GLBA FOR INSTITUTIONS OF HIGHER EDUCATION - NASFAA

U.S. Department of Education
Office of Student Financial Aid

Presenter: Margaret M Glick

U.S. Department of Education

June 14, 2023

Information presented today is on background and not for direct attribution.

WE WILL DISCUSS

1. The GLBA* Safeguards Rule
2. What Can You Do?
3. What Can Your I.T. Department Do?
4. Expanded Elements
5. Questions
6. Appendix/Resources

**Gramm-Leach-Bliley Act*

THE GLBA SAFEGUARDS RULE

PREVIOUS GLBA SAFEGUARD REQUIREMENTS

- Designate IT Point of Contact (POC)
- Perform Risk Assessment
- Document Safeguards

NEW GLBA SAFEGUARDS RULE

The institution is required to **develop**, **implement**, and **maintain** an information security program

The Information Security Program protects students' information with **administrative**, **technical**, and **physical** safeguards

The information security plan strives to:

- Ensure security and confidentiality
- Protect against anticipated threats or hazards
- Protect against unauthorized access

YOUR PROGRAM IS SCALABLE

It must be appropriate for:

The size and complexity of your institution

YOUR PROGRAM IS SCALABLE

It must be appropriate for:

The size and complexity of your institution

The nature and scope of your activities

YOUR PROGRAM IS SCALABLE

It must be appropriate for:

The size and complexity of your institution

The nature and scope of your activities

The sensitivity of the information

EXPANSION OF GLBA ELEMENTS

WHAT CAN I DO?

REDUCING RISK – FAA'S

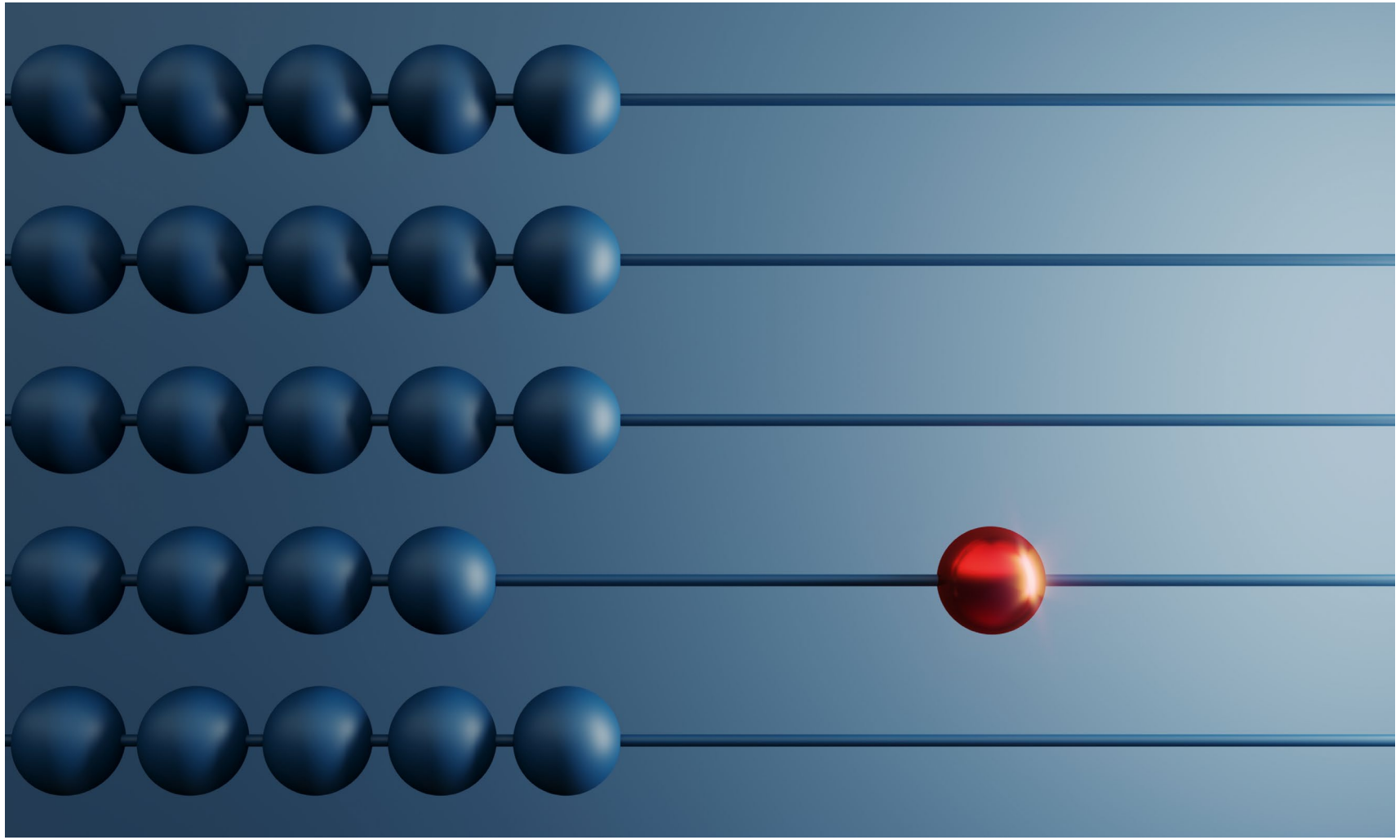
1. Train your staff
2. Encourage Multi-Factor Authentication (MFA)
3. Know what you have and where you have it
4. Encrypt information in transit
5. Dispose of personal information securely
6. Educate and Encourage
7. Prepare for an incident
8. Did I mention MFA?

TRAIN YOUR STAFF

ENCOURAGE MULTI-FACTOR AUTHENTICATION

KNOW WHAT YOU HAVE AND WHERE YOU HAVE IT

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

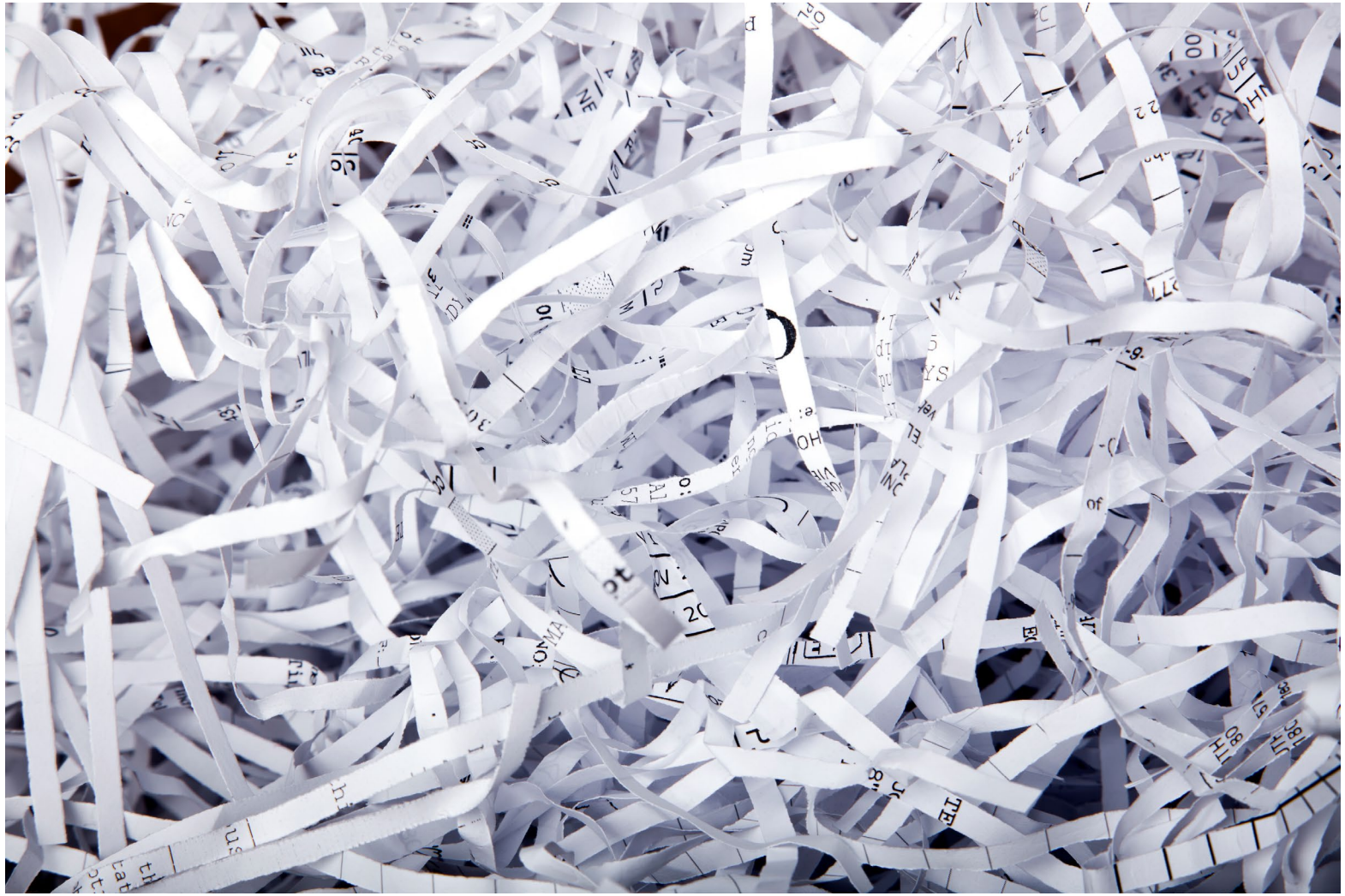


ENCRYPT DATA ON YOUR SYSTEM AND IN TRANSIT

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

Gmail	Outlook	MS Office Docs	PDFs
• Click Compose. • Click the lock icon placed on the right of the recipient. • Set a passcode and an expiration date. You'll get the passcode via SMS or email. • Click Save.	• Compose an email. • Click File. • Click Properties. • Click Security Settings. • Click "Encrypt message contents and attachments." • Click Send.	• Click Info from the File drop-down menu. • Click Protect Document. • From the pop-up menu, click Encrypt with Password. • Type in and verify your password.	• Open the PDF file. • Click File. • Click Info. • Click Protect Document. • Click Encrypt with Password. • Type in and verify your password.

DISPOSE OF DATA SECURELY



STRONGLY ENCOURAGE LEADERSHIP

PREPARE FOR AN INCIDENT

WHAT CAN I.T. DO?

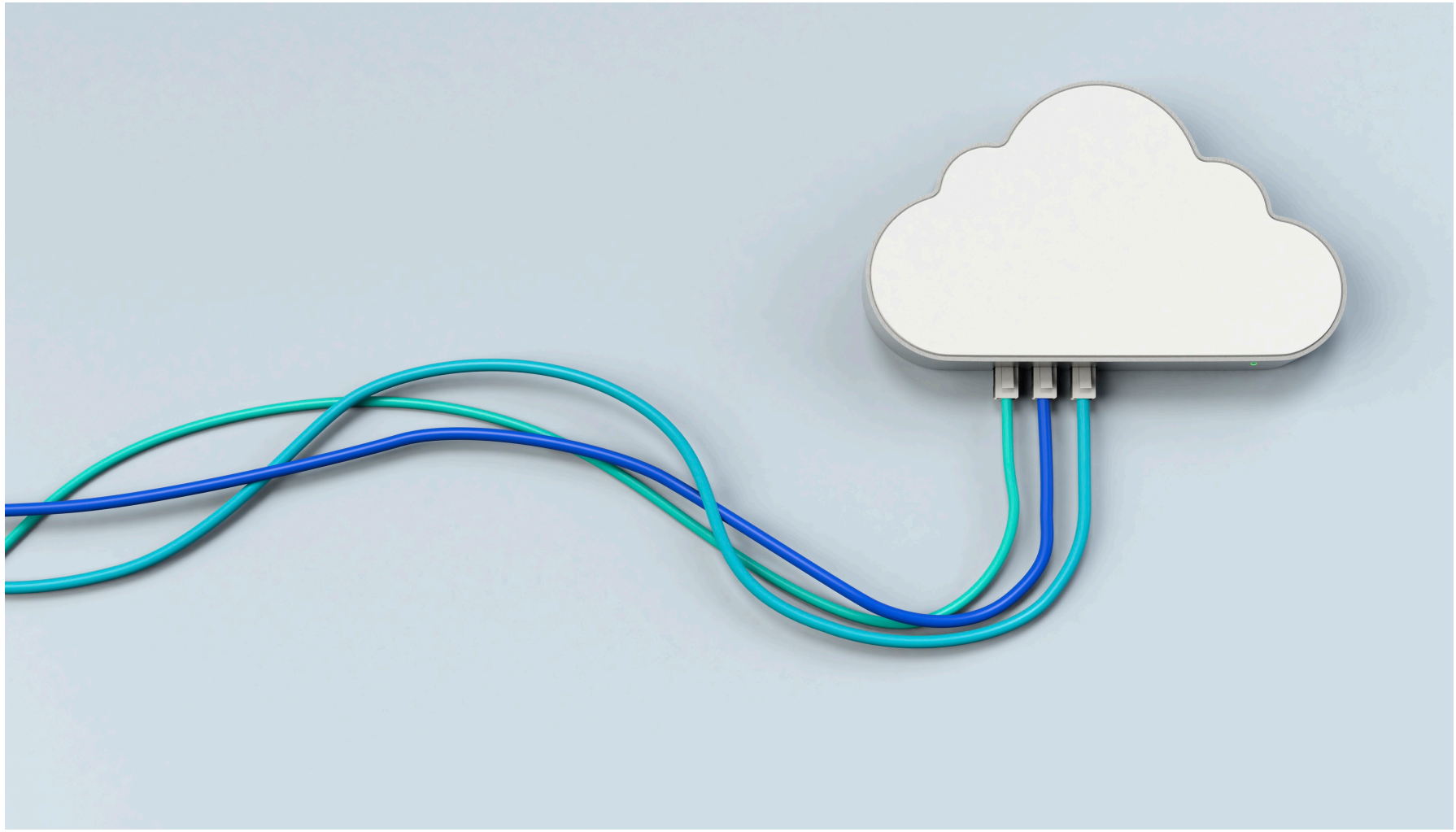
REDUCING RISK – IT DEPARTMENTS

1. CONDUCT A RISK ASSESSMENT
2. DESIGN AND IMPLEMENT SAFEGUARDS
3. REGULARLY MONITOR AND TEST
4. MONITOR SERVICE PROVIDERS
5. DESIGNATE QUALIFIED INDIVIDUAL
6. KEEP YOUR SECURITY CURRENT
7. WRITE AN INCIDENT RESPONSE PLAN

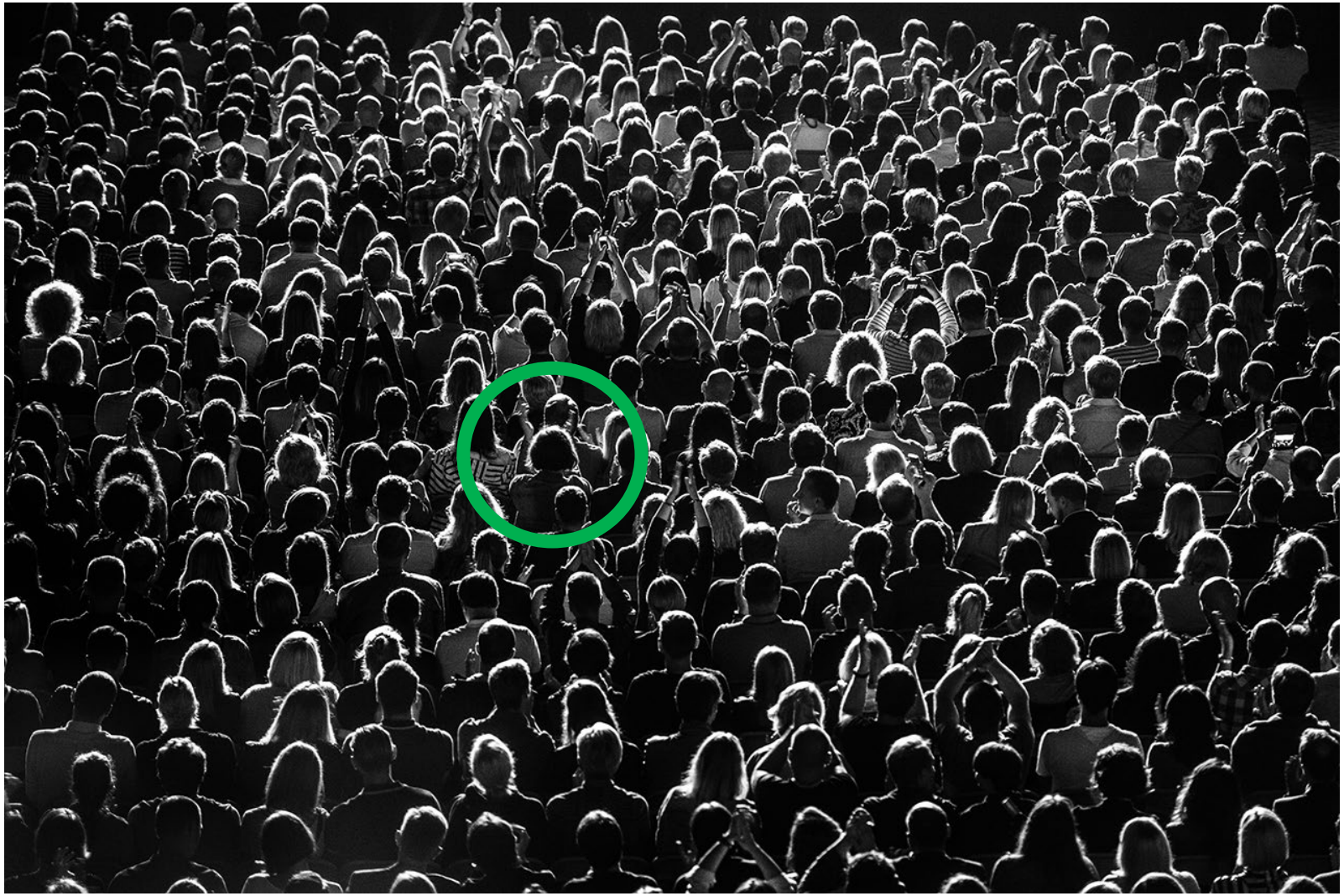
DESIGN AND IMPLEMENT SAFEGUARDS

REGULARLY MONITOR AND TEST

MONITOR SERVICE PROVIDERS



DESIGNATE A QUALIFIED INDIVIDUAL



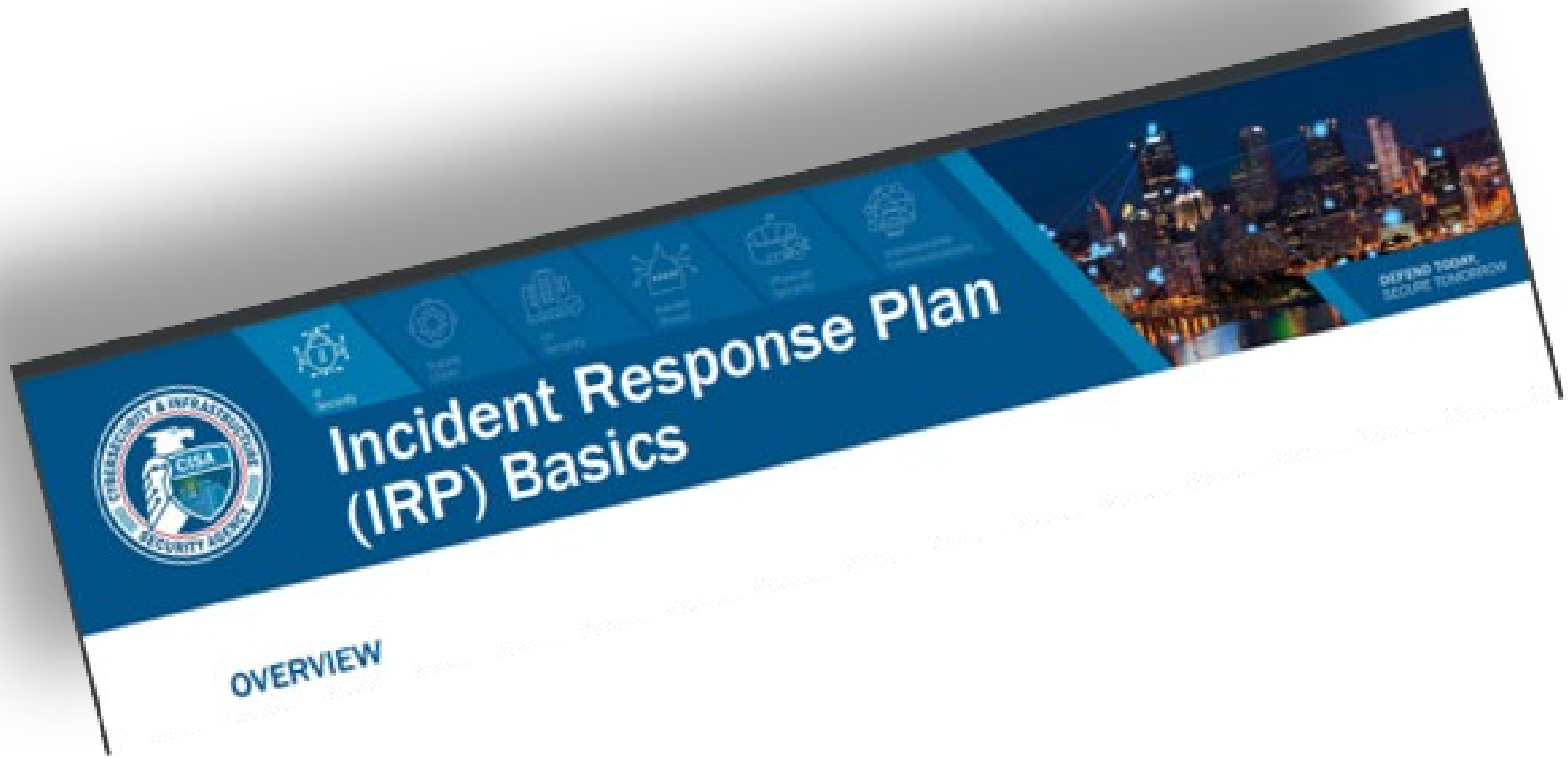
KEEP YOUR SECURITY CURRENT

TWO IMPORTANT ELEMENTS TO REDUCE RISK

TWO HIGHLIGHTED ELEMENTS

CONDUCT A RISK ASSESSMENT

WRITE AN INCIDENT RESPONSE PLAN



YOUR INCIDENT RESPONSE PLAN

- ✓ Internal processes
- ✓ Roles
- ✓ Communications
- ✓ A process to fix weaknesses
- ✓ Procedures for documentation
- ✓ A post-mortem

DISPLAY THE BADGE YOU EARNED

QUESTIONS?

Report breaches to:

- FSASchoolCyberSafety@ed.gov
- OR use the Cybersecurity Breach Intake Form

IHE CYBERSECURITY NEWSLETTER

- Actionable Information
- Sent Quarterly to 20,000+ IT and Compliance Pros at IHEs
- To sign up and receive FSA's new cybersecurity newsletter, please email FSASchoolCyberSafety@ed.gov with the subject line: "Send me the FSA Cybersecurity Newsletter for IHEs."

APPENDIX

WHERE CAN I FIND MORE INFORMATION?

- More information regarding GLBA requirements is available at The Federal Register and at the Federal Trade Commission (FTC)
- Additional guidance can be found in the Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements electronic announcement.
- Find additional cybersecurity resources on the FSA Partner Connect Cybersecurity page.

FSA CYBERSECURITY WEBSITE
HTTPS://FSAPARTNERS.ED.GOV/TITLE-IV-PROGRAM-ELIGIBILITY/CYBERSECURITY

FTC GLBA GUIDANCE
HTTPS://WWW.FTC.GOV/BUSINESS-GUIDANCE/PRIVACY-SECURITY/GRAMM-LEACH-BLILEY-ACT

NIST CYBERSECURITY FRAMEWORK
HTTPS://WWW.NIST.GOV/CYBERFRAMEWORK

CISA RESOURCES
HTTPS://WWW.CISA.GOV/CYBERSECURITY

TEXT OF THE FTC SAFEGAURDS RULE:
HTTPS://WWW.ECFR.GOV/CURRENT/TITLE-16/CHAPTER-I/SUBCHAPTER-C/PART-314

HOW CAN MY INSTITUTION PREPARE?

- Review guidance on conducting a risk assessment, creating an incident response plan, and building an Information Security Program.