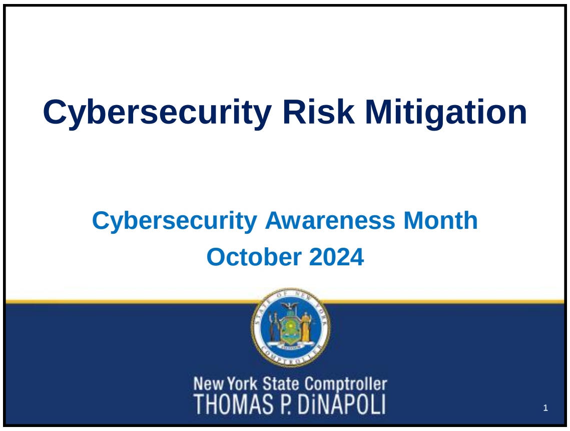
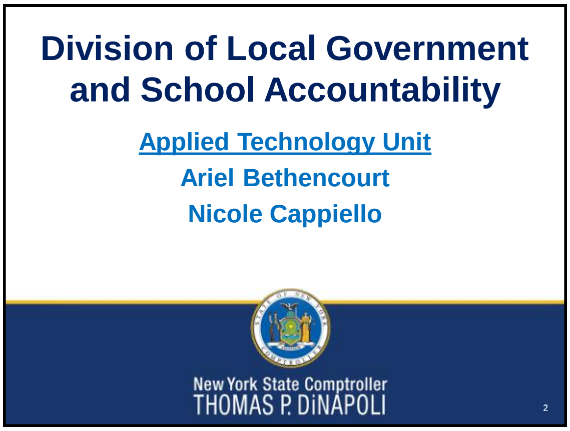


Cybersecurity Risk Mitigation

Cybersecurity Awareness Month
October 2024

New York State Comptroller
THOMAS P. DiNAPOLI

1

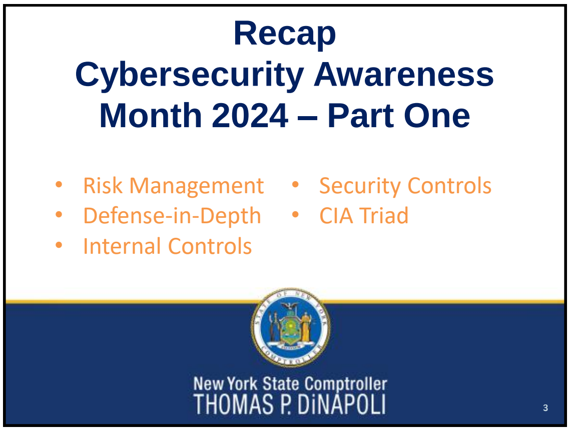


Division of Local Government and School Accountability

Applied Technology Unit
Ariel Bethencourt
Nicole Cappiello

New York State Comptroller
THOMAS P. DiNAPOLI

2

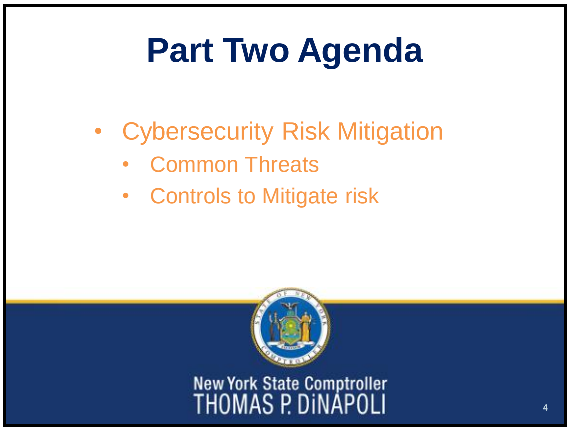


Recap Cybersecurity Awareness Month 2024 – Part One

- Risk Management
- Defense-in-Depth
- Internal Controls
- Security Controls
- CIA Triad

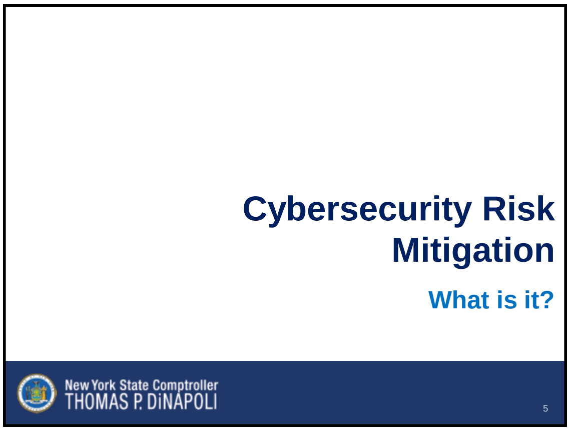
New York State Comptroller
THOMAS P. DiNAPOLI

3



Part Two Agenda

- Cybersecurity Risk Mitigation
  - Common Threats
  - Controls to Mitigate risk



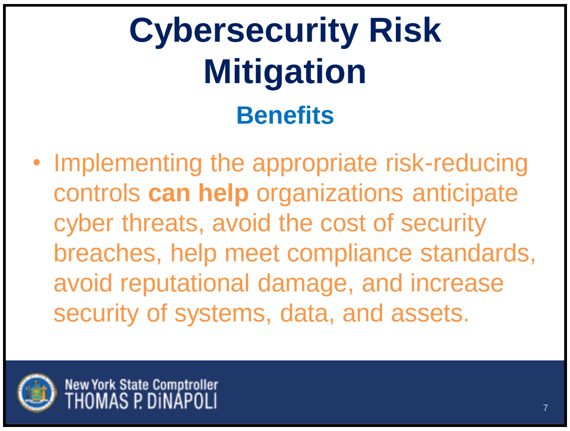
Cybersecurity Risk Mitigation

What is it?

Cybersecurity Risk Mitigation

What is it?

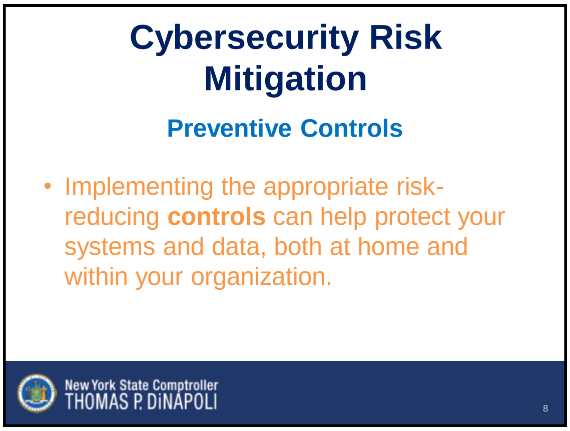
- **Cybersecurity risk mitigation** is prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.



Cybersecurity Risk Mitigation

Benefits

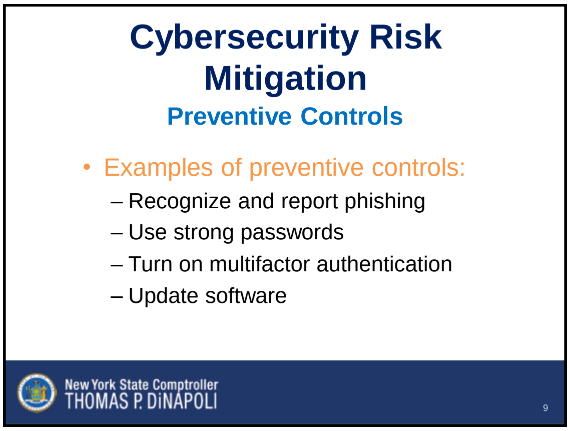
- Implementing the appropriate risk-reducing controls **can help** organizations anticipate cyber threats, avoid the cost of security breaches, help meet compliance standards, avoid reputational damage, and increase security of systems, data, and assets.



Cybersecurity Risk Mitigation

Preventive Controls

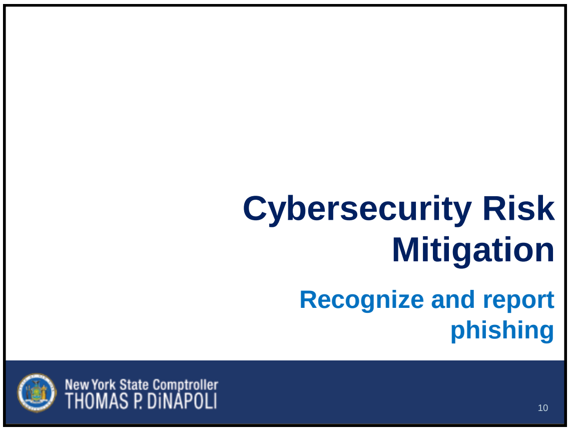
- Implementing the appropriate risk-reducing **controls** can help protect your systems and data, both at home and within your organization.



Cybersecurity Risk Mitigation

Preventive Controls

- Examples of preventive controls:
  - Recognize and report phishing
  - Use strong passwords
  - Turn on multifactor authentication
  - Update software

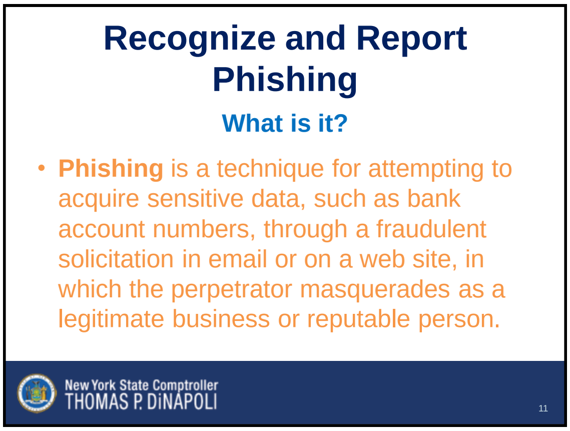


Cybersecurity Risk Mitigation

Recognize and report phishing

New York State Comptroller
THOMAS P. DiNAPOLI

10



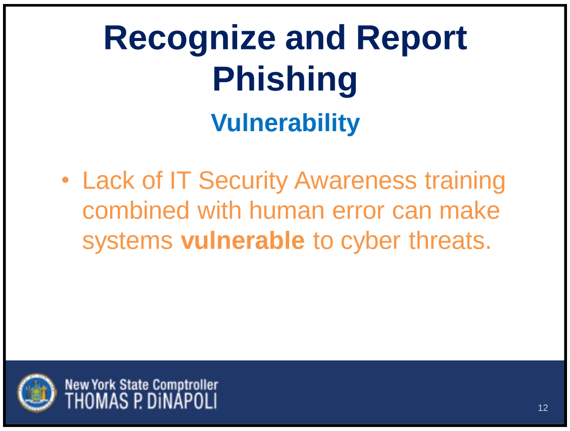
Recognize and Report Phishing

What is it?

- **Phishing** is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.

New York State Comptroller
THOMAS P. DiNAPOLI

11



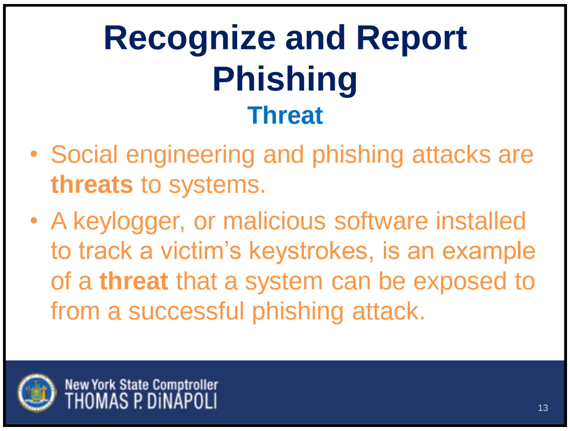
Recognize and Report Phishing

Vulnerability

- Lack of IT Security Awareness training combined with human error can make systems **vulnerable** to cyber threats.

New York State Comptroller
THOMAS P. DiNAPOLI

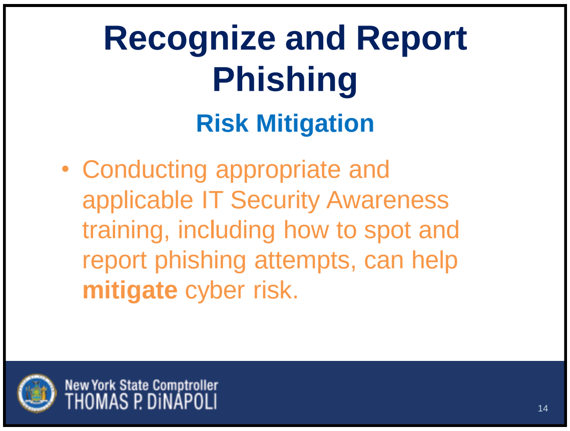
12



Recognize and Report Phishing

Threat

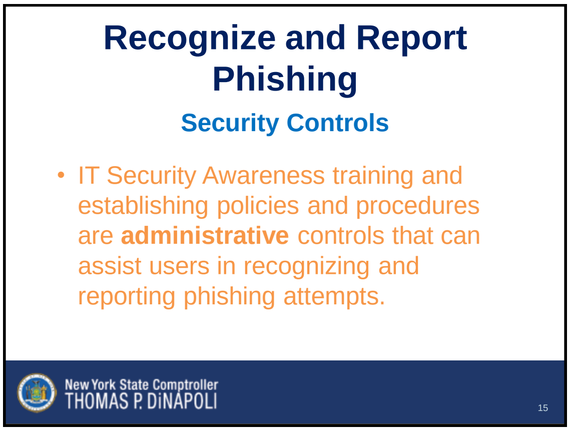
- Social engineering and phishing attacks are **threats** to systems.
- A keylogger, or malicious software installed to track a victim's keystrokes, is an example of a **threat** that a system can be exposed to from a successful phishing attack.



Recognize and Report Phishing

Risk Mitigation

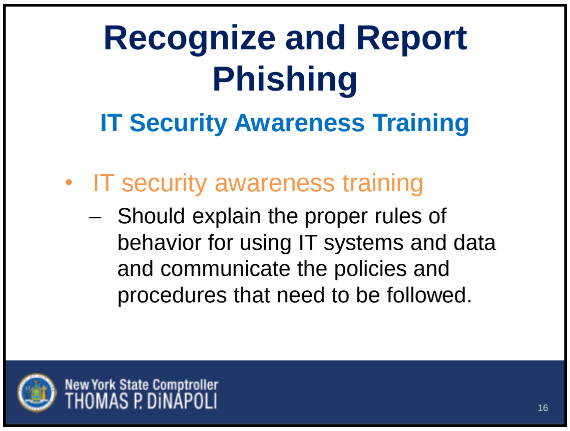
- Conducting appropriate and applicable IT Security Awareness training, including how to spot and report phishing attempts, can help **mitigate** cyber risk.



Recognize and Report Phishing

Security Controls

- IT Security Awareness training and establishing policies and procedures are **administrative** controls that can assist users in recognizing and reporting phishing attempts.



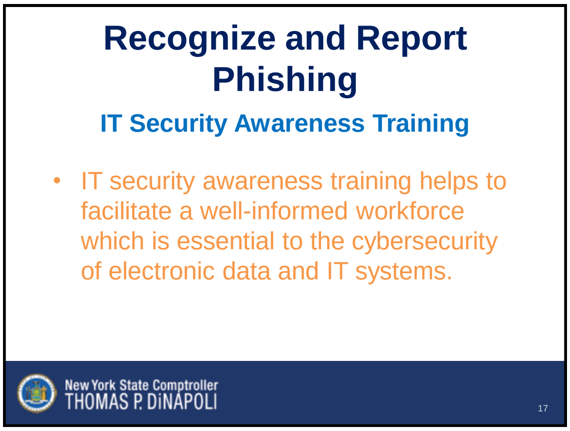
Recognize and Report Phishing

IT Security Awareness Training

- IT security awareness training
  - Should explain the proper rules of behavior for using IT systems and data and communicate the policies and procedures that need to be followed.

New York State Comptroller
THOMAS P. DiNAPOLI

16



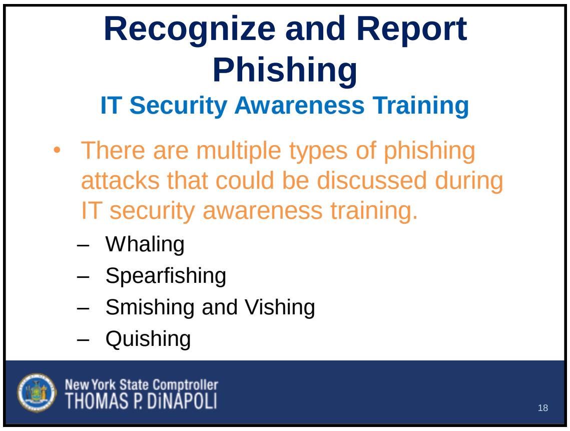
Recognize and Report Phishing

IT Security Awareness Training

- IT security awareness training helps to facilitate a well-informed workforce which is essential to the cybersecurity of electronic data and IT systems.

New York State Comptroller
THOMAS P. DiNAPOLI

17



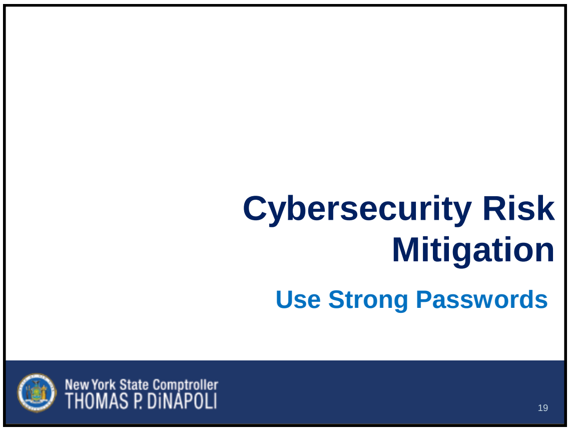
Recognize and Report Phishing

IT Security Awareness Training

- There are multiple types of phishing attacks that could be discussed during IT security awareness training.
  - Whaling
  - Spearfishing
  - Smishing and Vishing
  - Quishing

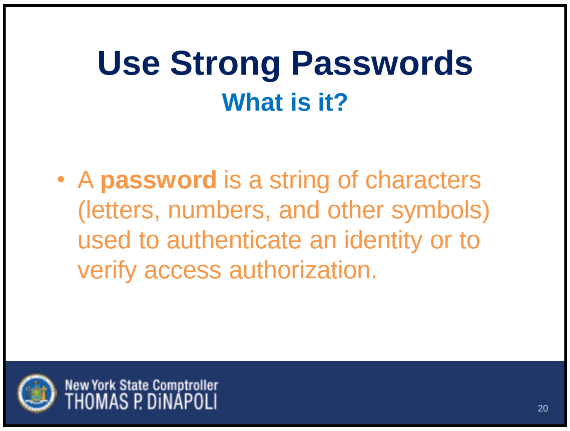
New York State Comptroller
THOMAS P. DiNAPOLI

18



Cybersecurity Risk Mitigation

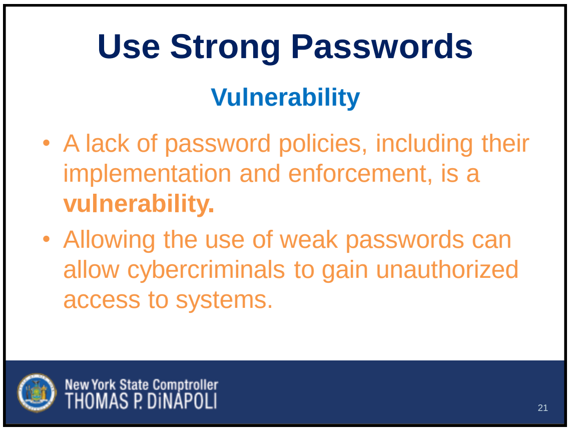
Use Strong Passwords



Use Strong Passwords

What is it?

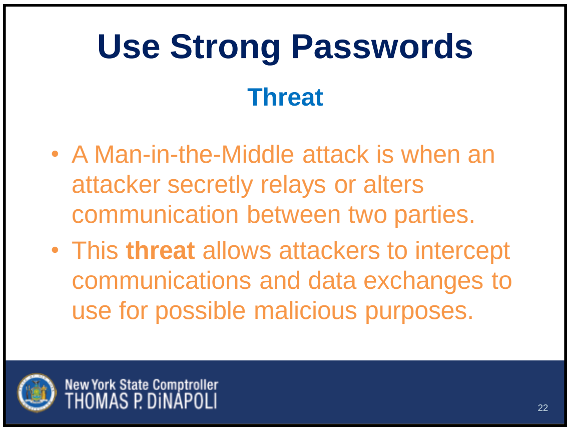
- A **password** is a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.



Use Strong Passwords

Vulnerability

- A lack of password policies, including their implementation and enforcement, is a **vulnerability.**
- Allowing the use of weak passwords can allow cybercriminals to gain unauthorized access to systems.



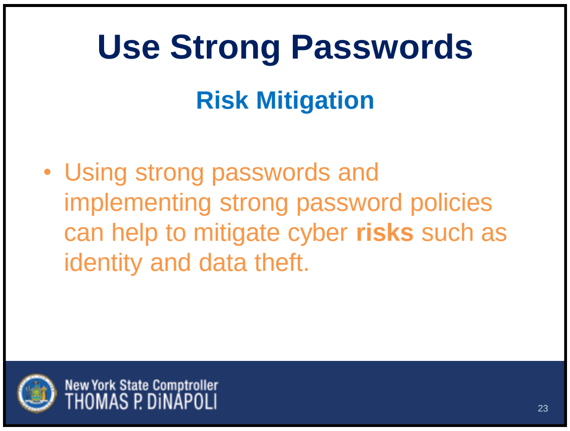
Use Strong Passwords

Threat

- A Man-in-the-Middle attack is when an attacker secretly relays or alters communication between two parties.
- This **threat** allows attackers to intercept communications and data exchanges to use for possible malicious purposes.

New York State Comptroller
THOMAS P. DiNAPOLI

22



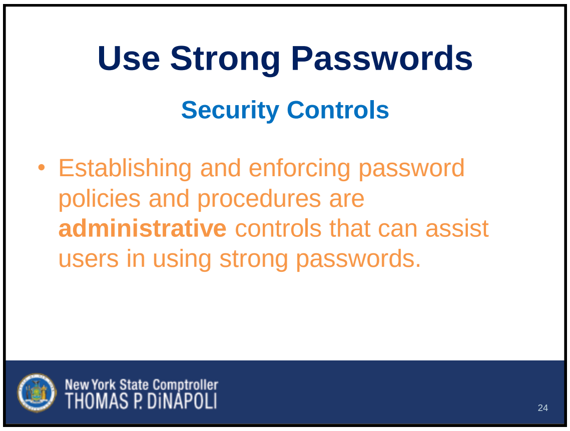
Use Strong Passwords

Risk Mitigation

- Using strong passwords and implementing strong password policies can help to mitigate cyber **risks** such as identity and data theft.

New York State Comptroller
THOMAS P. DiNAPOLI

23



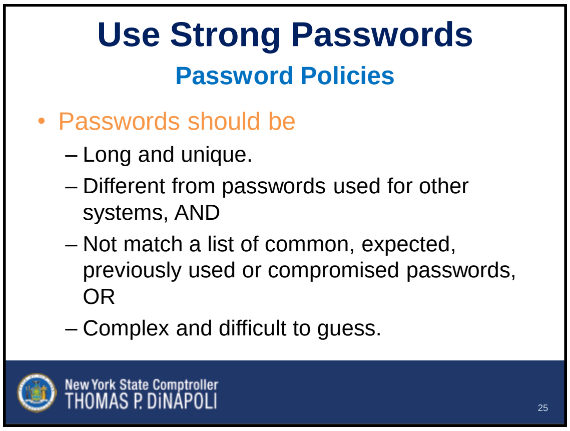
Use Strong Passwords

Security Controls

- Establishing and enforcing password policies and procedures are **administrative** controls that can assist users in using strong passwords.

New York State Comptroller
THOMAS P. DiNAPOLI

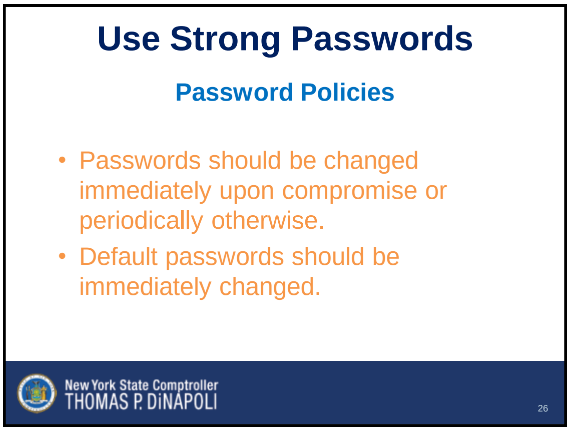
24



Use Strong Passwords

Password Policies

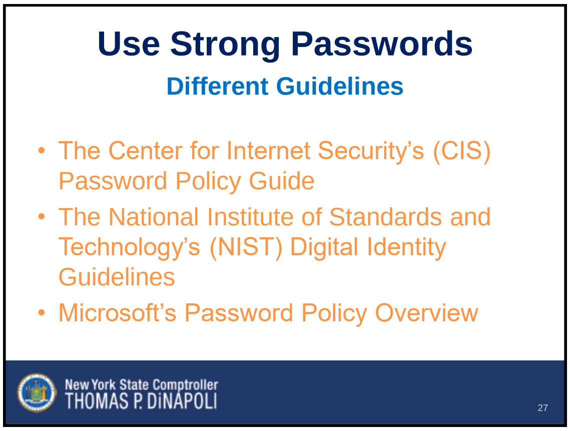
- Passwords should be
  - Long and unique.
  - Different from passwords used for other systems, AND
  - Not match a list of common, expected, previously used or compromised passwords, OR
  - Complex and difficult to guess.



Use Strong Passwords

Password Policies

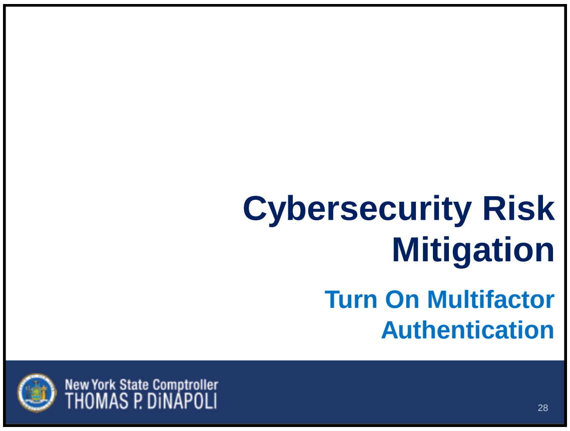
- Passwords should be changed immediately upon compromise or periodically otherwise.
- Default passwords should be immediately changed.



Use Strong Passwords

Different Guidelines

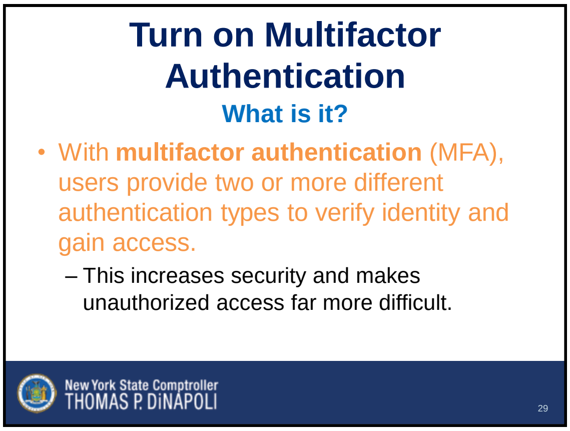
- The Center for Internet Security’s (CIS) Password Policy Guide
- The National Institute of Standards and Technology’s (NIST) Digital Identity Guidelines
- Microsoft’s Password Policy Overview



Cybersecurity Risk Mitigation

Turn On Multifactor Authentication

New York State Comptroller
THOMAS P. DiNAPOLI

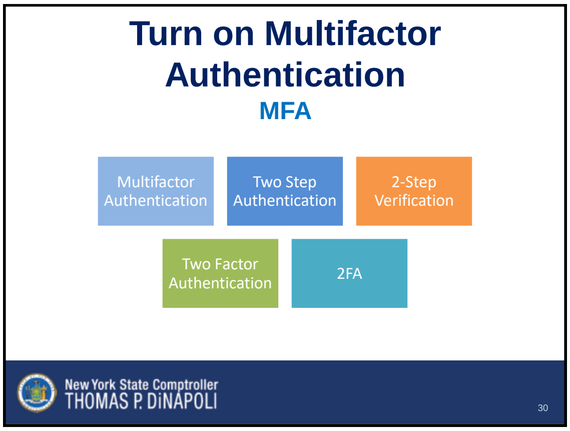


Turn on Multifactor Authentication

What is it?

- With **multifactor authentication** (MFA), users provide two or more different authentication types to verify identity and gain access.
  - This increases security and makes unauthorized access far more difficult.

New York State Comptroller
THOMAS P. DiNAPOLI



Turn on Multifactor Authentication

MFA

Multifactor Authentication

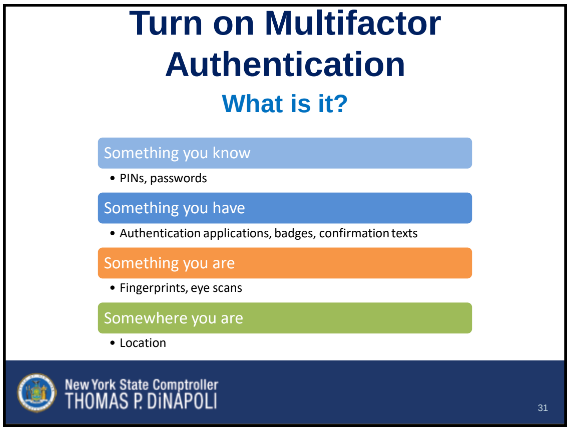
Two Step Authentication

2-Step Verification

Two Factor Authentication

2FA

New York State Comptroller
THOMAS P. DiNAPOLI



Turn on Multifactor Authentication

What is it?

Something you know

- PINs, passwords

Something you have

- Authentication applications, badges, confirmation texts

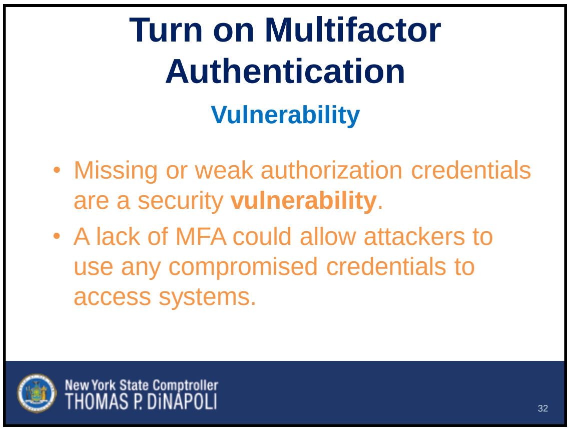
Something you are

- Fingerprints, eye scans

Somewhere you are

- Location

New York State Comptroller
THOMAS P. DiNAPOLI

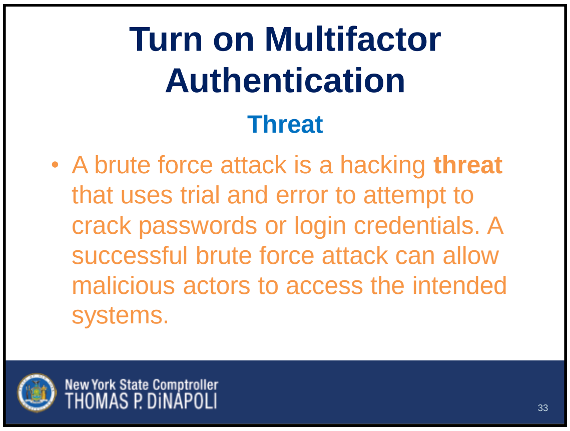


Turn on Multifactor Authentication

Vulnerability

- Missing or weak authorization credentials are a security **vulnerability**.
- A lack of MFA could allow attackers to use any compromised credentials to access systems.

New York State Comptroller
THOMAS P. DiNAPOLI

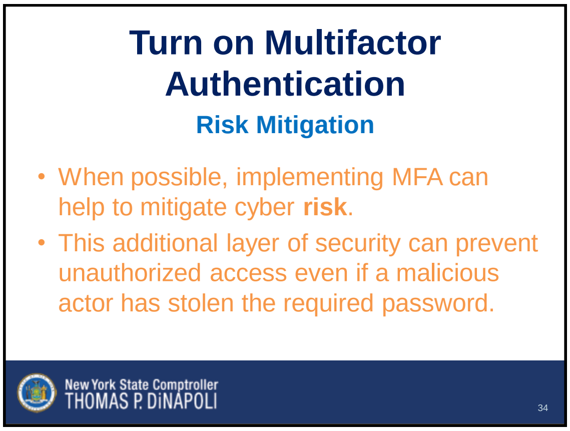


Turn on Multifactor Authentication

Threat

- A brute force attack is a hacking **threat** that uses trial and error to attempt to crack passwords or login credentials. A successful brute force attack can allow malicious actors to access the intended systems.

New York State Comptroller
THOMAS P. DiNAPOLI



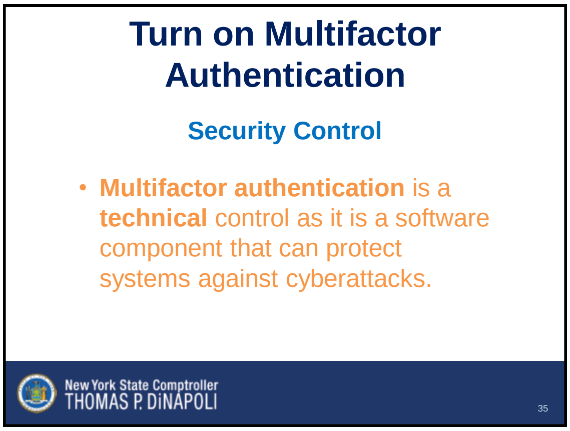
Turn on Multifactor Authentication

Risk Mitigation

- When possible, implementing MFA can help to mitigate cyber **risk**.
- This additional layer of security can prevent unauthorized access even if a malicious actor has stolen the required password.

New York State Comptroller
THOMAS P. DiNAPOLI

34



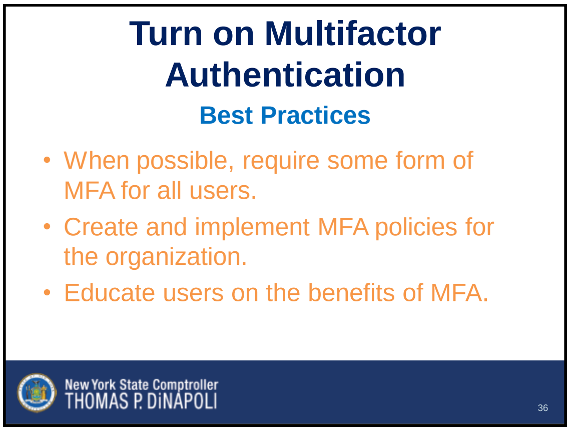
Turn on Multifactor Authentication

Security Control

- **Multifactor authentication** is a **technical** control as it is a software component that can protect systems against cyberattacks.

New York State Comptroller
THOMAS P. DiNAPOLI

35



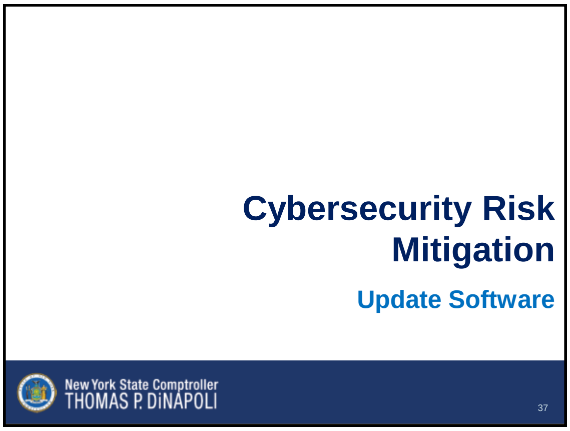
Turn on Multifactor Authentication

Best Practices

- When possible, require some form of MFA for all users.
- Create and implement MFA policies for the organization.
- Educate users on the benefits of MFA.

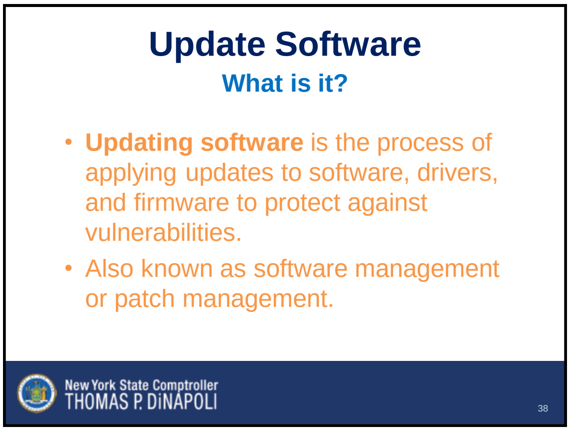
New York State Comptroller
THOMAS P. DiNAPOLI

36



Cybersecurity Risk Mitigation

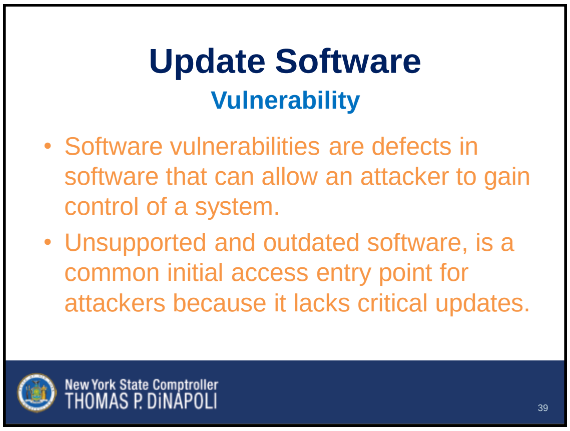
Update Software



Update Software

What is it?

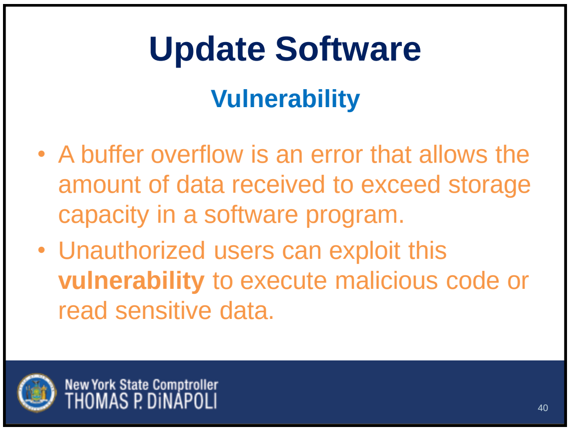
- **Updating software** is the process of applying updates to software, drivers, and firmware to protect against vulnerabilities.
- Also known as software management or patch management.



Update Software

Vulnerability

- Software vulnerabilities are defects in software that can allow an attacker to gain control of a system.
- Unsupported and outdated software, is a common initial access entry point for attackers because it lacks critical updates.



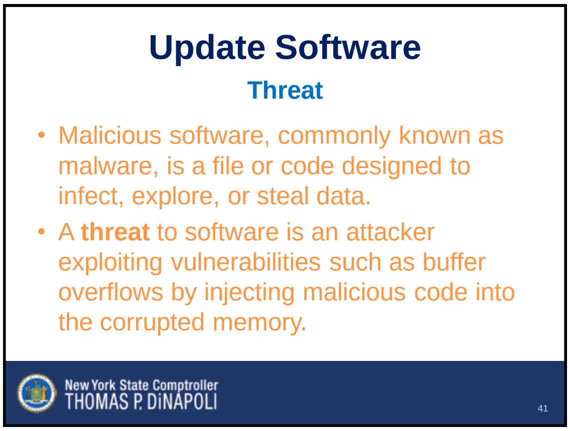
Update Software

Vulnerability

- A buffer overflow is an error that allows the amount of data received to exceed storage capacity in a software program.
- Unauthorized users can exploit this **vulnerability** to execute malicious code or read sensitive data.

New York State Comptroller
THOMAS P. DiNAPOLI

40



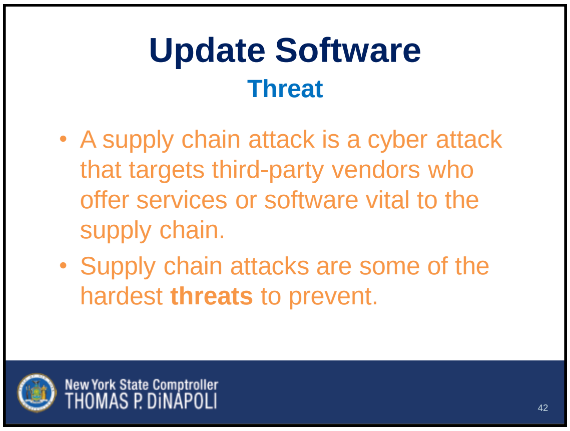
Update Software

Threat

- Malicious software, commonly known as malware, is a file or code designed to infect, explore, or steal data.
- A **threat** to software is an attacker exploiting vulnerabilities such as buffer overflows by injecting malicious code into the corrupted memory.

New York State Comptroller
THOMAS P. DiNAPOLI

41



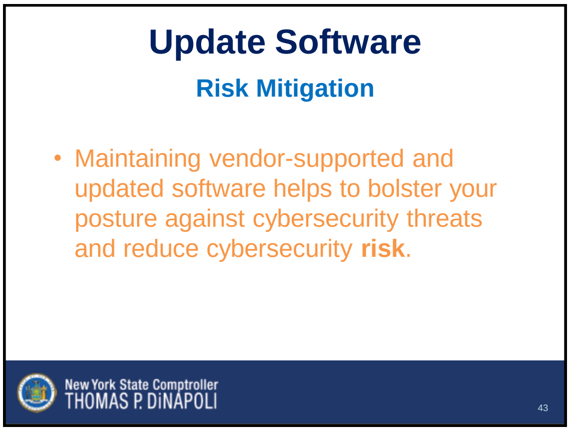
Update Software

Threat

- A supply chain attack is a cyber attack that targets third-party vendors who offer services or software vital to the supply chain.
- Supply chain attacks are some of the hardest **threats** to prevent.

New York State Comptroller
THOMAS P. DiNAPOLI

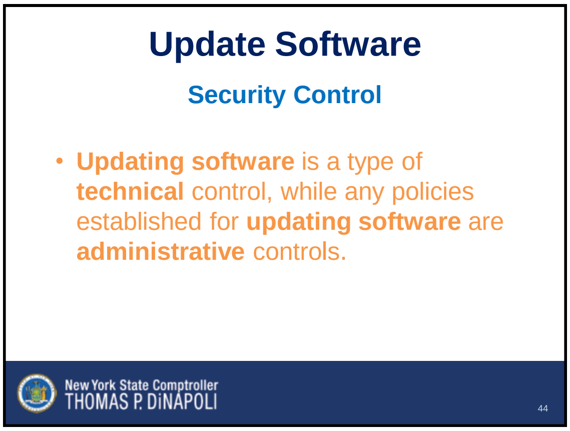
42



Update Software

Risk Mitigation

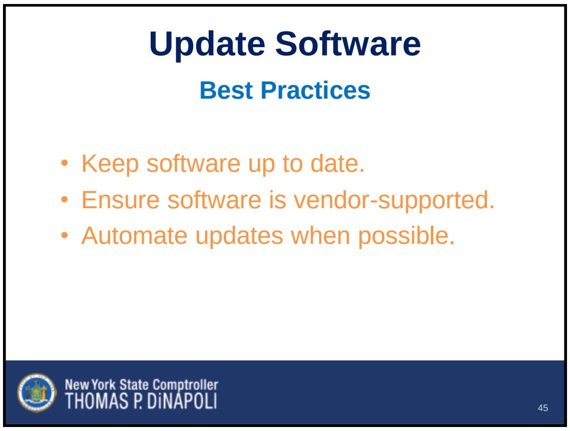
- Maintaining vendor-supported and updated software helps to bolster your posture against cybersecurity threats and reduce cybersecurity **risk**.



Update Software

Security Control

- **Updating software** is a type of **technical** control, while any policies established for **updating software** are **administrative** controls.



Update Software

Best Practices

- Keep software up to date.
- Ensure software is vendor-supported.
- Automate updates when possible.

Update Software

Best practices

- Use antivirus software, or similar malware protection mechanism.
  - While malware protection can help detect malicious software, it does not preclude you from actively managing your software.

Cybersecurity

Resources

Information Technology Governance

Local Government Management Guide

Information Technology Governance

Security Self-Assessment

Cyber Profile

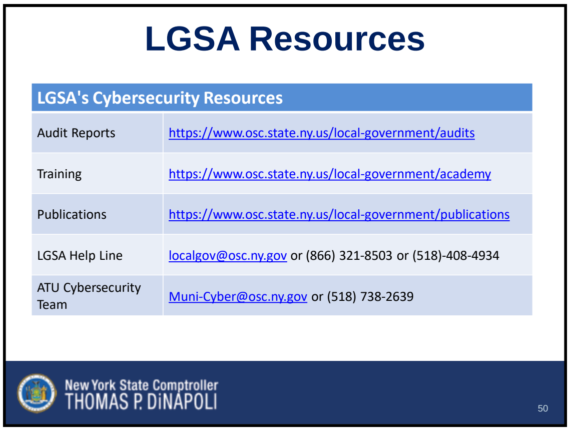
Division of Local Government and School Accountability

Cyber Profile

October 2023

New York State Comptroller
THOMAS P. DiNAPOLI

49

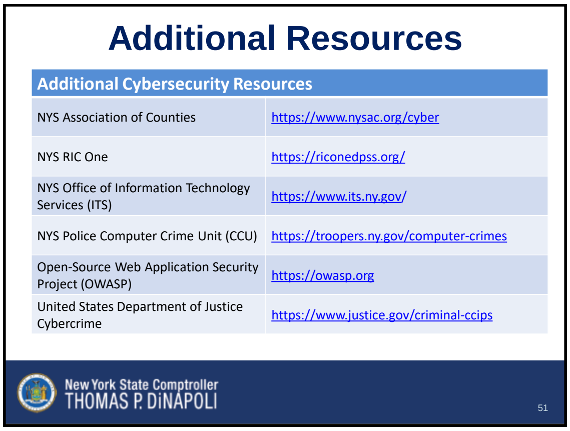


LGSA Resources

LGSA's Cybersecurity Resources	
Audit Reports	https://www.osc.state.ny.us/local-government/audits
Training	https://www.osc.state.ny.us/local-government/academy
Publications	https://www.osc.state.ny.us/local-government/publications
LGSA Help Line	localgov@osc.ny.gov or (866) 321-8503 or (518)-408-4934
ATU Cybersecurity Team	Muni-Cyber@osc.ny.gov or (518) 738-2639

New York State Comptroller
THOMAS P. DiNAPOLI

50

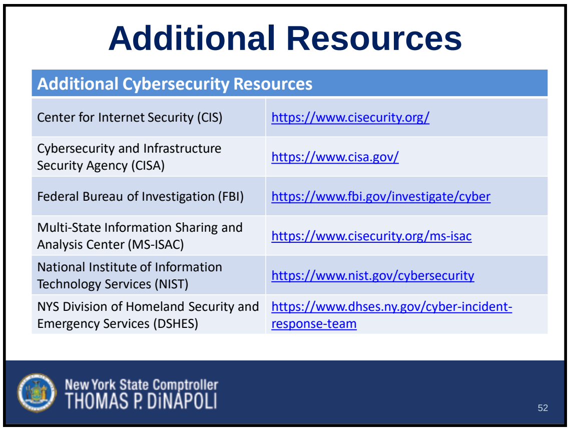


Additional Resources

Additional Cybersecurity Resources	
NYS Association of Counties	https://www.nysac.org/cyber
NYS RIC One	https://riconedpss.org/
NYS Office of Information Technology Services (ITS)	https://www.its.ny.gov/
NYS Police Computer Crime Unit (CCU)	https://troopers.ny.gov/computer-crimes
Open-Source Web Application Security Project (OWASP)	https://owasp.org
United States Department of Justice Cybercrime	https://www.justice.gov/criminal-ccips

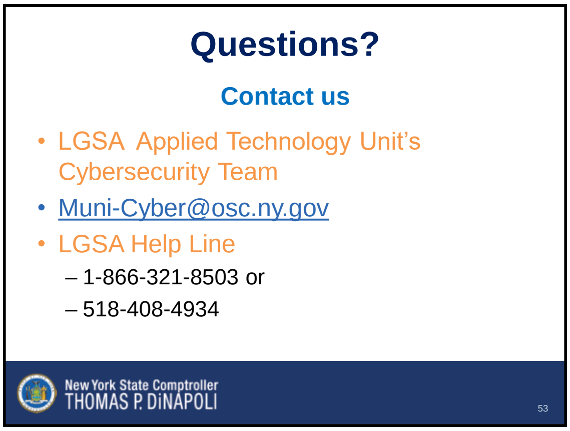
New York State Comptroller
THOMAS P. DiNAPOLI

51



Additional Resources

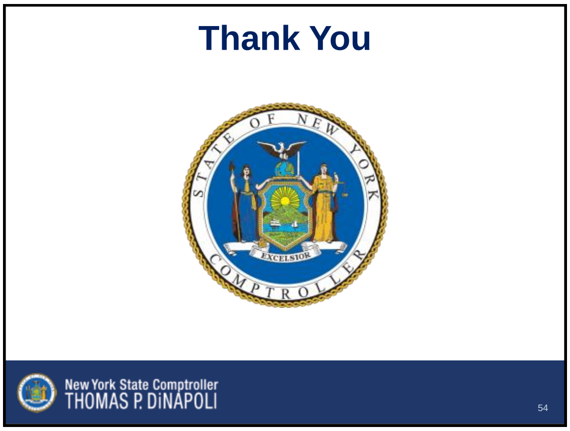
Additional Cybersecurity Resources	
Center for Internet Security (CIS)	https://www.cisecurity.org/
Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/
Federal Bureau of Investigation (FBI)	https://www.fbi.gov/investigate/cyber
Multi-State Information Sharing and Analysis Center (MS-ISAC)	https://www.cisecurity.org/ms-isac
National Institute of Information Technology Services (NIST)	https://www.nist.gov/cybersecurity
NYS Division of Homeland Security and Emergency Services (DSHES)	https://www.dhses.ny.gov/cyber-incident-response-team



Questions?

Contact us

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



Thank You

STATE OF NEW YORK
EXCELSIOR
COMPTROLLER