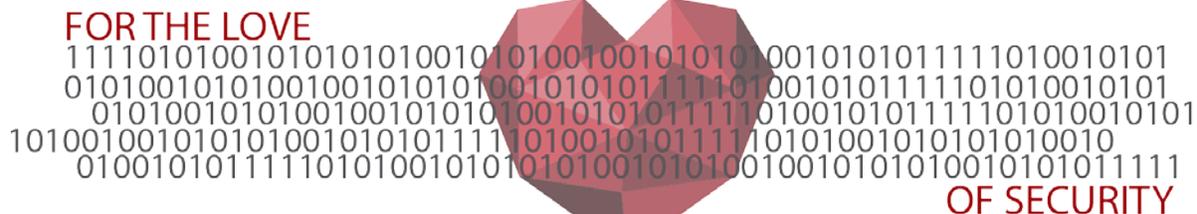


# THE DIR CYBERSECURITY INSIGHT

February FY2016 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV



## Save the Date!

### 16<sup>th</sup> Annual Information Security Forum

It's not exactly a Valentine's date, but it's a date nonetheless.

You don't need gifts or expensive roses. You don't even need to shell out any cash on a fancy dinner. Just be ready to share the love of security among public sector employees!

The 2016 Information Security Forum (ISF) will be held April 14 - 15 at the Palmer Events Center in Austin, Texas. Last year, we updated the format of the ISF and received a lot of great feedback. We hope to continue the tradition of improving this conference every year for our attendees, providing quality content with great networking opportunities. This year's ISF will feature informative break-out sessions and quality keynote speakers.

Share more than your love for security – share your knowledge and experiences by submitting a presentation for a break-out session! This is a great opportunity for collaboration with other security professionals in the public sector.

As planning efforts move forward, more information will become available, including the call for presentations and attendee registration links. Check our [ISF website](#) for more information.

Get ready to share the love...of security!



## CONTENTS

### Monthly Article

Save the Date **P.1**

### Program Updates

NSOC **P.2**

Archer **P.2**

### Our State ISO

### Spotlight

Aaron Blackstone **P.3**

### OCISO Corner

Hannah Kasper **P.4**

### From our State

CISO **p.5**

Events **p.6**

# Network Security Operations Center (NSOC)

---

In the fall of 2015, the NSOC was experiencing complications with email delivery, causing alerts to be quarantined by Office 365. At that time, the issue was addressed by distributing instructions for whitelisting our domain at state mail servers. Then, in December, our NSOC legacy mail server had a hardware failure. Because of this, NSOC Staff began utilizing back up email addresses. This mail server issue has since been recovered, but because of stability and quarantine issues, we are moving all NSOC staff to DIR Microsoft Office 365 email accounts.

What does this mean for you?

- Cleaner whitelisting and delivery of NSOC alerts/communications
- New email addresses to add to your contact list
- NSOC email addresses will now end in @dir.texas.gov (example:

juan.reyes@nsoc.dir.texas.gov would now be juan.reyes@dir.texas.gov)

- New and old addresses will run concurrently for 30 days beginning Feb. 1
- **The NSOC Security Team Distribution List: security-alerts@nsoc.dir.texas.gov will be changed to security-alerts@dir.texas.gov Feb. 1.** This list includes the entire DIR NSOC security team and can be used at any time to respond to alerts, report attacks, security blocking issues or any NSOC security related matter.

As a reminder, we will begin sending out informational alerts as mentioned in the last CISO newsletter beginning Feb 1.

Please don't hesitate to contact me directly with any questions about these changes at jeremy.wilson@dir.texas.gov.

## Archer Updates

---

Several new applications are going into production in the Archer portal this month. We will be hosting webinars to introduce these applications.

### Prioritization of Cybersecurity and Legacy Systems Funding Requests

**HB 1 Article 9, Section 9.10** states:

Out of funds appropriated elsewhere in this Act and in accordance with Government Code, Chapter 2054, the DIR shall submit a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems, as defined in the October 2014 Legacy Systems Study, to be considered for funding to the Legislative Budget Board (LBB) by Oct. 1, 2016. Agencies shall coordinate and cooperate with the department for implementation of this provision.

We provided an overview of the recent legislation charging DIR with submitting a prioritized list of cybersecurity and

legacy modernization projects to the LBB to be considered for funding. In addition, we have demonstrated how to complete the project assessments using the Archer online portal. This webinar was held Feb 4 and a recorded copy will be available on the DIR website.

### Security Plan Template and Policy Module

As you are probably already aware, the Security Plan Template will be due Oct. 15, 2016. We will host two webinars for preparing the security plan template and using the policy module in Archer. The same information will be presented at both webinars. We will be showing you how to enter and submit this information using the Archer portal. Additionally, we will show the various features of the Policy/Exception module in Archer. **Register for the webinar for Tuesday, February 9, 2016 at 1:00 PM CST OR Register for the webinar for Thursday, February 11, 2016 at 9:00 AM CST.**

# Information Security Officer Spotlight

---



**Aaron Blackstone**  
**Information Security Officer**  
 CISSP, CEH, GCIH, FITSI – O/A, Linux+, Sec+  
 Department of Public Safety

I am currently the Chief Information Security Officer for the Department of Public Safety and will be standing up the Cyber Unit within the Homeland Security Division. I am also currently a Captain in the Air National Guard as a Cyber Operations Officer. The past two years I was on active duty in support of the Air Force. Prior to that, I supported the FBI field office in Houston as their Information System Security Officer. I began my IT security career with the Army Research Laboratory in White Sands Missile Range certifying and accrediting military networks. I then took a position securing 5th Army's network and satellite communications. I received my commission from ROTC at Sam Houston State University as a 2nd Lt branching military intelligence. A native of Huntsville, I have a Bachelor of Science in Computer Science from Sam Houston State University.

## **How did you come to the security field?**

I started by trying to crack into my computer games which lead me down the path for computer programming.

## **Tell us how information security has changed since you started in your role.**

I think we, as an industry, are finally gaining traction with the public on the importance of cybersecurity.

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

My customers are all residents in the great state of Texas. Obtaining resources has been challenging as well as changing the mindset about cybersecurity.

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

The Mission. I am born and raised in Texas and love the fact that I am helping my state secure its networks and systems.

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

Commissioning as an officer in the US Army.

## **Top 3 life highlights.**

Passing my CISSP exam

Being accepted into the MBA program at UT

Scuba diving the USS Oriskany

## **What are your hobbies?**

Two-stepping, cycling, scuba diving, and lifting.

## **What books are on your nightstand?**

*Blink, Super Crunchers, and Freakonomics.*

## **What is your hidden talent?**

I'm a pretty good at country dancing.

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

Most people do not plan to fail; they simply fail to plan.

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

Usually the tough jobs no one wants are the best jobs for career growth.

# OCISO Corner – Getting to Know the Team



**Hannah Kasper**  
Marketing Specialist  
Department of Information Resources

## What is your responsibility in DIR and with the State?

I am primarily responsible for developing any publications that come out of the CISO office as well as formatting the monthly newsletter, maintaining web content and assisting in the development of the Texas Cybersecurity Council. In addition, I contribute to the planning of the annual Information Security Forum, Texas State Charitable Campaign and the DIR Wellness committee.

## When and where did you start your career?

My marketing career began almost two years ago at the quaint Texas Agency, DIR. I began as an intern and later accepted a full time position after I graduated from college.

## Why the security field?

It was by chance. I had minimal knowledge and experience with security, but was brought on to help develop and promote a cybersecurity awareness program.

## What is your personal background (born/raised/school/family?)

Born and raised in Austin.

College: Concordia University TX

Family: 1 sweet husband & 1 cute dachshund

## What did you think you were going to be when you grew up?

I still have a burning desire to be firefighter like my dad (excuse the pun).

Other options I have explored:

Doctor, until I realized how many years I would have to be in school.

Marine biologist, but it turns out I am a terrible swimmer and hate big fish & seaweed.

## What is the greatest lesson you have learned?

- 1: Never give up on what you believe in. This drives you to keep trying, learning and growing in every aspect of your life.
- 2: Find something you love and go for it. Don't be lukewarm about what you do.

## What do you want your legacy to be?

I want to be a person who can be the little glimmer of hope on someone's worst day.

I want to build a family that knows love, compassion and patience.

I want to contribute something meaningful to the community in my lifetime.

## Do you have a favorite hobby or pastime?

Baking! I love family recipes. I also enjoy running (a new found pastime) and playing soccer.

## What do you like best about working at DIR?

My team. No doubt about it. I was nervous about my lack of experience, but with their constant support I have learned so much about the cybersecurity field at DIR.

# Insight from our Texas CISO

---

One year ago, President Obama signed an executive order promoting the sharing of cybersecurity information among private sector organizations.<sup>1</sup> In his proclamation, he directed the Secretary of Homeland Security to encourage the development of Information Sharing and Analysis Organizations (ISAOs). Texas will be a key player in the development of the ISAOs and the structure under which they function.



*Eddie Block*  
*CISO, State of Texas*

In September, the Department of Homeland Security selected the University of Texas at San Antonio's Center for Infrastructure Assurance and Security (CIAS) to develop the standards by which ISAOs will function.<sup>2</sup> Not only was this a big win for UTSA and the CIAS, it is a sign that Texas is an important player in securing the information assets that fuel our national economy.

While Dr. Greg White and his team at UTSA are looking at the bigger picture, it prompted me to ask more questions. How are we doing with information sharing in state government? How do we share threat information? How can we be better?

Texas is a large state and trying to keep all 160+ state agencies and institutions of higher education informed (not to mention more than 325,000 state employees) is no easy task. The Office of the CISO has several ways of communicating data out to the state, including email lists, portals, webinars and meeting (both face-to-face and online).

We are always looking at the effectiveness of these notification methods and trying to determine if there is a better way to securely communicate important threat information. As we know, email is not an appropriate way to discuss details of ongoing issues.

The struggle we've faced in the past is getting information that is actionable and sharable. We attempt to get timely information out to state security personnel as quickly and responsibly as possible, but that is often a one-way street. We hope to be more efficient with this as the GRC program continues to mature.

Through the Archer GRC Portal, the OCSIO has better visibility into the ongoing threats, attacks, and responses that the state faces IF agencies and institutions of higher education provide timely information. Through the GRC portal we can capture much more information on attackers and indicators of compromise than we saw in the old Security Incident Reporting System (SIRS). This improved visibility allows us to connect attacks that affect multiple state entities and share mitigation techniques that have worked for others.

I'll be in San Antonio this month to attend meetings with the UTSA CIAS on ISAO standards and to learn how we can improve our sharing in Texas state government. I urge you to be a part of the effort and report through the portal as quickly as reasonable.

We all benefit from the sharing.

*Eddie Block*  
*CISO, State of Texas*

---

<sup>1</sup> <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>

<sup>2</sup> <http://www.utsa.edu/today/2015/09/dhsgrant.html>

# Events

---

## 2016 Save the Dates

- Information Sharing and Analysis Organization (ISAO) Standards Organization Public Meeting: February 9
- General Land Office Sponsored CISSP Boot Camp: February 22- 26 2016
  - Instructor: Doug Landoll
  - \$1750.00
  - Contact: Brandon Rogers 512-463-5763
- TASSCC Technology Education Conference: April 11
- Information Security Forum: April 14-15
- CyberTexas Conference: April 20-21

# OCISO Participation Around the State

---

- Eddie Block presented at the 2016 South Texas Maritime Awareness Security Terrorism Training (MASTT) Cybersecurity Symposium held in Corpus Christi, January 21.
- Eddie Block, Claudia Escobar, Jeremy Wilson and Ray VanHoose will be presenting on “Understanding Cybersecurity: Attack Methods and Defenses” at the Executive Leadership for Information Technology Excellence (ELITE) program on February 17.

THE DIR CYBERSECURITY INSIGHT



---

Feedback, comments, stories, etc. | [DIR OCISO](#) | [DIRSECURITY@DIR.TEXAS.GOV](mailto:DIRSECURITY@DIR.TEXAS.GOV)

---