A CALL FOR TWO FACTOR AUTHENTICATION

Peggy Bodin, CISA, Assistant Director of IT Audit, State of Washington
Kathy Lovejoy, CPA, CISA, Senior Audit Manager, State of Illinois
State of Illinois - Office of the Auditor General

Responsible for conducting financial audit and compliance examinations of State agencies and universities. We conduct about 150 audits a year, including the State’s CAFR and Single Audit.

Two divisions:

- Financial and Compliance - 55 staff
- Performance - 21 staff
In Washington, we audit every government in the state.

- Includes school districts, library districts, cities, counties, ports, and many others.
- We also audit state agencies, such as Department of Social and Health Services as well as universities and community colleges.
- In addition, we audit the finances of the state as a whole.

~ 2,300 local governments
Agenda

- Why use 2 factor authentication?
- What is 2 factor authentication?
- When to use 2 factor authentication
- How it is used - Illinois
- Cost, challenges, and difficulties
- Auditing 2 factor authentication
- Resources
- Questions
Is 2 Factor Authentication used in your State?

Yes

No

Unsure
Why use 2 factor authentication?
Washington’s experience

• 37 cyber frauds reported in past year
  ✓ Include 3 reported ransomware attacks
• Employee and email interfaces
DHS cyber director warns of surge in Iranian "wiper" hack attacks

"Wiper" attacks targeting US companies' data are on rise, CISA Director Krebs says.

Ransomware: Why cities have become such a big target for cyberattacks - and why it'll get worse

A number of US cities have paid ransoms of hundreds of thousands of dollars after getting caught out by hackers -- and if the business model is working, cybercriminals will keep exploiting it.
Oregon-Senator Wyden has requested the Department of Education to enact multi-factor authentication to access FAFSA records.

Free Applications for Federal Student Aid (FAFSA)

April 2017 the online tool was hacked and files of over 100,000 applicants were impacted.
What is multi-factor authentication?

- It is a security system that requires more than one method of authentication from independent categories of credentials to verify an individual’s identity.
Many ways to implement

- Hard tokens
- Soft tokens
- Certificate based
- Biometric
All, nothing, or somewhere in between?

- Critical operations
- Banking and wire transfers
- Confidential data and applications
- Employee self service
- Administrative users
- All users?
When is it required/strongly suggested?

- U.S. government
  - Mandatory to access specific government websites
- Healthcare
  - Health Insurance Portability and Accountability Act (HIPAA)
- Defense
  - Uses the Common Access Card
- Law enforcement
  - Criminal Justice Information Services (CJIS)
  - National Crime Information Center (NCIC)
When is it required/strongly suggested?

- Financial industry
  - Processing credit cards
    - PCI-DSS
    - NIST 800-53
  - ATMs
    - ATM card and PIN
State of Illinois

- Department of Innovation and Technology
  - Environment
    - HIPAA
    - CJIS
    - IRS
- Department of Corrections, Illinois State Police, Department of Juvenile Justice
  - Mobile devices
    - CJIS requirements
- Department of Revenue
- Department of Employment Security
  - State and federal tax information
    - IRS Publication 1075
Cost, challenges and difficulty

- Expensive: Smart card, hardware tokens
- Implementation complexity
- User buy-in, particularly biometric
- Circumvention

2 factor authentication solves a user access and credential theft problem. It doesn't stop all layers of exploitation.
Cost, challenges and difficulties: State of Washington experience

• State agency implementation
  ✓ External access to confidential data using State’s SecureAccess® Washington or Transact™ Washington
  ✓ Remote access to agency network

• Local governments
  ✓ CJIS requirements leading the way
  ✓ Collaboration is key (ACCIS)
Cost, challenges and difficulties: State of Illinois

- State’s environment
- Multiple users with different requirements
- Tokens and smart cards cost
Making it easier

The ‘built in factor’

- Windows 10 has MFA
- Phones - biometric controls
- VPNs - digital certificate

Easily available solutions

- Titan Security Key (Google)
  https://cloud.google.com/titan-security-key/

- Google authenticator
Are you conducting audits of two-factor authentication?

Yes

No

I don't know
Auditing 2FA in Washington

• Cybersecurity audits
  ✓ Admin Access (CSC 5.7): MFA or 15 characters

• State agency security compliance attestation audits using agreed-upon procedures
Encourage use of MFA

Protect your financial management system to prevent unauthorized access and service disruption, such as using strong passphrases and multi-factor authentication. SAO recommends multi-factor authentication be used for any online system that contains confidential information.

https://www.sao.wa.gov/becybersmart/
Auditing 2FA in Illinois

- DoIT SOC Examination
  - Environment requirements
- DOR/DES
  - Application requirements

https://www.auditor.illinois.gov/Audit-Reports/DoIT.asp
Resources

▶ National Institute of Standards and Technology
  ▶ NIST 800-63B Digital Identity Guidelines
  ▶ Multifactor Authentication Practice Guide for E-Commerce (sp 1800-17) (July 2019)
    https://csrc.nist.gov/publications/detail/sp/1800-17/final
  ▶ Public Safety / First Responder Mobile App Single Sign-on (SP 1800-13) (May 2019)
    https://www.nccoe.nist.gov/projects/use-cases/mobile-sso
Resources

Center for Internet Security

Securing Online Accounts with Multi-factor Authentication (May 2019)
https://www.cisecurity.org/newsletter/securing-online-accounts-with-multi-factor-authentication/
Resources

- IRS Publication 1075

- Criminal Justice Information Services

- U.S. Department of Health & Human Services
  - [https://www.hhs.gov/hipaa/index.html](https://www.hhs.gov/hipaa/index.html)

- Payment Card Industry Security Standards
  - [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org)
Questions
Contact information

- Peg Bodin: bodinp@sao.wa.gov or (360) 464-0113
- Kathy Lovejoy: Klovejoy@auditor.Illinois.gov or (217) 782-6046