DIR Town Hall: COVID-19 Series, *Cybersecurity*

Wednesday, April 22, 2020

Transforming How Texas Government Serves Texans

Texas Department of Information Resources

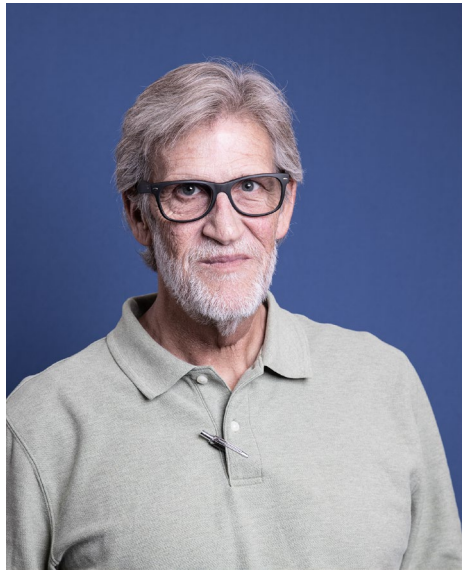
Welcome

Endi Silva

Director of Program Development

Introduction of Speakers

Endi Silva
Director of Program Development



Joe Poole
Network Security Operations Center, Security Operations Center Manager

Suzi Hilliard
Statewide Security Services Manager

Jonathan King
Statewide Cyber Resilience and Response Manager

Agenda

- Welcome and Introductions
- Network Security Operations Center COVID-19 Summary
- COVID-19 Cybersecurity Information
- Security Alerts and Communication
- Questions and Answers
- Conclusion

Network Security Operations Center COVID-19 Summary

Joe Poole
NSOC Security Operations Center Manager

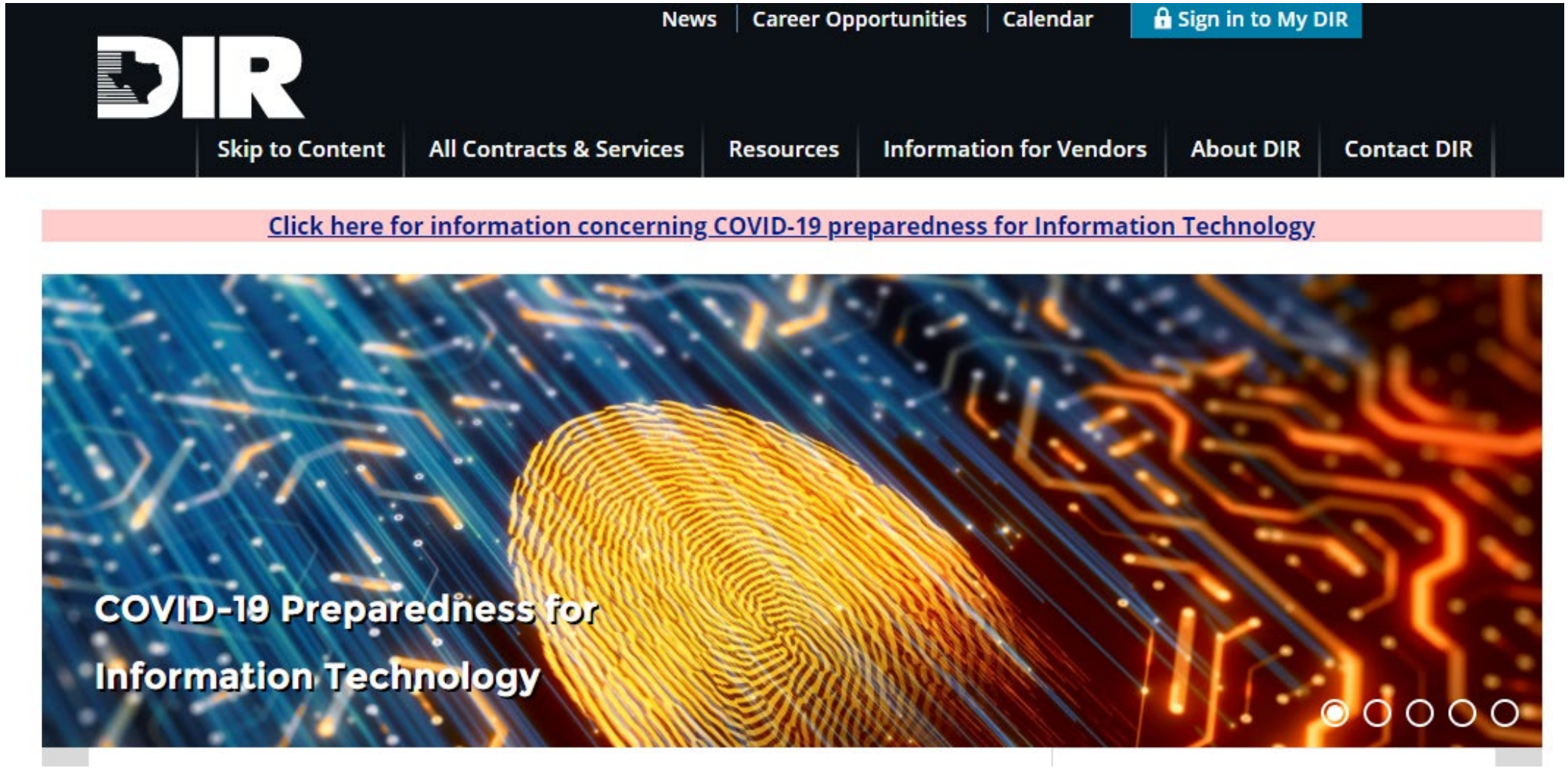
Network Security Operations Center – COVID-19 Summary

- Distributed Denial of Service (DDoS) attacks, where attackers attempt to flood the network to interrupt services, have increased over the past six weeks. So far, we have been able to mitigate these attacks through our DDoS prevention tools, with no decline in services.
- There has been an increase in Covid-19 themed phishing activity. We are blocking those domains as we receive that intelligence both from agencies and outside sources. This crisis presents many opportunities for phishing supply chain providers to target governments as every government entity is trying to procure supplies and services in response to Covid-19.
- Knowing that many governments have opened RDP ports to facilitate teleworking, there has been an increase in "BlueKeep" exploit attempts. Be sure patching is up to date if opening ports to meet teleworking demands.
- The NSOC doubled their Internet Gateway capacity this past month to meet increasing demand as state employees work from home. We see this continuing as some agencies are still adding VPN capacity for remote work. NSOC security tools successfully transitioned to the increased bandwidth and all traffic is being inspected and handled accordingly.

COVID-19 Cybersecurity Information

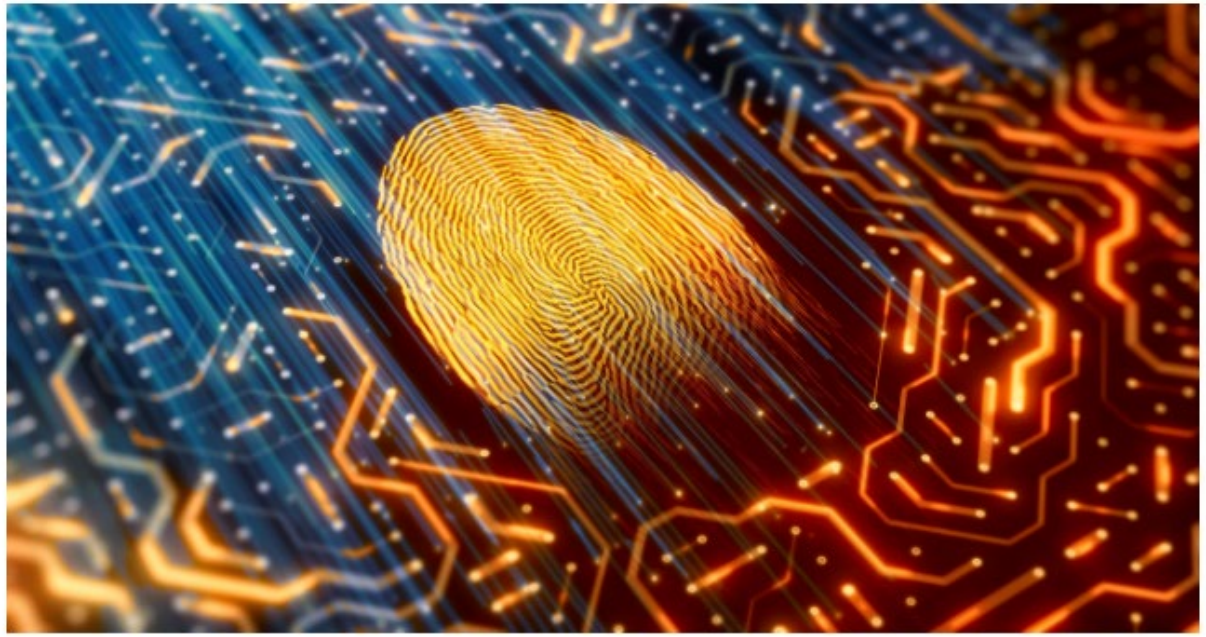
Suzi Hilliard
Statewide Security Services Manager

DIR COVID-19 Information



DIR COVID-19 Information

COVID-19 Preparedness for Information Technology



- Risk Management for COVID-19
- Cybersecurity Hygiene
- Cooperative Contracts for Remote Access and Remote Learning Tools, Products and Services
- Best Practices for Remote Work
- Virtual Private Network (VPN)
- Accessibility
- Resources
- Public Information Requests and the Open Data Portal

DIR COVID-19 Information

Cybersecurity Hygiene

All Texans need to remain vigilant and practice good cyber hygiene, especially during critical incidents. Threat actors often use pressing current events to bait their targets. The current COVID-19 threat is no different. DIR provides cyber hygiene practices everyone should consider for working remotely.

DIR OCISO Teleworking Tips (PDF | 138.28KB) DIR's Office of the Chief Information Security Officer provides the following information technology guidance for teleworkers.

DIR OCISO Virtual Collaboration Tools Security Tips (PDF | 215.77KB) DIR's recommendations for cybersecurity when using virtual collaboration tools.

DIR COVID-19 Information - Telework

DIR Office of the Chief Information Security Officer

Teleworking Tips

How To Be Cyber Safe While Teleworking

Due to the rapidly evolving concerns surrounding the COVID-19 virus, Texas organizations should leverage teleworking capabilities for continuity of operations.

Teleworking is a work arrangement that allows an employee to work during any part of regularly paid hours at an approved alternative worksite (e.g., home, telework center).

DIR provides the following information technology (IT) guidance for teleworkers.

CONNECT WITH CARE, BE CYBER AWARE

Update

- Staying up to date is the best defense against viruses and other online threats.
- Keep your devices, security software and web browsers updated with the latest patches.

Collaborate

- Utilize tools approved by your organization to collaborate, including instant messaging, conferencing software, soft phones and other collaboration tools.
- Depending on the

WiFi

- All WiFi connections should be treated as insecure.
- Ensure your home WiFi has WPA2 or WPA3 security enabled.
- Always connect through Virtual Private Networks

https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/DIR%20OCISCO%20Teleworking%20Tips.pdf

DIR COVID-19 Information – Virtual Collaboration

DIR Office of the Chief Information Security Officer

Virtual Collaboration Tools Security Tips

How to Securely Work and Learn Remotely

As more people are working and learning remotely, many are turning to virtual collaboration tools such as WebEx, Zoom, and Teams to share video, audio, and screen content.

A nationwide trend of disruption or hijacking these meetings, sometimes called "Zoom-bombing" is emerging. Individuals scheduling, hosting, and attending meetings using these tools should remain cyber aware to protect their content and meeting. DIR recommends the following:

CONNECT WITH CARE, BE CYBER AWARE

Secure

- Use your organization's provided services and devices.
- Require participants to enter an access code.
- Avoid reusing access codes

Share

- Avoid adding your meeting to any public calendars or posting it on social media.
- Distribute the meeting link and access code directly to the intended participants.

Manage

- Disable the "Anyone Can Share" feature to prevent unauthorized screen sharing.
- Muting users on entry can prevent potential disruptions.
- Prevent users from sharing

https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/DIR%20Virtual%20Collaboration%20Tools%20Security%20Tips.pdf

DIR COVID-19 Information – Virtual Collaboration

to enter a password.

- Create a unique password comprised of upper, lower case, numbers, and special characters for each meeting.

- Exclude the meeting password from attendee email invitations. Provide the password to attendees via a separate email or by phone.

to "Host Only."

- Check your workspace for unwanted objects, documents, or notes in view of attendees..
- Prevent unauthorized access by locking the meeting after all participants have joined. From the "Manage Participants" option click "Lock Meeting."

WebEx

Zoom

Teams/Skype

GoToMeeting

- Use the "Chat Pinning" tool to ensure you are chatting with the correct recipients.
- Understand that chat, channel, and files data are retained forever unless the system admin has actively modified

- Use the "Attendee List" pane to view all meeting attendees, change their presenter rights, or revoke attendee privileges.
- When sharing content select "Show Only" to share the desired information from your

Security Bulletins and Communication

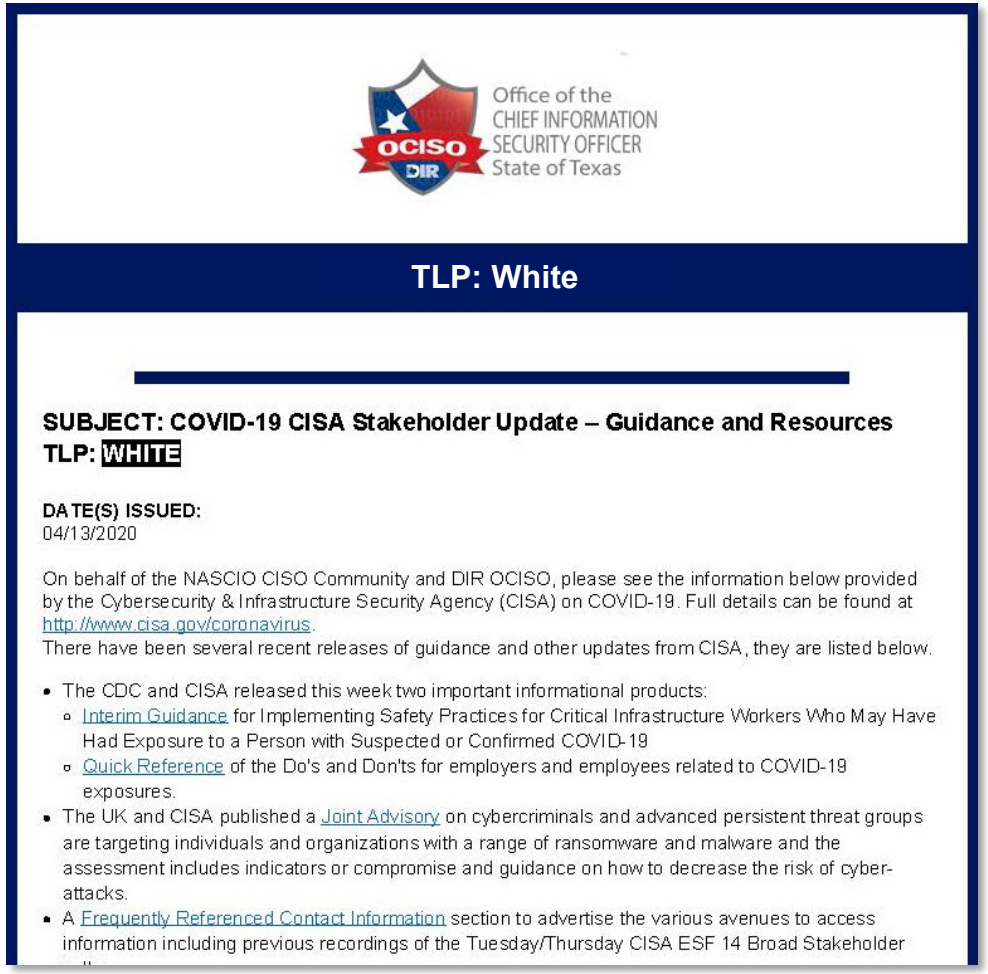
Jonathan King

Statewide Cyber Resilience & Response Manager

DIR COVID-19 Information – Security Bulletins

Bulletin Overview

- Security bulletins are distributed from the DIR Security email address. DIRSecurity@dir.Texas.gov
- Include actionable or situational information and resources for stakeholder community.
- Distributed to over 1400 state and local government employees.
- Classified on the Traffic Light Protocol (TLP).



Office of the CHIEF INFORMATION SECURITY OFFICER State of Texas

TLP: White

SUBJECT: COVID-19 CISA Stakeholder Update – Guidance and Resources
TLP: WHITE

DATE(S) ISSUED:
04/13/2020

On behalf of the NASCIO CISO Community and DIR OCISO, please see the information below provided by the Cybersecurity & Infrastructure Security Agency (CISA) on COVID-19. Full details can be found at http://www.cisa.gov/coronavirus.
There have been several recent releases of guidance and other updates from CISA, they are listed below.

- The CDC and CISA released this week two important informational products:
  - Interim Guidance for Implementing Safety Practices for Critical Infrastructure Workers Who May Have Had Exposure to a Person with Suspected or Confirmed COVID-19
  - Quick Reference of the Do's and Don'ts for employers and employees related to COVID-19 exposures.
- The UK and CISA published a Joint Advisory on cybercriminals and advanced persistent threat groups are targeting individuals and organizations with a range of ransomware and malware and the assessment includes indicators or compromise and guidance on how to decrease the risk of cyber-attacks.
- A Frequently Referenced Contact Information section to advertise the various avenues to access information including previous recordings of the Tuesday/Thursday CISA ESF 14 Broad Stakeholder

DIR COVID-19 Information – Security Bulletins

Bulletin Overview

- COVID-19 related security bulletins are also posted on the Cybersecurity Hygiene page of the DIR COVID-19 website.
- Bulletins posted online are approved for public distribution
- Posted daily as appropriate

Office of the Chief Information Security Officer Bulletins

COVID-19 CISA Stakeholder Update –Guidance and Resources (PDF|246.72KB) April 13, 2020: DIR's Office of the Chief Information Security Officer provides an update from CISA on recently published guides and resources for stakeholders responding to COVID-19.

ZOOM Issues and Alternatives (PDF|209.13KB) April 10, 2020: DIR's Office of the Chief Information Security Officer provides an update on the ZOOM Virtual Collaboration Tool, Potential Issues, and Alternatives.

National Cyber Awareness System Activity Alert COVID-19 Exploited by Malicious Cyber Actors (PDF|222.25KB) April 8, 2020: DIR's Office of the Chief Information Security Officer provides an Alert from the National Cyber Awareness System on COVID-19 Exploited by Malicious Cyber Actors.

Virtual Collaboration Tools Exploitation and Best Practices for Zoom Video Conferencing Service (PDF|232.43KB) April 3, 2020: DIR's Office of the Chief Information Security Officer provides an Alert for Potential Virtual Collaboration Tools Exploitation and Best Practices for Zoom Video Conferencing Service.

FBI PSA FBI Sees Rise in Fraud Schemes Related to the COVID-19 Pandemic (PDF|250.99KB) April 3, 2020: DIR's Office of the Chief Information Security Officer provides a FBI PSA About the Rise in Fraud Schemes Related to the COVID-19 Pandemic.

FBI PSA Cyber Actors Take Advantage of COVID19 Pandemic to Exploit Increased Use of Virtual Environments (PDF|301.6KB) April 2, 2020: DIR's Office of the Chief Information Security Officer provides a FBI PSA About Cyber Actors Take Advantage of COVID19 Pandemic to Exploit Increased Use of Virtual Environments.

Threat Actors Spoof Collaboration Tools (PDF|218.8KB) March 31, 2020: Reports on the rise of newly registered Zoom-themed domains being leveraged for malicious purposes.

DIR COVID-19 Information – Security Bulletins

Example of Bulletins Distributed

- Announcement and guidance on virtual collaboration tool's vulnerability to disruption
- COVID-19 phishing campaigns
- COVID-19 exploitation by malicious cyber actors
- Remote desktop protocol exploitation attempts
- Potential malicious domain name registration associated with COVID-19
- Malicious information analysis
- Interim CDC guidance for critical infrastructure workers
- Indicators of compromise (IoCs) with a COVID-19 nexus

DIR COVID-19 Information – Security Bulletins

Traffic Light Protocol (TLP)

- Created to facilitate greater information sharing.
- Indicates when and how information can be shared.
- Four TLP classification categories for information.

TLP:RED	Not for disclosure, restricted to participants only.
TLP:AMBER	Limited disclosure, restricted to participants' organizations.
TLP:GREEN	Limited disclosure, restricted to the community.
TLP:WHITE	Disclosure is not limited.

DIR COVID-19 Information – Resources

Resource List

- **DIR COVID-19 Website**
  https://dir.texas.gov/View-Resources/Pages/Content.aspx?id=69
- **Telework Tips Sheet**
  https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/DIR%20OCISCO%20Teleworking%20Tips.pdf
- **Virtual Collaboration Tools Tips Sheet**
  https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/DIR%20Virtual%20Collaboration%20Tools%20Security%20Tips.pdf
- **Webinars & Emergency Board Meetings**
  https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Tips%20for%20Conducting%20Open%20Meetings%20Remotely.pdf
- **OCISO Security Bulletins**
  https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=157

OCISO Contact Information

- The OCISO operates a 24/7 Security Incident Hotline at (877) DIR-CISO or (877) 347-2476.
- Monitored email: DIRSecurity@dir.texas.gov
- Security Mailing List Access Request http://lists.state.tx.us/mailman/listinfo/security

Thank You

dir.texas.gov

#DIRisIT

@TexasDIR

Transforming How
Texas Government
Serves Texans

Texas Department of Information Resources