THE DIR CYBERSECURITY INSIGHT

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

Get Smart. Not Lucky.

Feds Update Classification Policy, and the Effect this has for Texas

In 2010, President Obama established Executive Order (EO) 13556. This EO sets a consistent and uniform manner regarding the handling of Controlled but Unclassified Information (CUI).

Until now, every federal agency has enforced its own type of classification schema for data which requires safeguarding, but isn't considered classified. This has resulted in patchwork systems, inconsistencies in marking and safeguarding and unnecessary restrictions on some data.

EO 13556 provides information security reform that clarifies and limits what needs to be protected and promotes proper information sharing when possible. Out of this executive order, 32 CFR (Code of Federal Regulations) 2002 was created. This is the policy established regarding CUI. The effective date for 32 CFR 2002 was Nov. 14, 2016.

Another important document that was the result of this EO is NIST SP 800-171. This publication provides "federal agencies with recommended requirements for protecting the confidentiality of CUI: (i) when the CUI is resident in nonfederal information systems and organizations; (ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and (iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government wide policy for the CUI category or subcategory listed in the CUI Registry."

What effect will this have on Texas? Several agencies maintain/update federal data, and are required to follow NIST moderate. The policies that have come out of this EO could affect those agencies. Mark Riddle, with the National Archives and Records Administration (NARA) is one of the authors of NIST SP 800-171. He will be at the Information Security Forum in April, and will be sharing valuable insights into this change regarding Controlled but Unclassified Information. Mark will be a keynote speaker on Wednesday, April 11, and will be able to answer your questions and address your concerns. For more information regarding EO 13556, 32 CFR 2002, or NIST SP 800-171, please see the following links:

- Executive Order 13556
- 32 CFR 2002
- NIST SP 800-171

CONTENTS

Monthly Article

Updates

Interest

ISO Spotlight

EVENTS

Save the Date

- **Gartner Webinar**: Wednesday, March 15th
- **TASSCC TEC 2017**: Friday, March 31
- **Information Security Forum**: April 11-12, 2017, Palmer Events Center, Austin, TX

SANS Securing the Human Update

SANS has recently updated the Securing the Human content and the latest content is now available on the DIR Virtual Learning Environment (VLE). For organizations currently in training, your users will see the latest version of the module the next time they log in to complete training. In addition, there are new modules which are available for admins to assign to users. An email regarding these updates was sent to all admins on March 2. If you have any questions, please let us know at dirsecurity@dir.texas.gov

InfoSec Academy Update

The current contract on the Texas InfoSec Academy ends April 27, 2017, but there is still time to enroll in classes! The following certification prep courses are available for enrollment (seats are limited):

Course	Number of Days	Start Dates
Certified Information System Security Professional (CISSP)	5	March 13, March 27 April 10, April 24
Certified Information Security Manager (CISM)	3	March 22 (Online Live) April 19 (Instructor Led)
CompTIA Security+ Certification	5	March 6, March 13, March 20, March 27 April 3, April 10, April 24
Certified Ethical Hacker (CEH) v9.0	5	March 6, March 13, March 20 April 3, April 10, April 24

The online Texas Security Policy & Assurance course is a prerequisite for any of the courses listed above. DIR anticipates a break in service between the existing InfoSec Academy before the award of the new contract.

SPECTRIM

SPECTRIM
DIR
The Statewide Portal for Enterprise Cybersecurity
Threat, Risk and Incident Management

CHANGES COMING MARCH 21ST!

A new look and feel but with the same powerful functionality!!

Training and more information will be provided throughout the month.

Gartner Webinars

The next Gartner webinar will be held March 15, 2017 at 9 a.m. The topic is: **Managing an Aggressive Business Disruption Cybersecurity Attack**.

Awareness of the rapid increase in targeted cyberattacks and the resulting breadth and depth of financial, operational and reputational impact is skyrocketing in boardrooms. Organizations must integrate computer security incident response processes with those of business continuity management (BCM) to ensure effective and timely responses. In this webinar the presenter will discuss the key areas on which to focus your BCM efforts if your organization is a victim of such an event.

To register for this webinar, please visit the link below, click on the green "Attend" button and complete the required fields. You will receive a confirmation email with a calendar invitation containing a link to attend the session. You will also be able to download the presentation on the day of the webinar.

https://www.gartner.com/webinar/3618417

NSOC

Be on the lookout for the 2016 NSOC Threat Report! Attend our breakout session on the schedule or stop by our booth at DIR's annual Information Security Forum for a chat, and a grab a bound copy of the 3rd annual 2016 NSOC Threat Report. New improvements will be included in this year's report. With the continued use of SPECTRIM, the amount of threat data has increased, creating additional 2016 content to analyze and include in the report. We have broken this data into subcategories and are providing closer examinations in these areas:

- Jeremy Wilson is discussing threat categories and NSOC tools and process
- Richard Overfield is discussing DDOS and spear phishing
- Joe Poole is discussing phishing and social engineering
- Juan Reyes is discussing scanning and ports and protocol blocking
- Daniel Lyons is discussing Tor usage

The report is intended to be used as a tool not just for security staff, but also for leaders in state government. We received positive feedback last year from those who distributed copies to their leadership. This report helped them explain what is happening on the threat landscape from the NSOC perspective. We plan to continue improving the report and provide you with even more value this year. We look forward to seeing you at ISF 2017. For 2016 NSOC Threat Report or any NSOC security questions, contact Jeremy.wilson@dir.texas.gov.

RIP, SHA-1 support

Written by Nathan Goggin

After years of service as the NSA's most popular cryptographic hashing function, **SHA-1** (or Secure Hash Algorithm 1) is officially out.

SHA-1 was originally published in 1995 as part of the U.S. Government's Capstone Project, which was tasked with developing cryptography standards for both public and government use. It was designed to encrypt browsing sessions by utilizing a cryptographic hashing algorithm for TSL/SSL certificate validation. Unfortunately, after only 10 years of use, in 2005, SHA-1 was defeated. Tech blogs indicated that a research team from Shandong University in China had accomplished this feat by using collision attacks. This was verified and a paper showing the full attack description was published and distributed in August 2005 at the CRYPTO conference in Santa Barbara, CA.

Not many heeded the warning of SHA-1's potential exploitability as it seemed the means of defeating it were beyond affordability for the average attacker and too complex at the time. Nevertheless, as technology improved, so too has the availability of resources to defeat SHA-1. Earlier this month, researchers for CWI Amsterdam and Google discovered a practical technique for generating hashing collisions, to which SHA-1 is susceptible, which could cost as little as $110,000 on a PaaS.

The moment of truth for SHA-1 came when it was discovered that Git, the huge open-source distributor, still deemed it safe for use. Git is one of the biggest version control systems (VCS) in the world. They, and hundreds of big-name software packages, still rely on SHA-1 signatures for their software installation, data integrity, and version updates distributed over the internet. Linus Torvalds, creator of the Linux kernel, did chime in to counter the bad publicity. He recently posted:

I thought I'd write an update on git and SHA1, since the SHA1 collision attack was so prominently in the news.
Quick overview first, with more in-depth explanation below:
(1) First off - the sky isn't falling. There's a big difference between using a cryptographic hash for things like security signing, and using one for generating a "content identifier" for a content-addressable system like git.
(2) Secondly, the nature of this particular SHA1 attack means that it's actually pretty easy to mitigate against, and there's already been two sets of patches posted for that mitigation.
(3) And finally, there's actually a reasonably straightforward transition to some other hash that won't break the world - or even old git repositories.

Even with such optimism, one major software company, Microsoft, has deemed SHA-1 unsafe and announced in 2013 that they would no longer accept SHA-1 certificates after 2016. This announcement was shortly followed up the next year by Google, indicating that they would go as far as penalizing sites that still implemented SHA-1 hashing certificates as the standard.

To be prepared, it is highly encouraged that organizations immediately stop the use of SHA-1 in favor of its successor, SHA-2. Organizations should also begin to inventory their servers for old SHA-1 certificates currently securing connections to those servers. They should also conduct an audit on their server platforms to determine compatibility with the new standard, SHA-2. Finally, it is recommended that organizations start a migration plan to replace expired SHA-1 certificates to maintain as much of an error-free presence online as possible. For those interested in learning more about the end of life for SHA-1, please check out the references below.

REFERENCES:

https://blogs.windows.com/msedgedev/2016/11/18/countdown-to-sha-1-deprecation/
https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html
https://blog.mozilla.org/security/2016/10/18/phasing-out-sha-1-on-the-public-web/
https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html https://blog.mozilla.org/security/
https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html
https://blogs.technet.microsoft.com/yurikasensei/2016/11/29/sha1-users-guide/

Information Security Officer Spotlight

Robert Edamala, CISSP, CISA, Six Sigma, ITIL
Chief Information Security Officer & Director of Information Security
University of Texas at Arlington

I earned a Bachelor of Arts degree in Accounting and Business Administration from Gordon College, Wenham, MA and a Master of Science degree in Management Information Systems from Temple University in Philadelphia, PA. I hold CISSP, CISA, ITIL, Six Sigma (green belt) and TrendMicro TippingPoint Engineer certs.

I've worked in higher education all my life, starting at the IT Service Desk and, over the course of 15 years, worked my way to Director of IT and University Privacy Officer at Temple University in Philadelphia. I have worn many IT hats including system administrator, database administrator and web application developer. I've been CISO at UTA since 2012.

<u>What agency do you work for? Tell us a little about it.</u>

I'm a proud employee of the University of Texas at Arlington, which is a growing Carnegie Research-1 "highest research activity" powerhouse committed to life-enhancing discovery, innovative instruction, and caring community engagement. An educational leader in the heart of the thriving North Texas region, UTA nurtures minds within an environment that values excellence, ingenuity, and diversity. Check us out at http://www.uta.edu.

<u>How did you come to the security field?</u>

My interest started in early 1993 when, as a computer lab assistant at Gordon College, I helped fellow students recover (when possible) from viruses. I was amazed at the elegance of the malware (as annoying and destructive as they were) and consequently, out of curiosity, tinkered with operating systems and programming as a personal interest. This curiosity paid off at Temple University where I helped the CISO combat malware and to secure systems. Amongst other things, I was responsible for Temple's information security program, managed their anti-malware infrastructure, was involved with their IDM deployment, assisted with investigations and stood in place of the CISO when asked. My dual roles of Director of IT and University Privacy officer, combined with mentorship by the CISO, helped me to understand how to balance security and service delivery. This made information security a natural career path.

<u>Tell us how information security has changed since you started in your role.</u>

Technology disruptors like cloud based technology and smartphones have challenged the traditional notion of a network perimeter — it is increasingly difficult to define. Additionally, vendors are continually developing strategies to ensure lock-in, making exit strategies a focus. Last but not the least, the volume and variety of complex malicious network attacks, as well as phishing attacks, has grown significantly. I've also seen a great degree of maturity in information security practices and awareness. For institutions within UT System, the role of the CISO has prominence which has helped drive several initiatives to improve our overall security posture.

<u>Who are your users/customers, and what is one of the most challenging areas for you?</u>

My primary customers are UTA's faculty, researchers, students and staff. Much like my peers, as a 21st century CISO, my goal is to enable the education, research and to support the overall mission and business of running a world-class institution. The most challenging aspect of my job is keeping abreast of every major information technology use case within the institution and to understand associated security risks (from the physical security and network layer all the way up to technology implementation and use).

<u>What do you like best of your job?</u>

I work with very smart and collegial people throughout the organization who are generally very willing to consider security in their operations or research. This makes my job tremendously easier when discussing risk, security controls and mitigation strategies. Best of all, I do get to see my colleagues succeed in their endeavors and to watch students graduate.

<u>What has been the greatest challenge that you have faced, and how did you resolved it?</u>

Working with limited resources is a challenge, which is normal in most organizations. I focus on what I can do with what I have, explain risk to customers with language that can be understood, listen to them for opportunities for improvement, empower them to mitigate risks, and work hard to meet their needs where possible. I’m also not bashful about requesting help from peers within the organization; I give them credit where due. This formula has never failed, and has in fact helped me achieve many significant goals for the institution.

Tell us about your most proud accomplishment.

Becoming a U.S. Citizen.

Where did you grow up?

I was raised in Zambia. (Google it and then plan your next Safari vacation!)

People would be surprised to know that you…

I learned spoken English from TV reruns in Zambia (notwithstanding English being the official language).

Any favorite line from a movie?

“They're here!” – Poltergeist, 1982

(That moment you observe your intrusion prevention blocking reconnaissance on a recently advertised vulnerability)

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

English meat pies (Cornish pies to be precise).

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

Be quick to recognize, encourage and never stifle creativity in your staff.

What would be your advice for a new security professional?

Don’t settle for mindless, repetitive tasks that only lead to pointless rabbit holes - be resourceful, creative and work hard to make your job easier. Collaborate and never cease learning. Never take things personally and never hold grudges. Above all, understand that your role is to help your customers succeed.