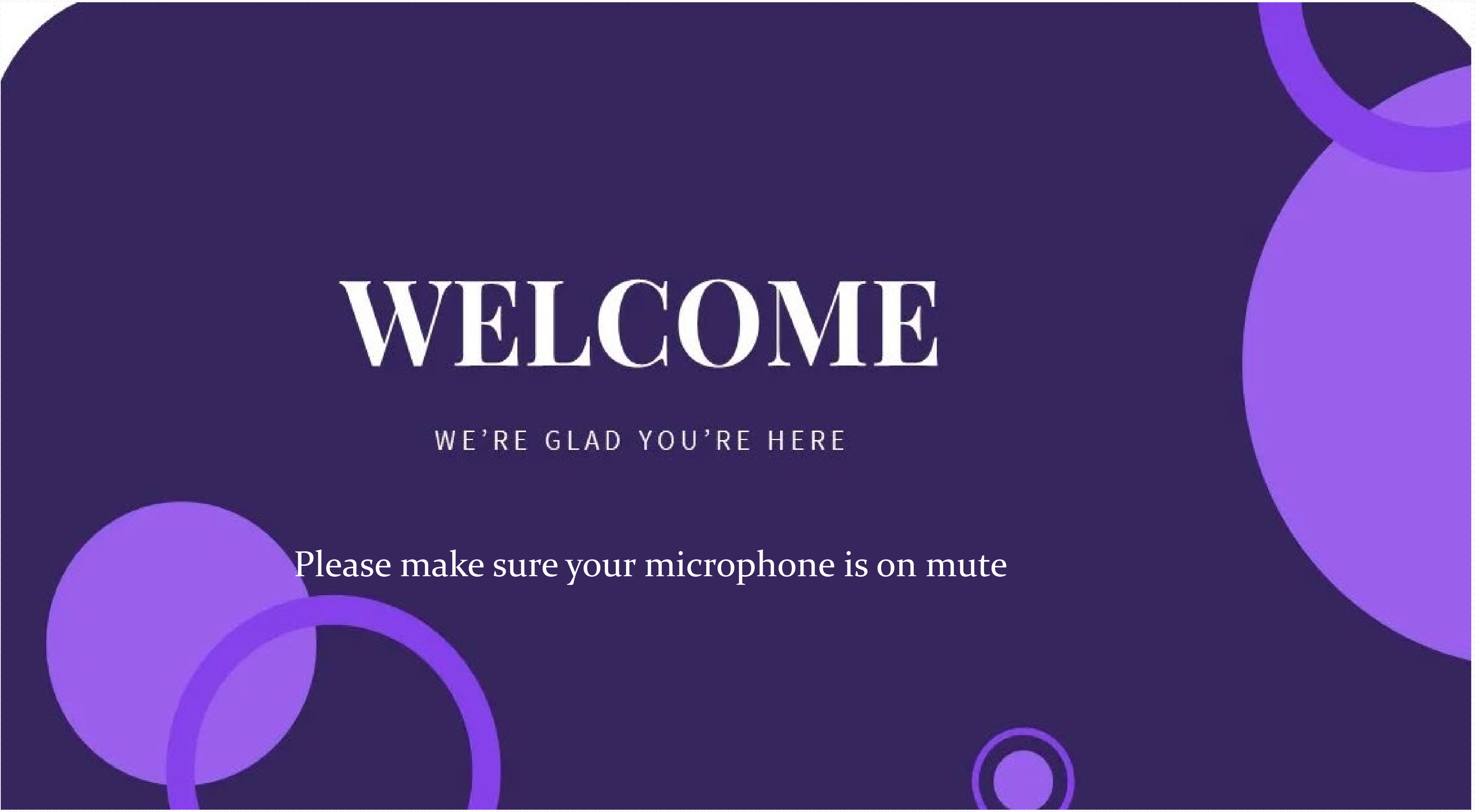


WELCOME

WE'RE GLAD YOU'RE HERE

Please make sure your microphone is on mute

STAY SAFE: PROTECT YOUR IT SYSTEMS FROM VULNERABILITIES

Legal Services Corporation
Office of Inspector General
September 28, 2023

Why Are We Here?

Overview

- I. Mission & Purpose of the Assessments
- II. Background
- III. What we Found
- IV. What is Recommended
- V. Summary and Resources

OIG Mission
Assure-Advise-Anticipate

- Promote economy, efficiency, and effectiveness in LSC and LSC grantee operations

- Prevent and detect fraud, waste, and abuse

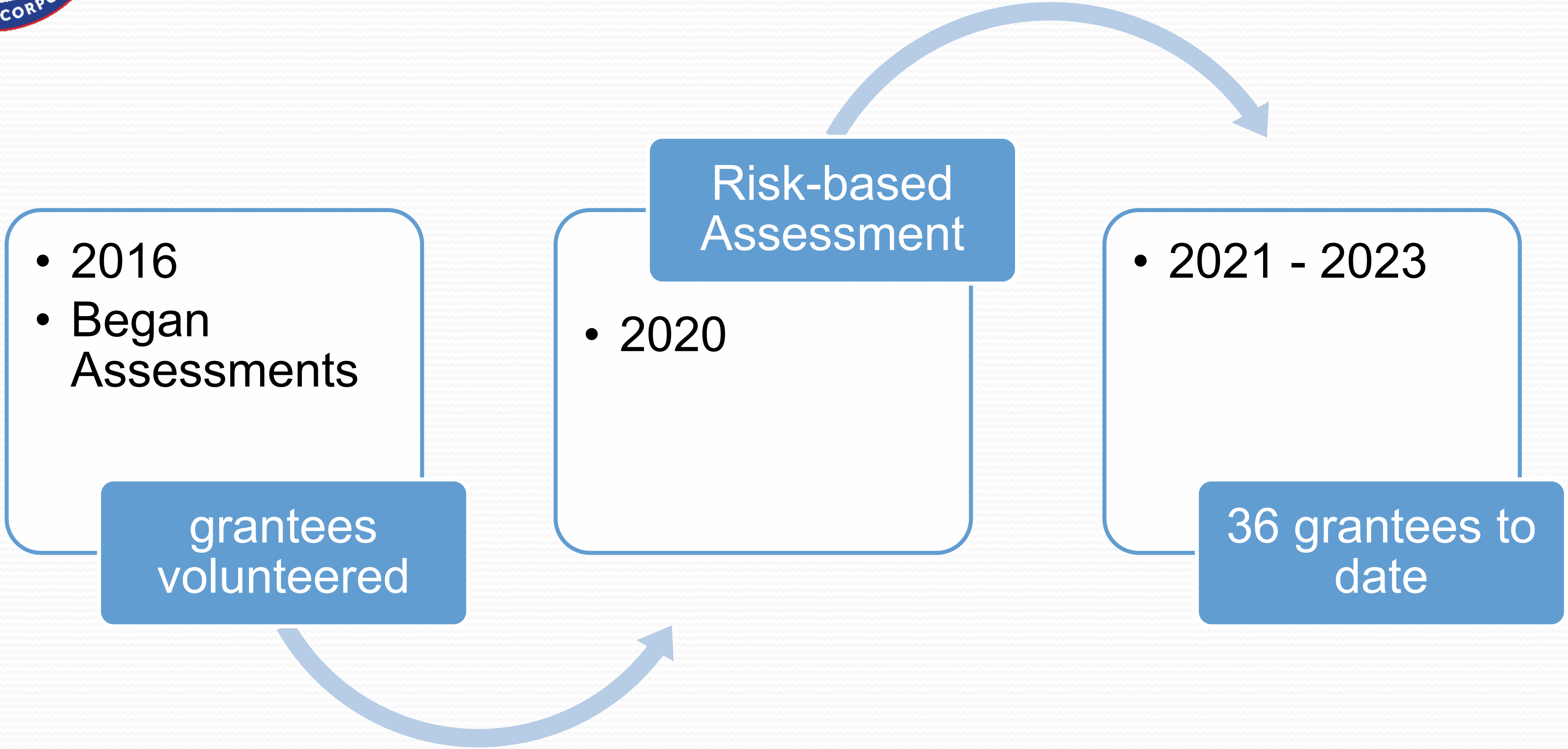
IT Vulnerability Assessments

- Test for potential vulnerabilities in computer network architecture, technologies, and processes.

- Identify vulnerabilities outside of the network that can be exploited.

- Identify vulnerabilities inside the network that can be exploited.

Background



- 2016
- Began Assessments

grantees volunteered

Risk-based Assessment

- 2020

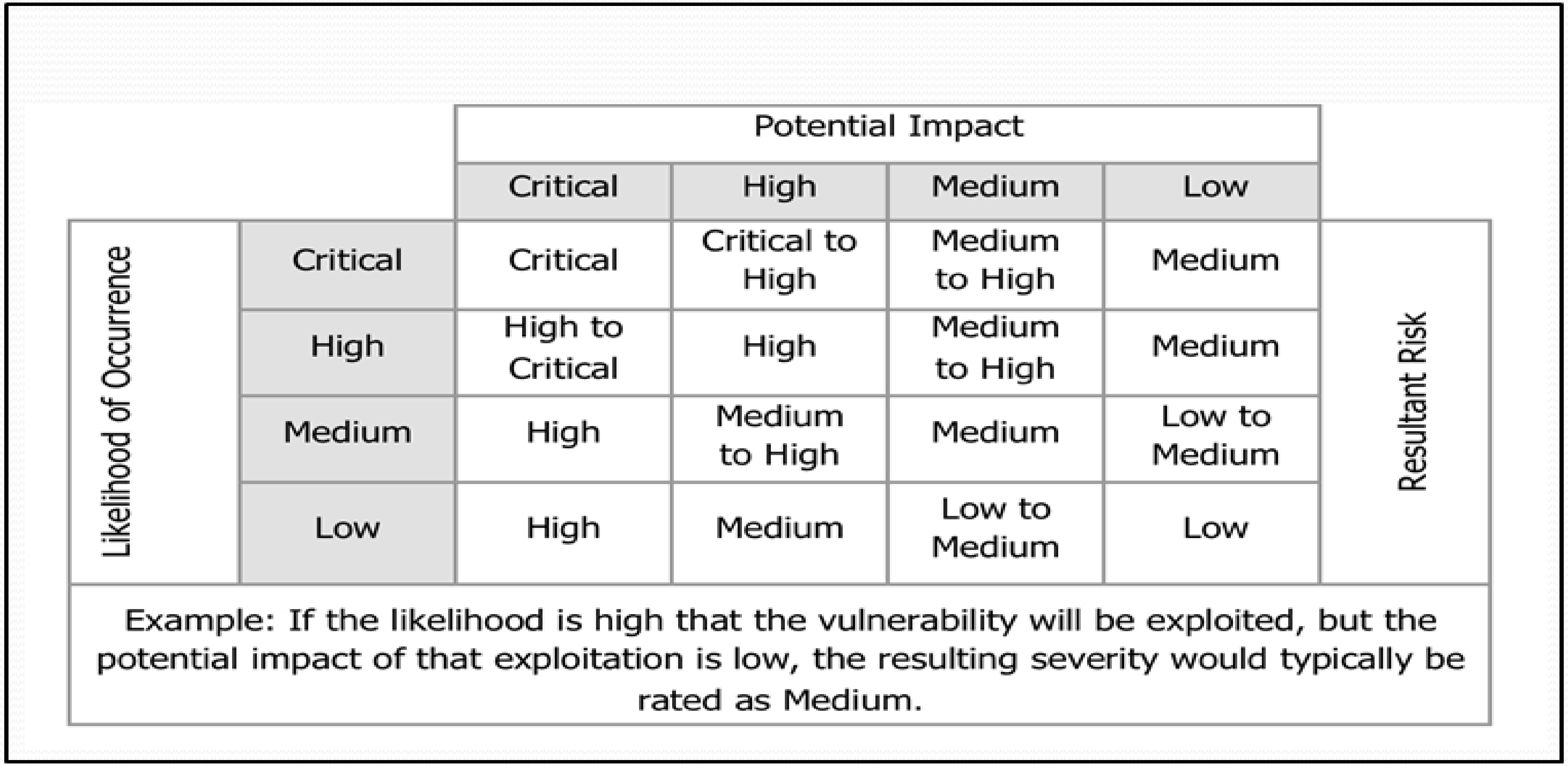
- 2021 - 2023

36 grantees to date

Annual Summary Report

- Summarizes common findings
- Provides recommendations to mitigate the findings
- Offers IT Security Best Practices

Assigning the Severity of a Vulnerability



		Potential Impact				
		Critical	High	Medium	Low	
Likelihood of Occurrence	Critical	Critical	Critical to High	Medium to High	Medium	Resultant Risk
	High	High to Critical	High	Medium to High	Medium	
	Medium	High	Medium to High	Medium	Low to Medium	
	Low	High	Medium	Low to Medium	Low	

Example: If the likelihood is high that the vulnerability will be exploited, but the potential impact of that exploitation is low, the resulting severity would typically be rated as Medium.

Critical Vulnerability

- Operating Systems and Third-Party Software that is unpatched or unsupported
  - No longer receive vendor support
  - May not receive security updates and patches

High Vulnerabilities

- *Simple Network Management Protocol* (SNMP) is not secure.

Protocol to manage and monitor network devices. A vulnerability exists if messages are sent unencrypted. An attacker can steal login credentials or take control of SNMP-enabled devices.

- *Intelligent Platform Management Interface* (IPMI) is not secure.

A hardware interface used to remotely manage and monitor server health. If insecure, hackers can reboot the system, install a new OS, and access data.

- *Secure Socket Layer/Transport Layer Security* (SSL/TLS) is not secure.

SSL and TLS are used to secure data transmission to keep transmissions private. Hackers can take advantage of old versions of SSL and TLS to intercept the traffic, read the exchange in plain text, and use it for man-in-the-middle or eavesdropping attacks.

Immediate Recommendations

- Apply operating system and software updates.
- Update and/or patch third party firmware and software.
- Segment network boundaries using a firewall or router and apply firewall rules or access control lists to allow or deny traffic between zones.
- When possible, remove unnecessary or unsupported software.
- Develop and maintain an approved port, protocols, and services whitelist, close undocumented open ports.
- Create inventory and maintain asset lists and network architecture diagrams.

Long-Term Recommendations

- Routinely conduct vulnerability scanning
- Implement a comprehensive patch management program to apply all available patches, firmware, and software updates.
- Ensure that all communications at the external managed interfaces are properly monitored according to the organization’s overall security architecture.

Long-Term Recommendations-continued

- Research and employ zero-trust architectures (zero-trust acknowledges the need to end reliance on a singular authentication).
- Conduct routine manual and automated device inventories.
- Establish clear physical and logical separation between systems and personally owned devices.

Best Practices

- Implement a defense-in-depth strategy. Suggested core layers include:
  - Strong, complex passwords
  - Antivirus software
  - Secure gateway
  - Firewall
- Backup and Recovery
- The principle of least privilege, or give users the minimum access level or permissions needed to do their job

Best Practices-continued

- Add additional security layers such as:

  - Two-factor authentication (2FA) or multi-factor authentication (MFA)
  - Intrusion detection and prevention systems
  - Endpoint detection and response (EDR)
  - Network segmentation
  - Encryption
  - Data loss prevention
  - Virtual Private Networks (VPN)

Key Take-Aways

- Grantee networks did not present a significant risk of exposure from outside the network.
- Vulnerabilities were internal to the network (an attacker must get into the network to exploit the vulnerabilities).
- The common critical finding among grantees is out-of-date Operating Systems (OS) and applications, and unpatched or out of date software.
- Take proactive measures to improve your organization’s security posture
- Good News! - These vulnerabilities can be remediated .

Resources for LSC Grantees

Request an ITVA by sending an email to Audits@oig.lsc.gov

Additional LSC and OIG guidance on information technology security is available on the OIG and LSC Website:

- Cyber Security Resources | OFFICE OF INSPECTOR GENERAL (lsc.gov)
- Fraud Alerts and Best Practices | OFFICE OF INSPECTOR GENERAL (lsc.gov)
- LSC Technology Baselines (Issued by LSC President, Ron Flagg in August 2023; security best practices are in Chapter 3) *Technology Baselines: Technologies that Should Be in Place in a Legal Office Today*

Questions?

If you have additional questions, please send them to:

Audits@oig.lsc.gov