleet, I worked for more than a decade at College of the Mainland in Texas City, Texas filling such roles as instructor, network engineer, UNIX sys-ad, and interim CIO. Making the move to IT security, I made the leap to Texas State University where I moved up the ranks from Security Analyst to interim ISO. When the opportunity presented itself, I accepted the opportunity to serve as the current ISO for Teacher Retirement System of Texas (TRS). I can personally attest that the strong culture and core values of TRS are the reason we are consistently named a Top Workplace in Austin.

## **Who are your customers, and what is one of the most challenging areas for you?**

My customers consist of the 1.4 million public educators and retirees for Texas, as well as the more than 600 talented employees of TRS. The challenge is finding secure solutions that meet the proper balance of our calculated risks.

## **What do you like best of your job?**

The chance to give back to Texas on such a wide scale is definitely the best part of my job. Building a strong comprehensive security program into the culture of an

organization is honestly something I am very passionate about.

## **Top 3 life highlights:**

- Marrying my beautiful wife
- Earning my Submarine Warfare insignia "dolphins" in the Navy
- Teaching my first Cisco Networking Academy class

## **Tell us about your most proud accomplishment.**

After years of attending night school, finally graduating with my bachelor's degree.

## **What books are at your bedside?**

"CISO Soft Skills" by Ron Collette, Mike Gentile, and Skye Gentile.

## **What are your hobbies?**

Besides collecting hacking tools, I enjoy taking out my Nikon on the weekends, tinkering with my guitars, and flying my drone on calm days.

## **If you had to eat one meal, every day for the rest of your life, what would it be?**

Tikka Masala from the Clay Pit.

## **If given a chance, who would you like to be for a day?**

A high school teacher covering emerging technology.

## **What is the best advice you have received and that you have used?**

Always keep Occam's razor handy.

## **What would be your advice for a new security professional?**

Do not just stay behind your keyboard, get involved in your local community. Remember security is a small field, be respectful of those who have come before you

# Events

---

## 2016 Save the Dates

- DIR Technology Forum: Tuesday, October 11, Austin, TX  
[REGISTER HERE](#)
- October 12 (2-4): Threat Report Briefing by NTT Data, William B. Travis Building, room 1-111, Austin, TX  
[REGISTER HERE](#)
- October 19 (9:30 – 10:30): Social Engineering presentation by Denim Group in the Capitol building Room E1.004, Austin, TX  
[REGISTER HERE](#)
- HHS 2016 Cybersecurity Awareness Fair: October 28, 701 W 51st Street, Austin, TX  
9:00a-2pm in the John Winters Building, Public Hearing Room
- MS-ISAC Annual Meeting: October 30 – November 2, San Antonio, TX
- Innotech Austin: November 17, Austin, TX