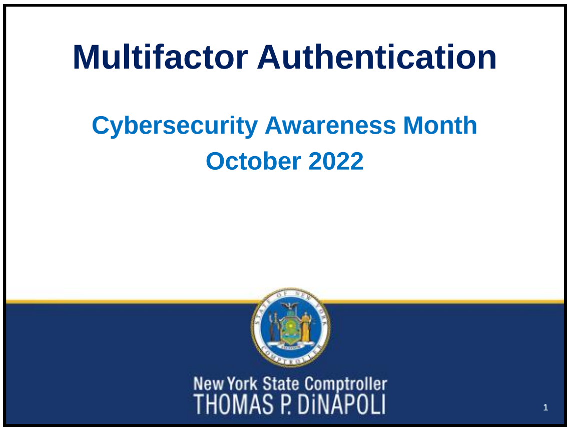
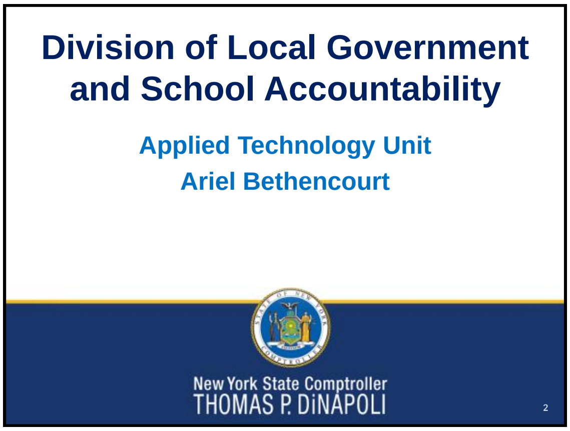


Multifactor Authentication

Cybersecurity Awareness Month

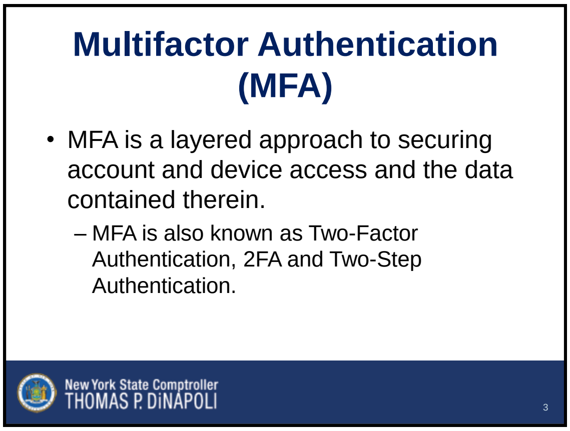
October 2022



Division of Local Government and School Accountability

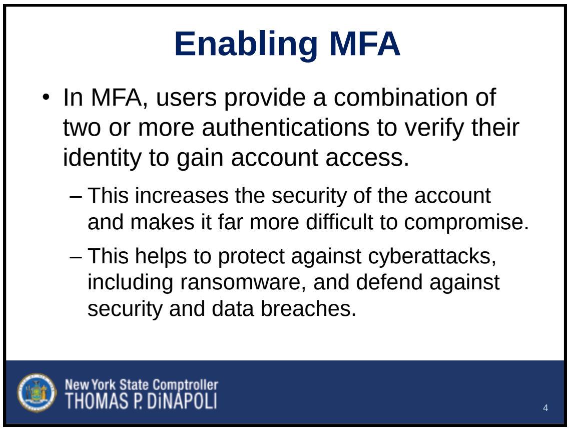
Applied Technology Unit

Ariel Bethencourt



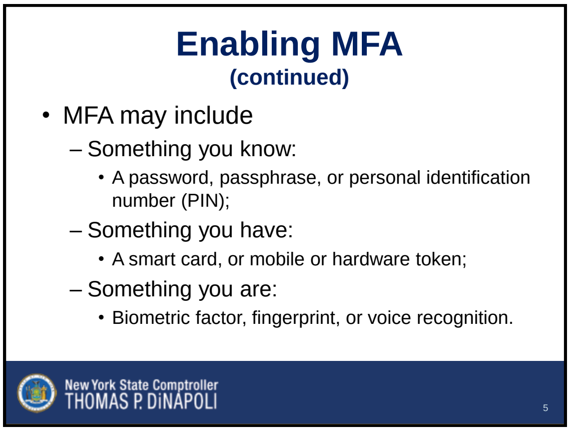
Multifactor Authentication (MFA)

- MFA is a layered approach to securing account and device access and the data contained therein.
  - MFA is also known as Two-Factor Authentication, 2FA and Two-Step Authentication.



Enabling MFA

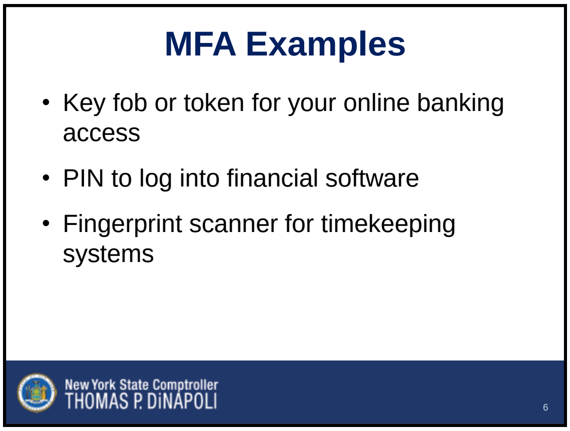
- In MFA, users provide a combination of two or more authentications to verify their identity to gain account access.
  - This increases the security of the account and makes it far more difficult to compromise.
  - This helps to protect against cyberattacks, including ransomware, and defend against security and data breaches.



Enabling MFA

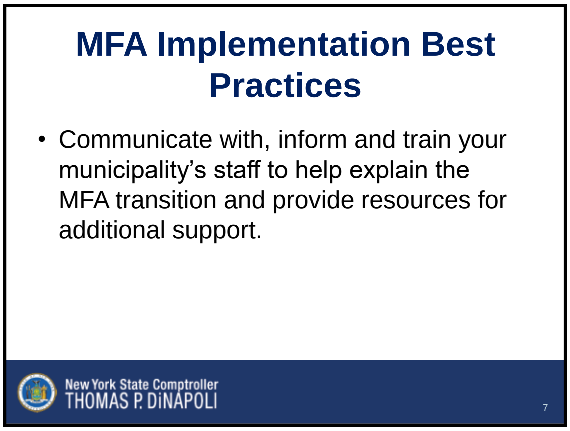
(continued)

- MFA may include
  - Something you know:
    - A password, passphrase, or personal identification number (PIN);
  - Something you have:
    - A smart card, or mobile or hardware token;
  - Something you are:
    - Biometric factor, fingerprint, or voice recognition.



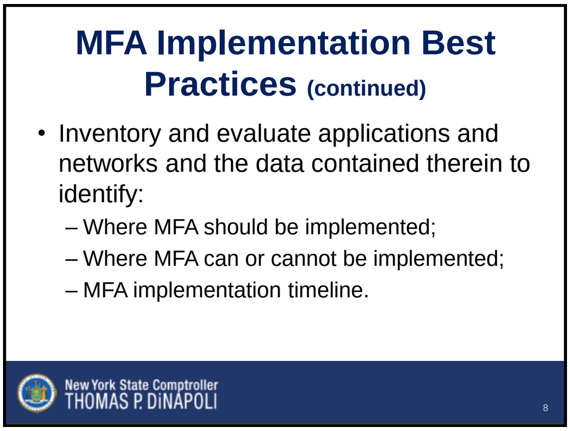
MFA Examples

- Key fob or token for your online banking access
- PIN to log into financial software
- Fingerprint scanner for timekeeping systems



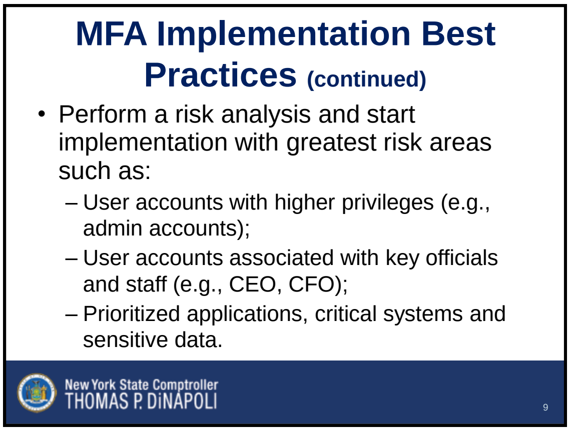
MFA Implementation Best Practices

- Communicate with, inform and train your municipality’s staff to help explain the MFA transition and provide resources for additional support.



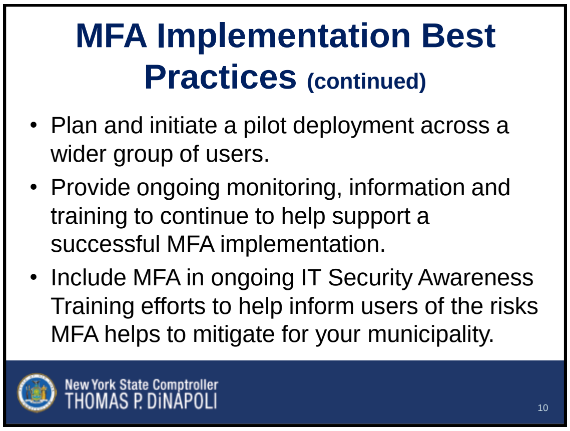
MFA Implementation Best Practices (continued)

- Inventory and evaluate applications and networks and the data contained therein to identify:
  - Where MFA should be implemented;
  - Where MFA can or cannot be implemented;
  - MFA implementation timeline.



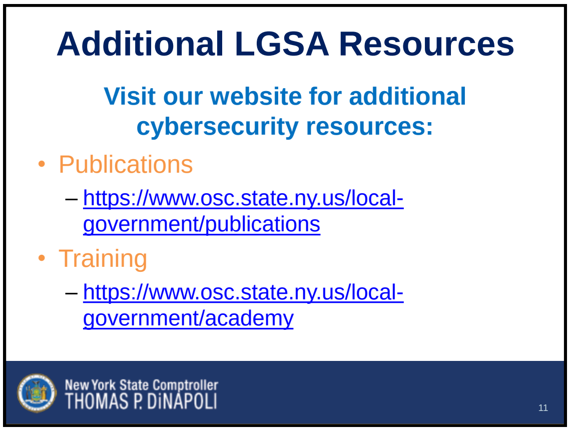
MFA Implementation Best Practices (continued)

- Perform a risk analysis and start implementation with greatest risk areas such as:
  - User accounts with higher privileges (e.g., admin accounts);
  - User accounts associated with key officials and staff (e.g., CEO, CFO);
  - Prioritized applications, critical systems and sensitive data.



MFA Implementation Best Practices (continued)

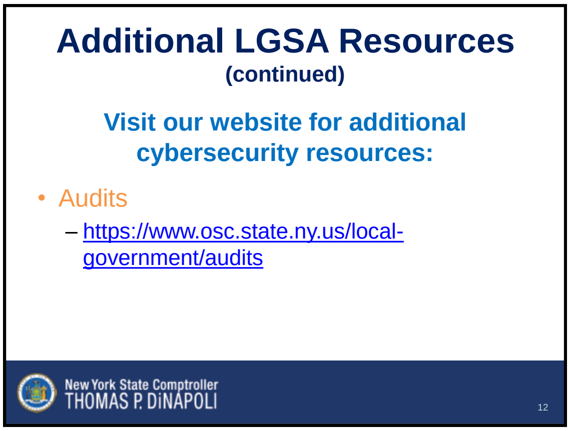
- Plan and initiate a pilot deployment across a wider group of users.
- Provide ongoing monitoring, information and training to continue to help support a successful MFA implementation.
- Include MFA in ongoing IT Security Awareness Training efforts to help inform users of the risks MFA helps to mitigate for your municipality.



Additional LGSA Resources

Visit our website for additional cybersecurity resources:

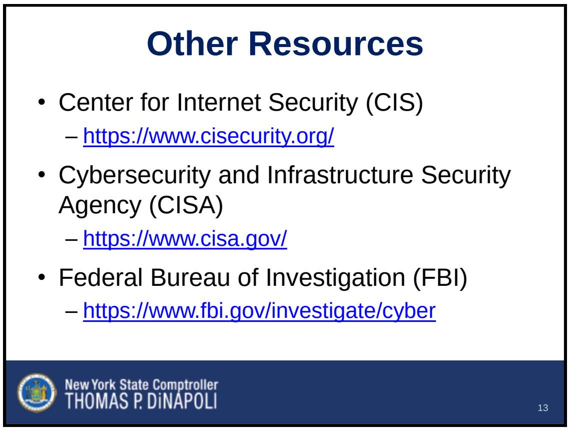
- Publications
  - https://www.osc.state.ny.us/local-government/publications
- Training
  - https://www.osc.state.ny.us/local-government/academy



Additional LGSA Resources (continued)

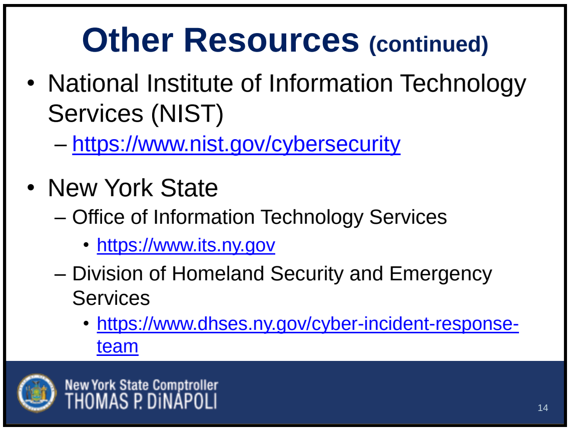
Visit our website for additional cybersecurity resources:

- Audits
  - https://www.osc.state.ny.us/local-government/audits



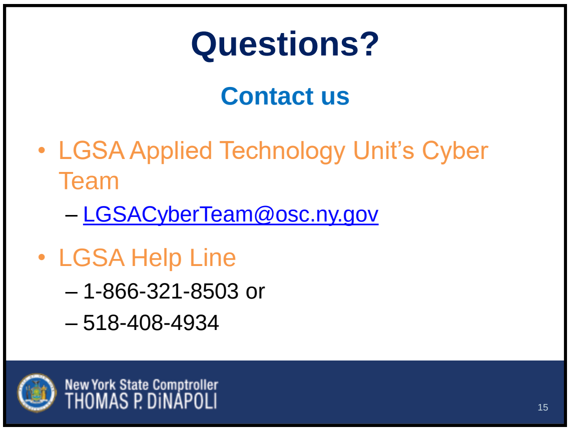
Other Resources

- Center for Internet Security (CIS)
  - https://www.cisecurity.org/
- Cybersecurity and Infrastructure Security Agency (CISA)
  - https://www.cisa.gov/
- Federal Bureau of Investigation (FBI)
  - https://www.fbi.gov/investigate/cyber



Other Resources **(continued)**

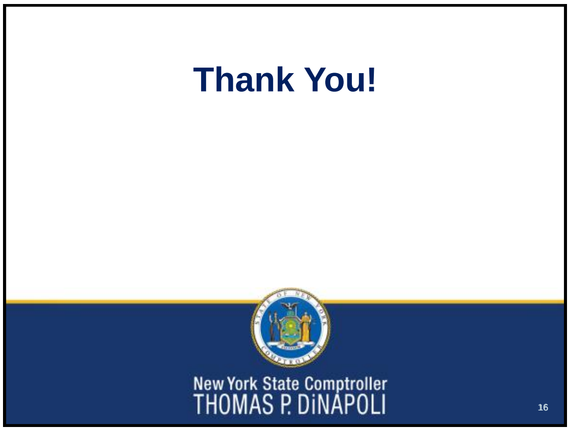
- National Institute of Information Technology Services (NIST)
  - https://www.nist.gov/cybersecurity
- New York State
  - Office of Information Technology Services
    - https://www.its.ny.gov
  - Division of Homeland Security and Emergency Services
    - https://www.dhses.ny.gov/cyber-incident-response-team



Questions?

Contact us

- LGSA Applied Technology Unit's Cyber Team
  - LGSACyberTeam@osc.ny.gov
- LGSA Help Line
  - 1-866-321-8503 or
  - 518-408-4934



Thank You!

New York State Comptroller
THOMAS P. DiNAPOLI

16