City of Austin

Cybersecurity Briefing

Community Technology & Telecommunications Commission

November 19, 2020

Shirley A. Erp
Chief Information Security Officer (CISO)

Shirley Erp
Chief Information Security Officer
City of Austin

About Shirley

Over 20 years Information Security Experience in Health, Education, Banking, Retail, Insurance, Energy, Government (Federal, State, and Local)

Education:

- Master of Science (MS) in Technology Management
- Bachelor of Science (BS) in Computer Science

Certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Project Management Professional (PMP)
- Certified Data Privacy Solutions Engineer (CDPSE)
- IT Infrastructure Library (ITIL)

Agenda

- Information Security Office (ISO) Introduction
- FY2021 High-Level Plan
- “BlueLeaks“ Third-Party Data Exposure
- Protecting Residents and the City of Austin

Information Security Office Introduction

CoA Cybersecurity Program

Alignment with:

- Federal - National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
- State - State of Texas Laws, Regulations, and Rules
- Cybersecurity Best Practices

Protection of:

- Critical information systems and assets
- Confidential information including personal private information

Collaborative with:

- City departments
- Regional partners
- State and local entities

CoA Information Security Program

Security and Privacy:

The How: Information security is a set of practices intended to keep data secure from unauthorized access or alterations. Here's a broad look at the policies, principles, and people used to protect data

- **Confidentiality** - Protecting confidentiality is dependent on being able to define and enforce certain access levels for information
- **Integrity** - Integrity assures that the data or information system can be trusted
- **Availability** - Authentication mechanisms, access channels, and systems all have to work properly to protect information and ensure it is available when needed

The What: Information privacy pertains to personally identifiable information. At the City, this includes the personal data collected, assembled, maintained, or prepared on behalf of the City of Austin.

City Code

§ 2-11-16 - INFORMATION SECURITY OFFICE

- Leads, directs, and manages the citywide information security program, including:
  - Policy
  - Risk management
  - Security operations
  - Security architecture
  - Incident response
  - Governance
  - Privacy

§ 2-11-17 - DUTIES OF DEPARTMENT DIRECTORS - INFORMATION SECURITY

- Implement security program requirements
- Include resource expenditures for information security and privacy

Overview

What We Want

VISION: Austin is a beacon of sustainability, social equity, and economic opportunity…

Strategic Outcomes

- Economic Opportunity and Affordability
- Mobility
- Safety
- Health and Environment
- Culture and Lifelong Learning
- Government That Works for All

Risks We Face

CHALLENGE: If we do not manage these risks, we have a problem

- Third-Party Risk
- Regulatory & Compliance Risk
- Ad-Hoc Practices
- Complexity of Technology
- Loss of Data / Services
- Being Unaware of Incidents
- Being Unprepared to Respond

How We Mitigate This

How We Do It

In order to implement the solutions, we have adopted the *National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)*

Objectives

- Manage cybersecurity risk to systems, assets, data, and capabilities
- Implement safeguards to ensure delivery of critical infrastructure services
- Identify the occurrence of a cybersecurity event
- Take action regarding a detected cybersecurity event
- Maintain plans for resilience and restore capabilities or services impaired due to a cybersecurity event

Identify

Protect

Detect

Respond

Recover

Connecting Strategy and NIST CSF

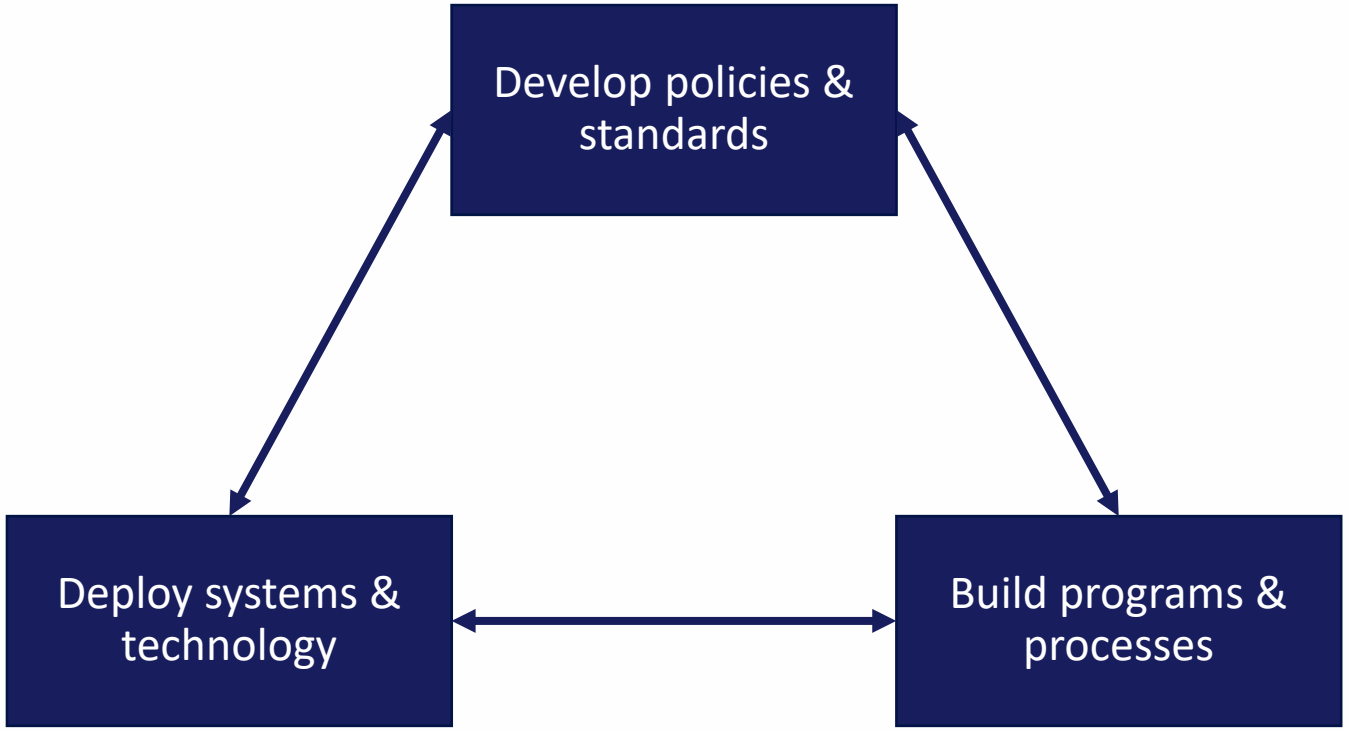
Objectives

- Manage cybersecurity risk to systems, assets, data, and capabilities
- Implement safeguards to ensure delivery of critical infrastructure services
- Identify the occurrence of a cybersecurity event
- Take action regarding a detected cybersecurity event
- Maintain plans for resilience and restore capabilities or services impaired due to a cybersecurity event

Function	Categories
Identify	Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management
Protect	Identity Management, Authentication, and Access Control • Awareness & Training • Data Security • Info. Protection Processes and Procedures • Protective Technology
Detect	Anomalies and Events • Security Continuous Monitoring • Detection Processes
Respond	Response Planning • Communications • Analysis • Mitigation • Improvements
Recover	Recovery Planning • Improvements • Communications

FY2021 High-Level Plan

ISO General Strategy



CoA Cybersecurity Projects

Continue to Mature:

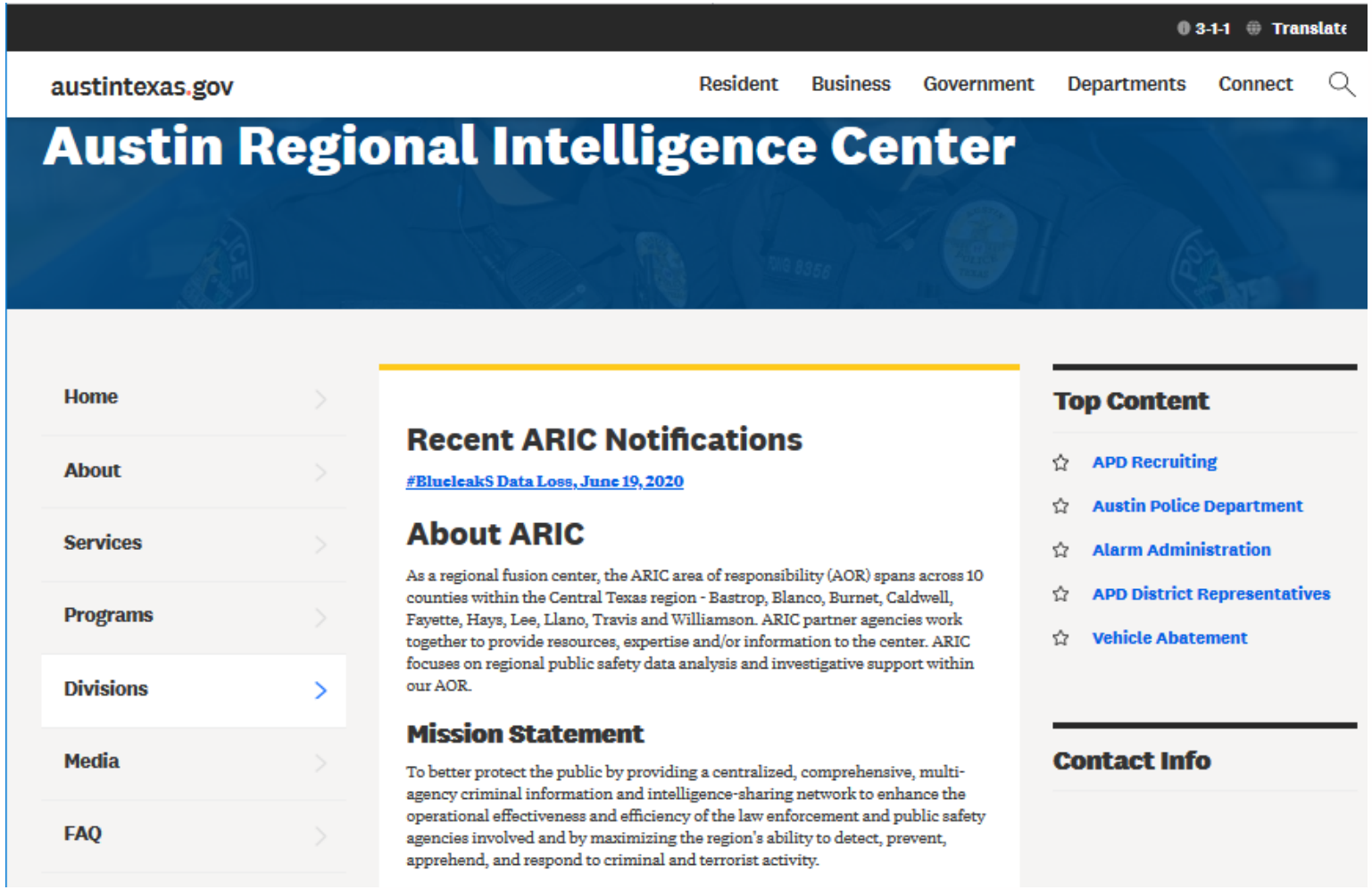
- Policy and standards
- Multi-factor authentication (MFA)
- Identity and Access Management (IAM)
- Defense-in-depth technologies
- Cybersecurity monitoring

“BlueLeaks” Third-Party Data Exposure

Public Information About BlueLeaks

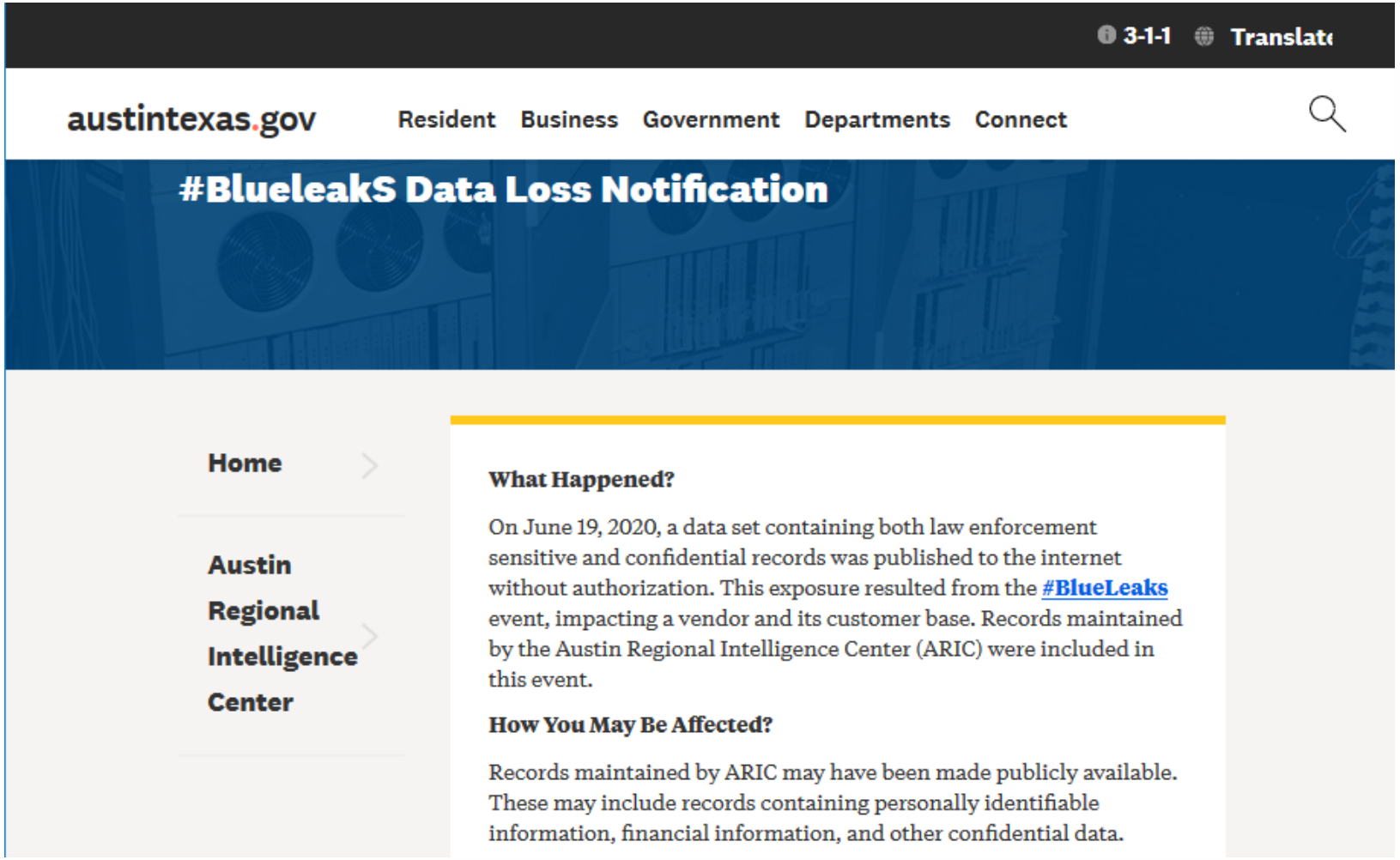
- Third-party vendor was compromised impacting over 200 nationwide law enforcement agencies
- June 19, 2020 –269 gigabytes of internal U.S. law enforcement data was exposed
- Exposure included personal data of 700,000 police officers
- Austin Regional intelligence Center (ARIC) is one of the 200 agencies
- ARIC responsibility spans 10 counties and various agencies, including the City of Austin

ARIC Notification



https://www.austintexas.gov/department/austin-regional-intelligence-center

ARIC Notification



https://www.austintexas.gov/page/blueleaks-data-loss-notification

Protecting Residents and the City of Austin

Technology & Cybersecurity Considerations

- Attack Surfaces - are the different points where an unauthorized user can attack a system, such as:
  - Physical
  - Network
  - Software
  - People
- Attack Vectors - are the methods cybercriminals use to gain unauthorized access to a system, such as:
  - Compromised credentials
  - Misconfiguration
  - Vulnerabilities
  - Missing or weak encryption

How CTTC Can Help

- Include security and privacy requirements in recommendations:
  - Architecture
  - NIST Controls
  - Security awareness
  - Contract agreements
  - Separation of resident services from City business infrastructure
  - Physical protections
  - Budget for Security