All You Need to Know About MSS

DuWayne Aikins | AT&T

Suzi Hilliard | DIR

Texas Department of Information Resources

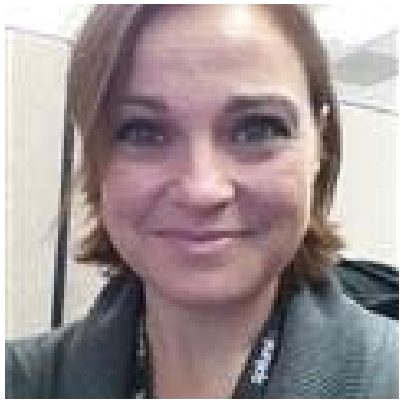
Today's Speakers

DuWayne Aikins, Jr.

AT&T

Suzi Hilliard

DIR



Agenda

Today's webinar will cover the following topics:

- What is MSS?
- What services are included in the MSS offering?
- Does DIR pay for any services? How can I take advantage of that?
- How do I get started?

Managed Security Services: Overview

Available Now!

Texas Department of Information Resources

What is Managed Security Services?

Managed Security Services (MSS) is an offering within DIR's Shared Services program, providing a cost-effective solution to state, local, municipal, and higher-education cybersecurity needs.

MSS is composed of three (3) Service Components, each containing multiple services to choose from to meet your IT security needs:

- Security Monitoring and Device Management
- Incident Response
- Risk and Compliance

Am I eligible for all MSS services?

Certain security services are included within the scope of the DCS infrastructure services contract and therefore cannot be procured separately for devices residing in a Consolidated Data Center (CDC) or covered by the DCS public cloud offering. An MSS FAQ and Service Matrix is available with specific details for you to determine whether certain services are available to your device(s), depending on their location.

http://dir.texas.gov/View-Contracts-And-Services/Pages/Content.aspx?id=45

Managed Security Services: Overview

Texas Department of Information Resources

Security Services

Security Monitoring and Device Management

- Security Information and Event Management (SIEM)
- Threat Research
- Security Operations Center Services
- Managed Endpoint Security
- Host Based IDS/IPS
- Network Based IDS/IPS
- Managed Firewall
- Managed Web App Firewall
- Malware Detection System

Incident Response

- Incident Response Preparedness
- Digital Forensics
- Security Incident Management

Risk and Compliance

- Penetration Test
- Web and Mobile Application Test
- Vulnerability Scanning
- Web App Vulnerability Scanning
- Risk Assessment
- Cloud Compliance Assessment

Security Monitoring and Device Management (SMDM)

Texas Department of Information Resources

What SMDM services are available?

Available Only in Legacy Data Centers:

- Endpoint Management Services
- Intrusion Detection/Prevention System Services
- Managed Firewall Services
- Malware Detection Systems
- Security Operations Center (SOC) Services
- Host-based Intrusion Prevention Systems*

Available for Non-DCS managed systems:

- Host-based Intrusion Prevention Services
- Security Information and Event Management (SIEM)

Available for ALL Systems and Locations:

- Web Application Firewall Services
- Threat Research

Remote Management and Operations

San Antonio, Texas	Tampa, Florida
Dallas, Texas	San Jose, California

Security Operations Center Services (Onsite Management)

DIR NSOC
Austin, Texas

Where Needed
Texas

Where Needed
Texas

Incident Response Services

Texas Department of Information Resources

Incident Response Services

Incident Response Preparedness*

Provides a critical review of current internal processes and procedures for handling events, incidents, and evidence. Includes:

- Detective control configurations
- Deployed preventative and detective solution sets throughout the environment
- Current incident response plans
- Incident responder and handler skillset evaluations
- Incident responder and handler training evaluations
- Evidence seizure and storage procedure analysis
- Electronic data recovery
- Litigation support

Digital Forensics

- "On Demand" service
- Use of Encase and/or Carbon Black for analysis of hard drive images

Incident Response Management

- No retainer for this service
- Address adverse events, issues, or occurrences that may occur in your environment
- Includes detection, triage, response activities, and containment of computer security events

*** Important Note:** DCS Program customers already receive Incident Response services as part of your DCS assurances. However, if a security incident moves beyond the level of Atos contracted support to security incident analysis, the analysis can be performed by the MSS vendor (AT&T) upon Customer request.

Risk and Compliance Services

RISK & COMPLIANCE

SERVICES

- Penetration Testing
- Vulnerability Scanning
- Web Application Scanning
- Web and Mobile Application Penetration Testing

- Risk Assessment
- Cloud Compliance

What Can I Get for Free?

State agencies and Institutions of Higher Education can request DIR-funded services. Services are available on a first come, first served basis as funding permits

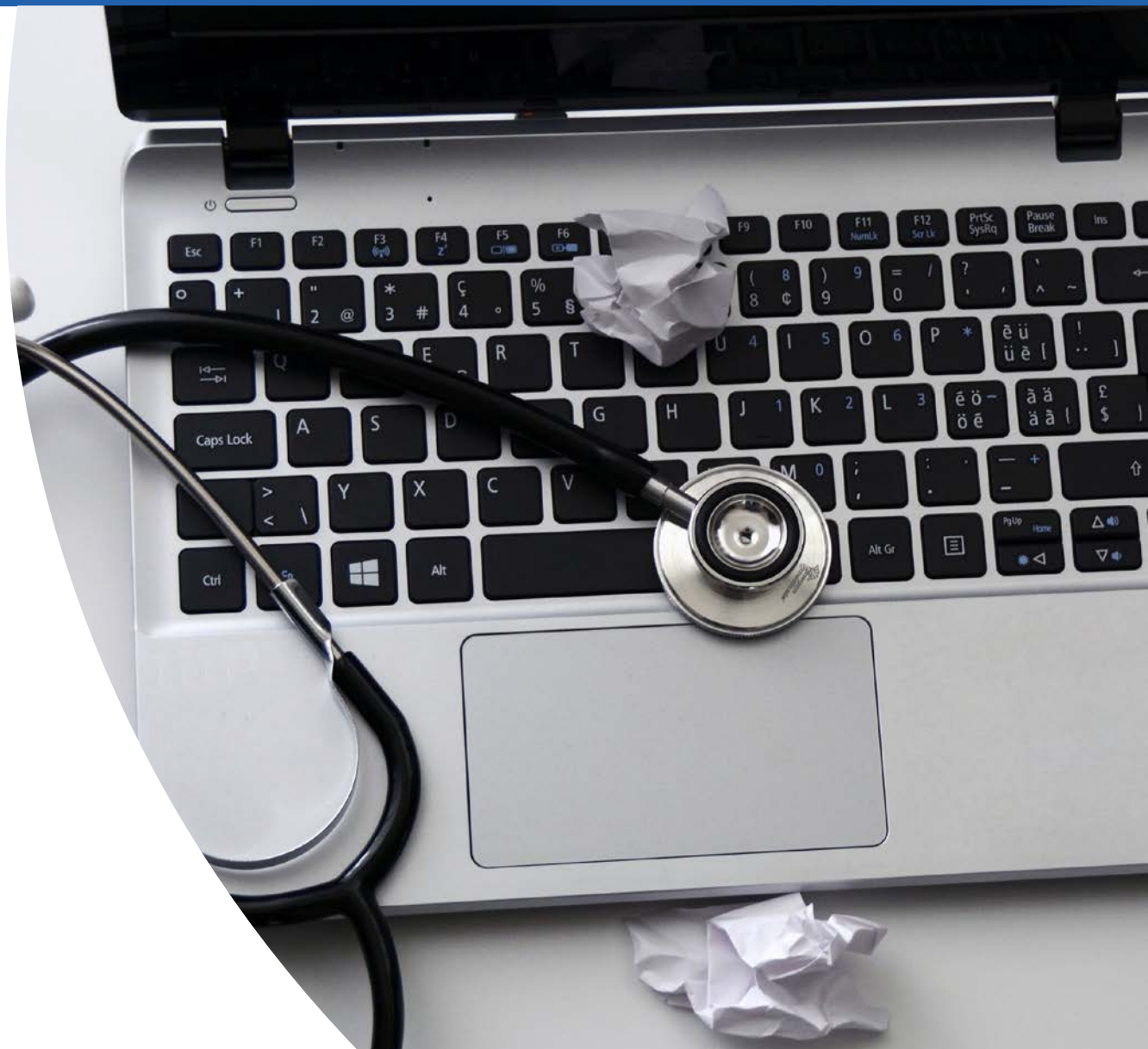
- Texas Cybersecurity Framework (TCF) Assessments
- Black Box-Remote External Penetration Tests
- Web/Mobile Application Penetration Tests (Limited to one per organization)

TCF Assessments

- House Bill 8, passed in the 85th Session, requires each state agency to conduct an information security assessment at least once every two years

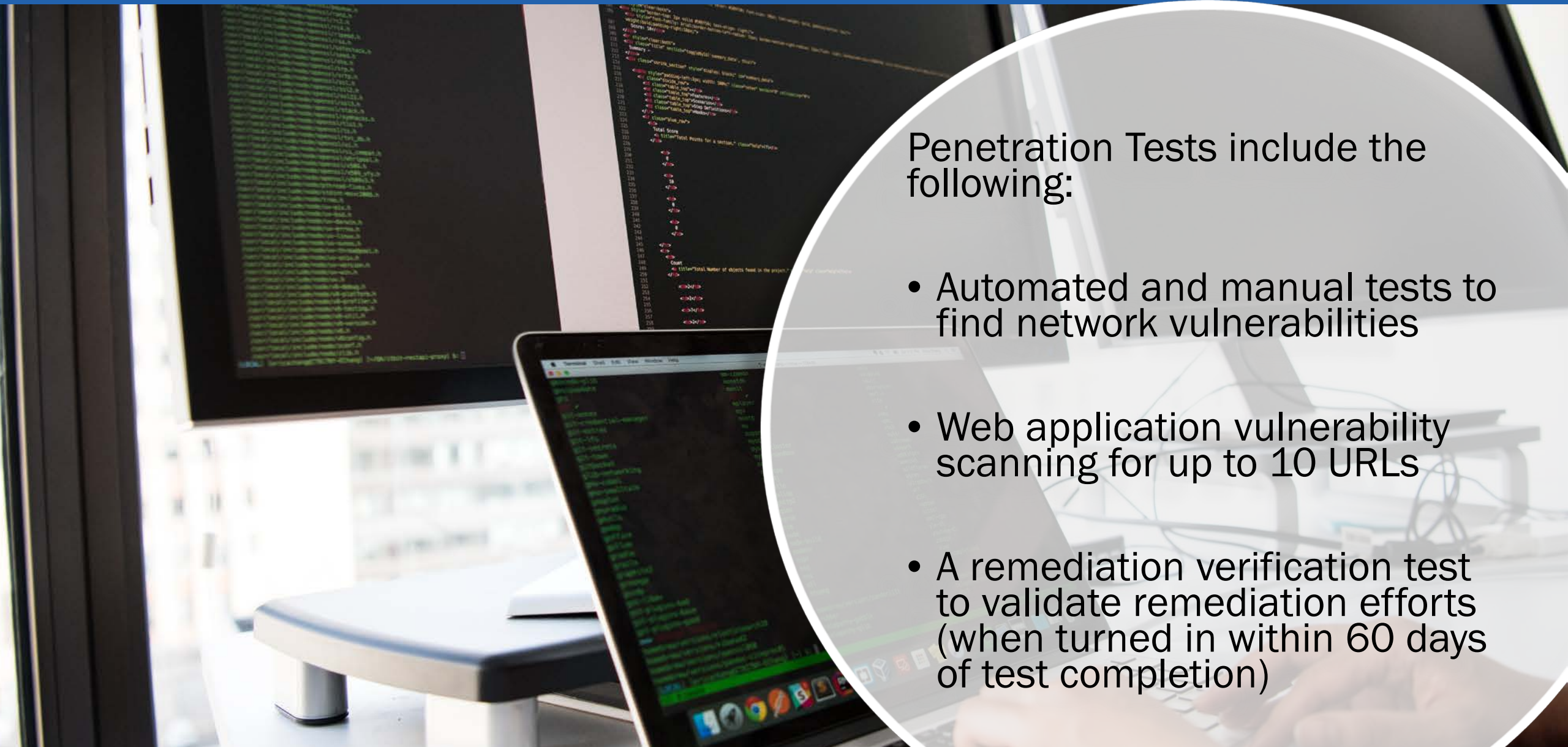
- The Texas Cybersecurity Framework Assessment is offered to meet this requirement

- The TCF assessment is an overall gauge of the ‘health’ of the organization



Penetration Tests

Texas Department of Information Resources



Penetration Tests include the following:

- Automated and manual tests to find network vulnerabilities
- Web application vulnerability scanning for up to 10 URLs
- A remediation verification test to validate remediation efforts (when turned in within 60 days of test completion)

Web/Mobile App Pen Testing

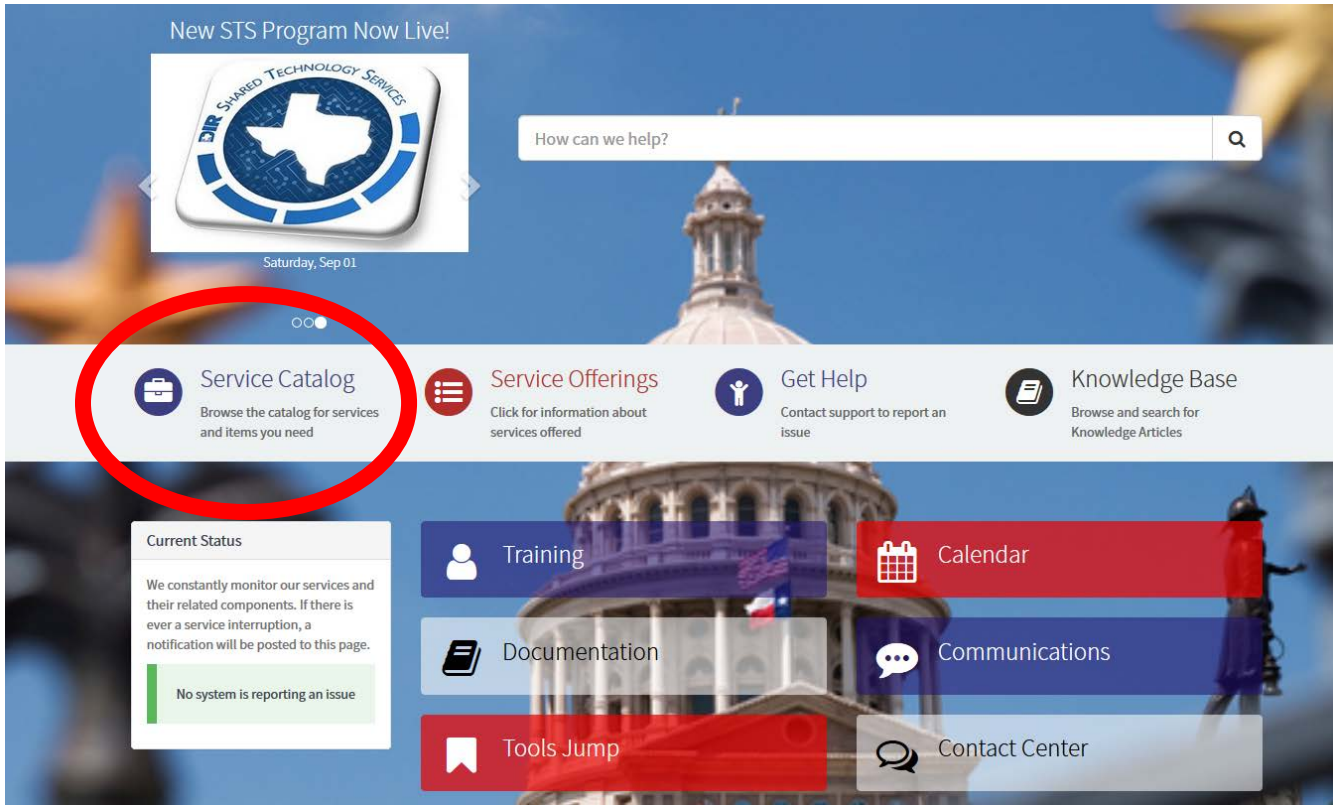
- House Bill 8 from the 85th Legislative session requires all state agencies to conduct a penetration test on any web or mobile application that processes any sensitive personal information or confidential information

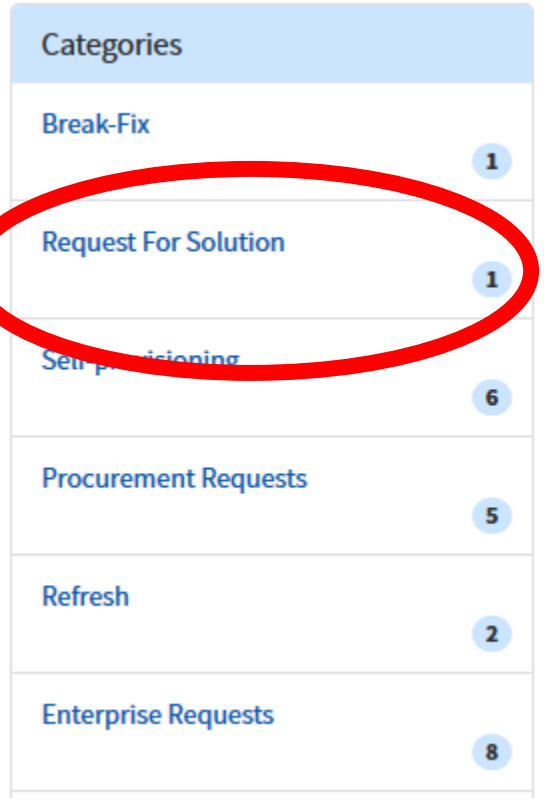
- DIR received limited funding to assist agencies with this effort.

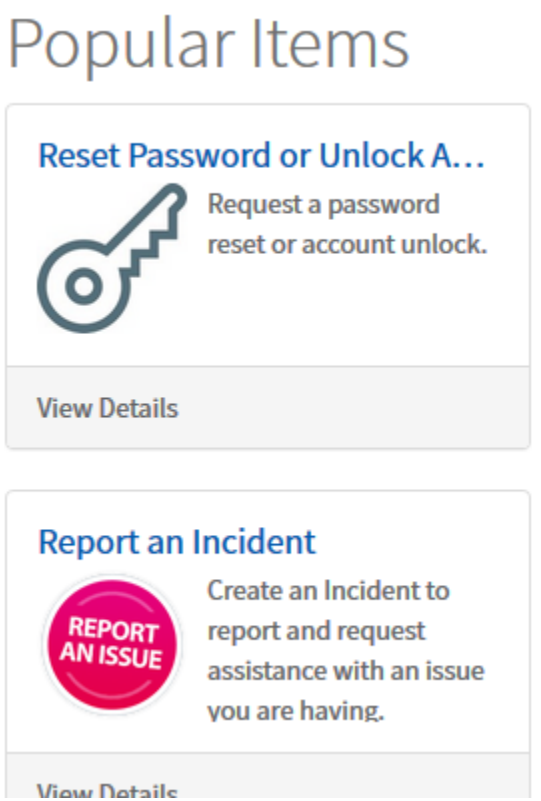
- Web/mobile application penetration testing includes an automated Web Application Vulnerability Scan along with manual tests to find vulnerabilities and potential exploits

How Do I get Started?

- If you are already a Shared Technology Services (STS) customer, you can submit a Request for Solution in the new STS portal

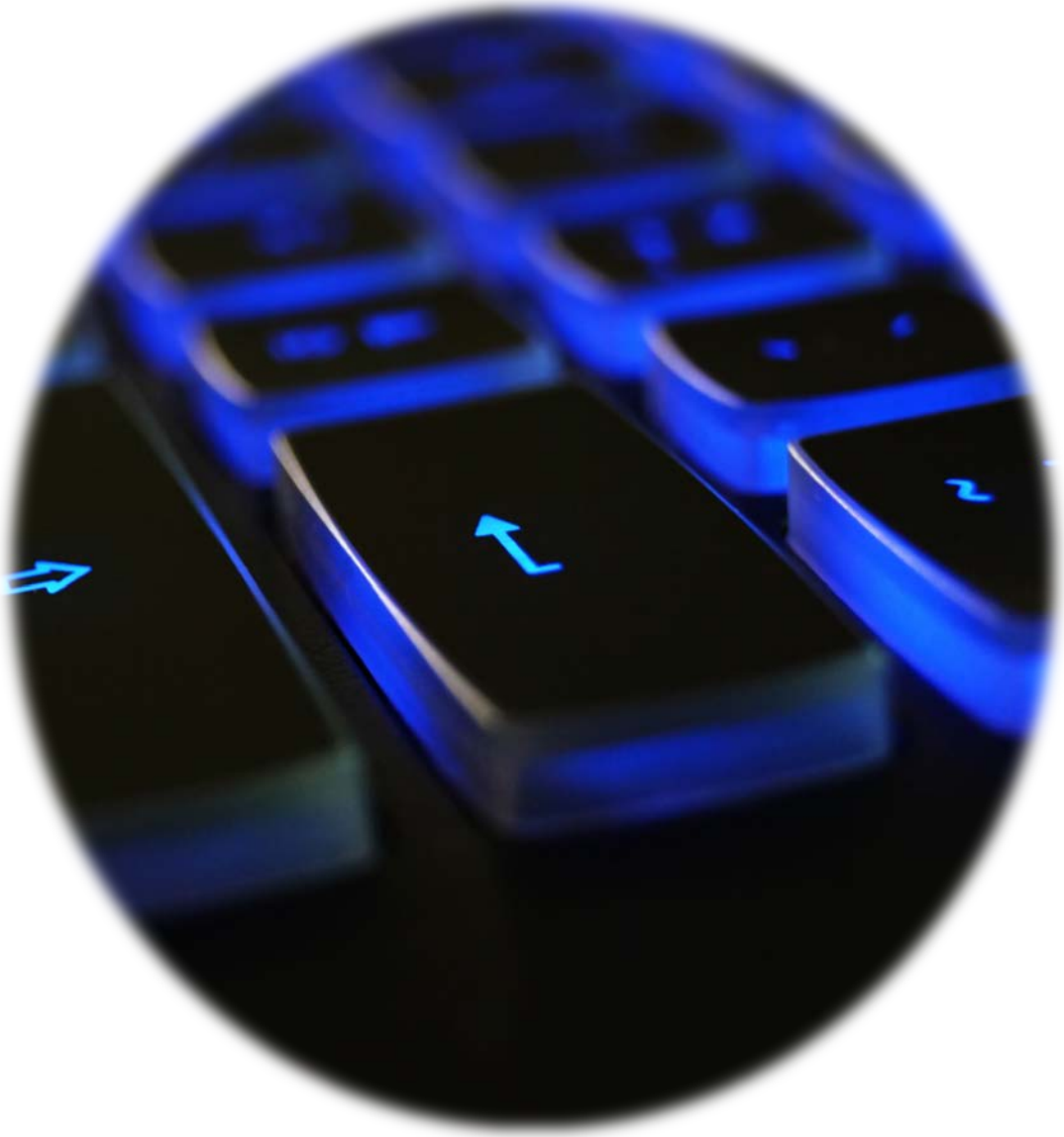






Getting Started – Existing Customers

- Select “Managed Security Services”, and the service component you’re interested in:
  - Incident Response
  - Risk and Compliance, or
  - Security Monitoring Device Management
- Complete all required fields.
  - If requesting DIR-paid services:
    - Penetration testing: Select Penetration Testing – Black Box-Remote External
    - TCF assessment: Select Texas Cybersecurity Framework Assessment
    - Web/Mobile App Pen test: Select Penetration Testing – either Web or Mobile Application
- Submit!



Getting Started – New Customers

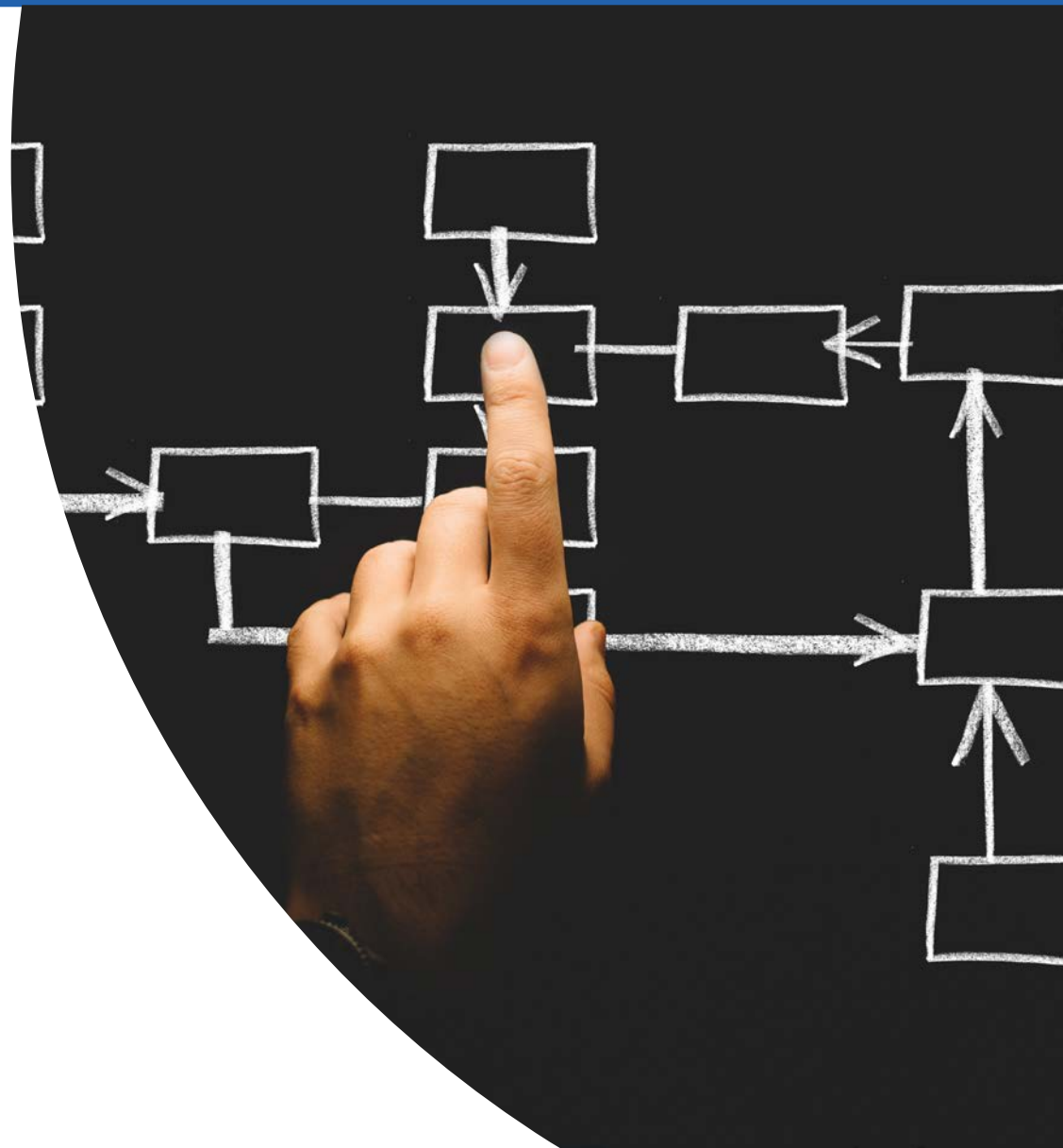
- If you are not currently a DIR Shared Technology Services customer, but are interested in onboarding, contact DIRSharedServices@dir.Texas.gov, or DIRSecurity@dir.Texas.gov.
- DIR will send you a New Customer Form. If you are also interested in DIR-paid services, we will send you an RFS Information form.
- Once we get those back, a few things will happen in parallel:
  - We will draft and send you an Inter-Agency or Inter-Local Contract (IAC/ILC)
  - We will submit your first request on your behalf
  - We will begin the process to get you onboarded

Getting Started – New Customers

Texas Department of Information Resources

Note that no work can actually begin until the IAC/ILC is executed

- AT&T will be assigned to the ticket, and they will reach out to you to get more details about your request
- Once the IAC/ILC is returned and fully executed, and you have agreed to the MSS Terms and Conditions, AT&T will work with you to set engagement dates for the project
- Work begins!



Thank you!

For more information:

DIRSharedServices@dir.Texas.gov

DIRSecurity@dir.Texas.gov

da892r@att.com (DuWayne Aikins – AT&T)

Texas Department of Information Resources