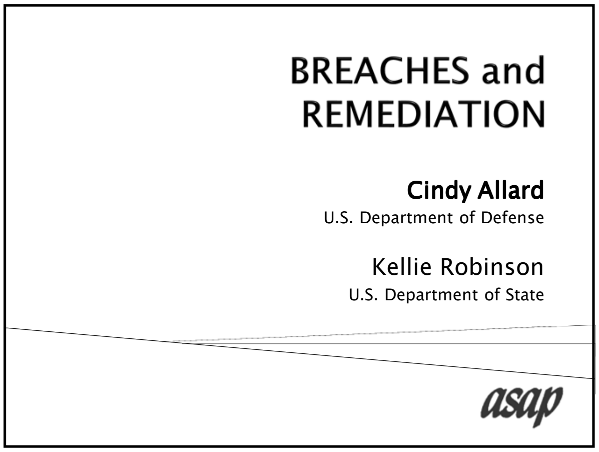
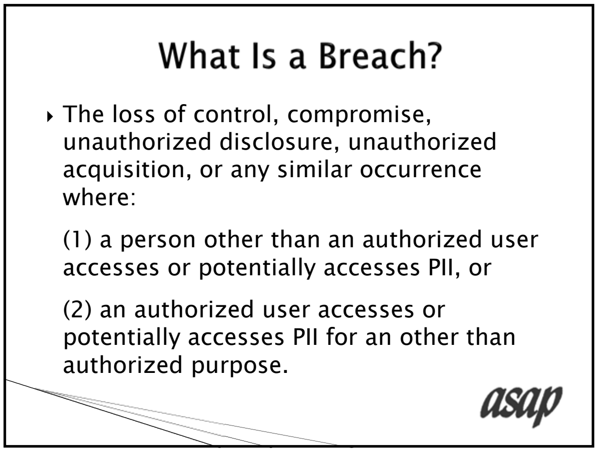


BREACHES and REMEDIATION

Cindy Allard
U.S. Department of Defense

Kellie Robinson
U.S. Department of State

asap



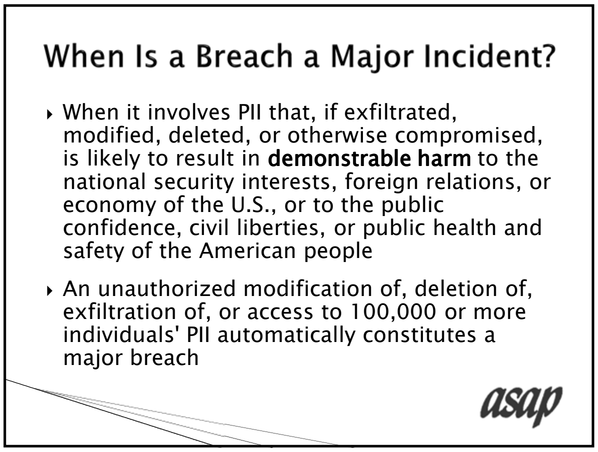
What Is a Breach?

- The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

  (1) a person other than an authorized user accesses or potentially accesses PII, or

  (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose.

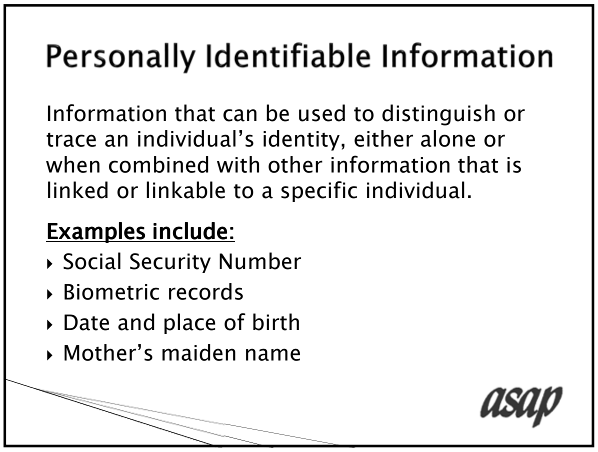
asap



When Is a Breach a Major Incident?

- When it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in **demonstrable harm** to the national security interests, foreign relations, or economy of the U.S., or to the public confidence, civil liberties, or public health and safety of the American people
- An unauthorized modification of, deletion of, exfiltration of, or access to 100,000 or more individuals' PII automatically constitutes a major breach

asap



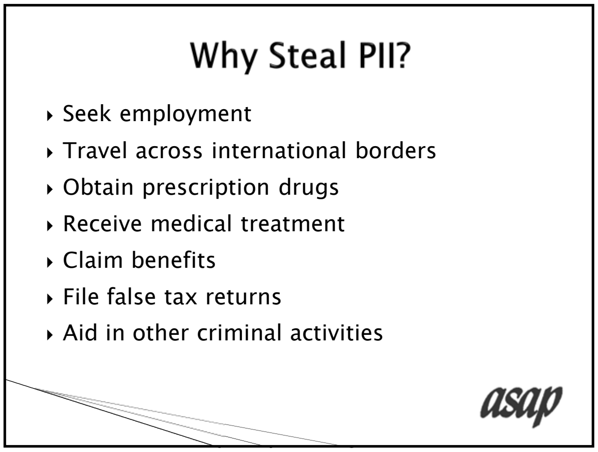
Personally Identifiable Information

Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Examples include:

- Social Security Number
- Biometric records
- Date and place of birth
- Mother's maiden name

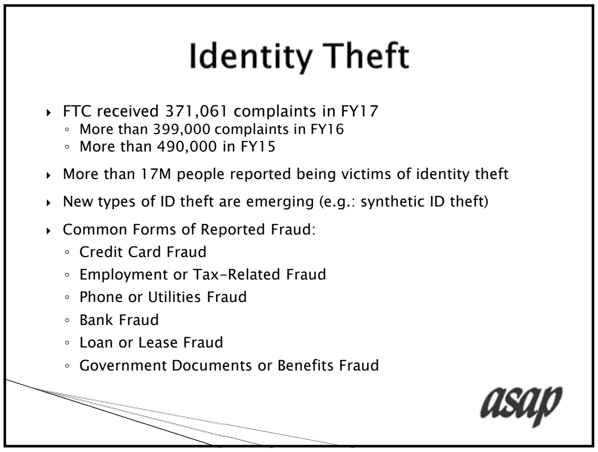
asap



Why Steal PII?

- Seek employment
- Travel across international borders
- Obtain prescription drugs
- Receive medical treatment
- Claim benefits
- File false tax returns
- Aid in other criminal activities

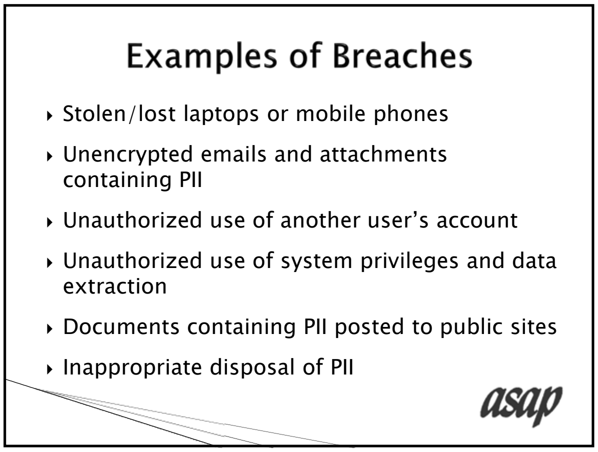
asap



Identity Theft

- FTC received 371,061 complaints in FY17
  - More than 399,000 complaints in FY16
  - More than 490,000 in FY15
- More than 17M people reported being victims of identity theft
- New types of ID theft are emerging (e.g.: synthetic ID theft)
- Common Forms of Reported Fraud:
  - Credit Card Fraud
  - Employment or Tax-Related Fraud
  - Phone or Utilities Fraud
  - Bank Fraud
  - Loan or Lease Fraud
  - Government Documents or Benefits Fraud

asap

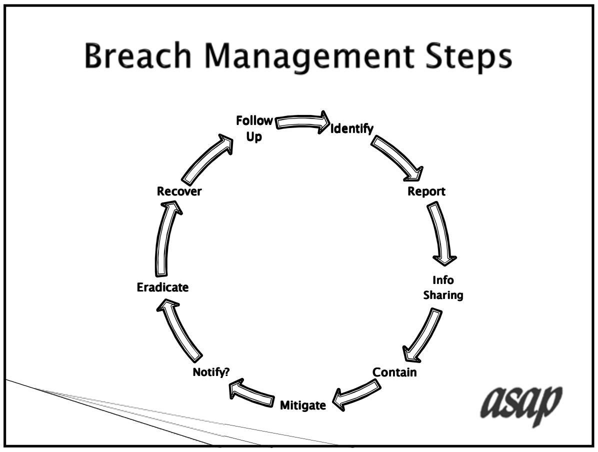


Examples of Breaches

- Stolen/lost laptops or mobile phones
- Unencrypted emails and attachments containing PII
- Unauthorized use of another user's account
- Unauthorized use of system privileges and data extraction
- Documents containing PII posted to public sites
- Inappropriate disposal of PII

We Have a Breach– What Happens Now?

You Need a Breach Response Plan.



Breach Management Steps

Follow Up

Identify

Report

Info Sharing

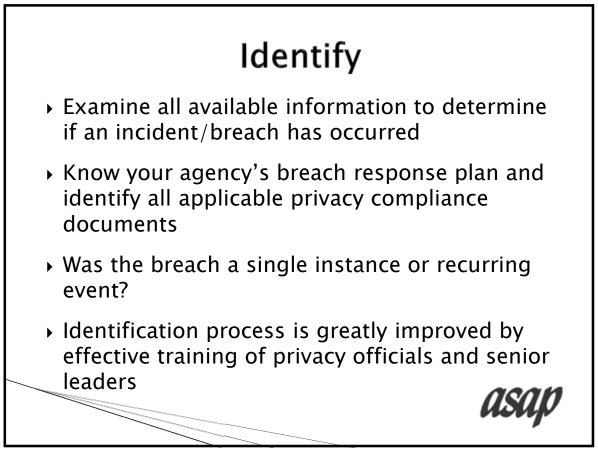
Contain

Mitigate

Notify?

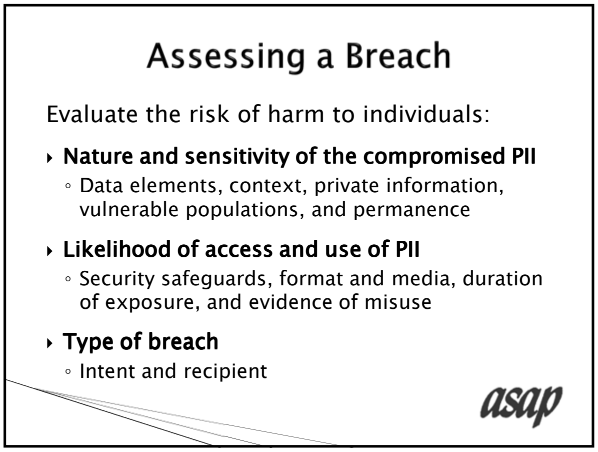
Eradicate

Recover



Identify

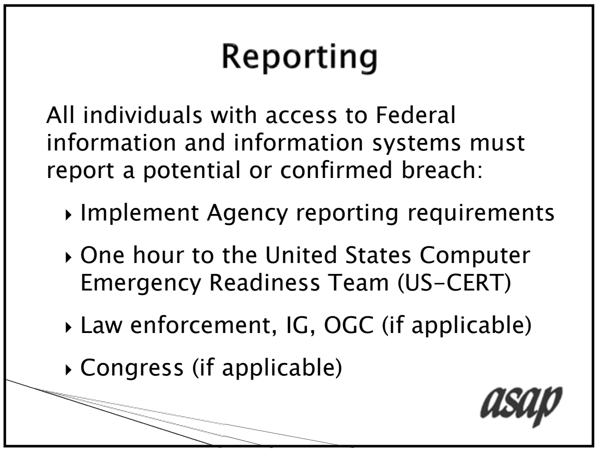
- Examine all available information to determine if an incident/breach has occurred
- Know your agency's breach response plan and identify all applicable privacy compliance documents
- Was the breach a single instance or recurring event?
- Identification process is greatly improved by effective training of privacy officials and senior leaders



Assessing a Breach

Evaluate the risk of harm to individuals:

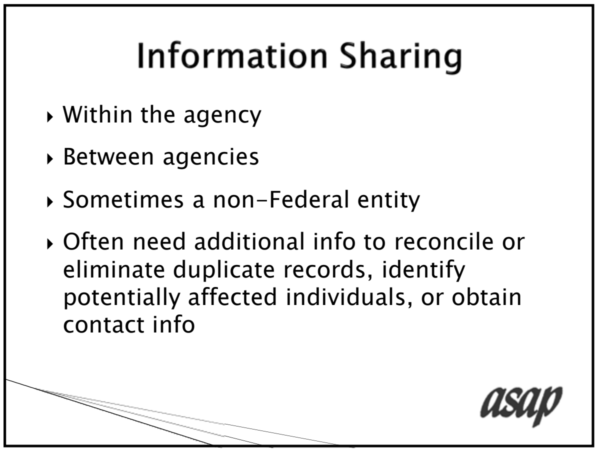
- **Nature and sensitivity of the compromised PII**
  - Data elements, context, private information, vulnerable populations, and permanence
- **Likelihood of access and use of PII**
  - Security safeguards, format and media, duration of exposure, and evidence of misuse
- **Type of breach**
  - Intent and recipient



Reporting

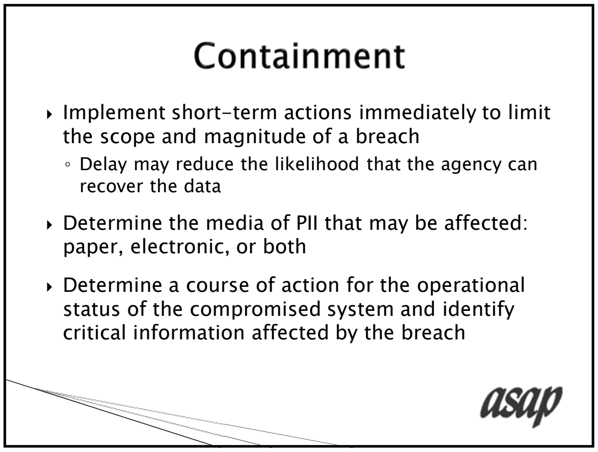
All individuals with access to Federal information and information systems must report a potential or confirmed breach:

- Implement Agency reporting requirements
- One hour to the United States Computer Emergency Readiness Team (US-CERT)
- Law enforcement, IG, OGC (if applicable)
- Congress (if applicable)



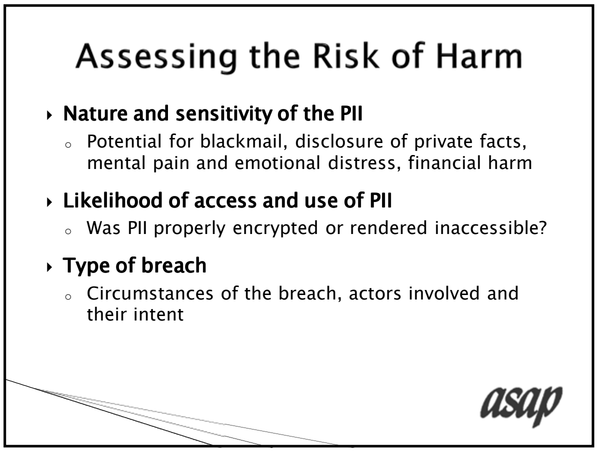
Information Sharing

- Within the agency
- Between agencies
- Sometimes a non-Federal entity
- Often need additional info to reconcile or eliminate duplicate records, identify potentially affected individuals, or obtain contact info



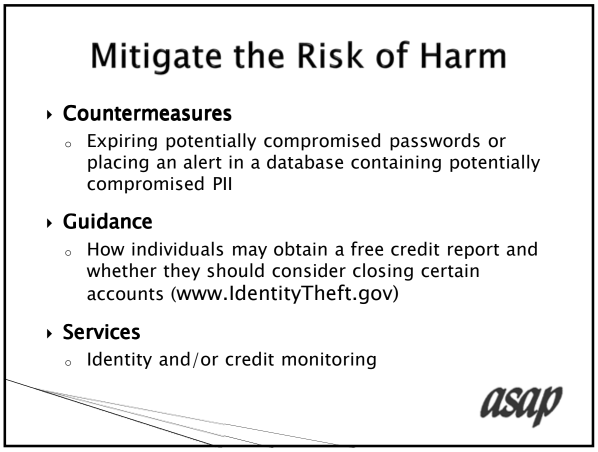
Containment

- Implement short-term actions immediately to limit the scope and magnitude of a breach
  - Delay may reduce the likelihood that the agency can recover the data
- Determine the media of PII that may be affected: paper, electronic, or both
- Determine a course of action for the operational status of the compromised system and identify critical information affected by the breach



Assessing the Risk of Harm

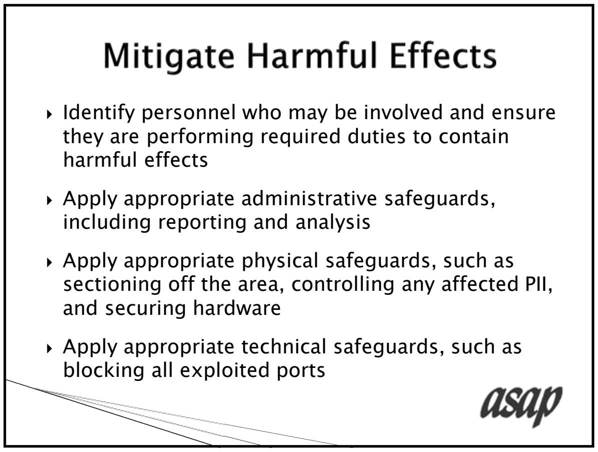
- **Nature and sensitivity of the PII**
  - Potential for blackmail, disclosure of private facts, mental pain and emotional distress, financial harm
- **Likelihood of access and use of PII**
  - Was PII properly encrypted or rendered inaccessible?
- **Type of breach**
  - Circumstances of the breach, actors involved and their intent



Mitigate the Risk of Harm

- **Countermeasures**
  - Expiring potentially compromised passwords or placing an alert in a database containing potentially compromised PII
- **Guidance**
  - How individuals may obtain a free credit report and whether they should consider closing certain accounts (www.IdentityTheft.gov)
- **Services**
  - Identity and/or credit monitoring

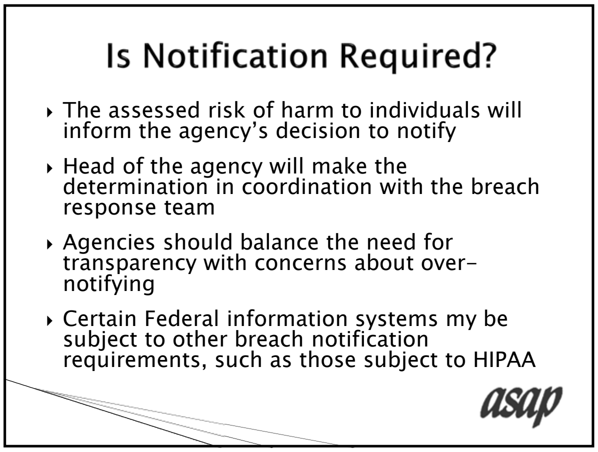
asap



Mitigate Harmful Effects

- Identify personnel who may be involved and ensure they are performing required duties to contain harmful effects
- Apply appropriate administrative safeguards, including reporting and analysis
- Apply appropriate physical safeguards, such as sectioning off the area, controlling any affected PII, and securing hardware
- Apply appropriate technical safeguards, such as blocking all exploited ports

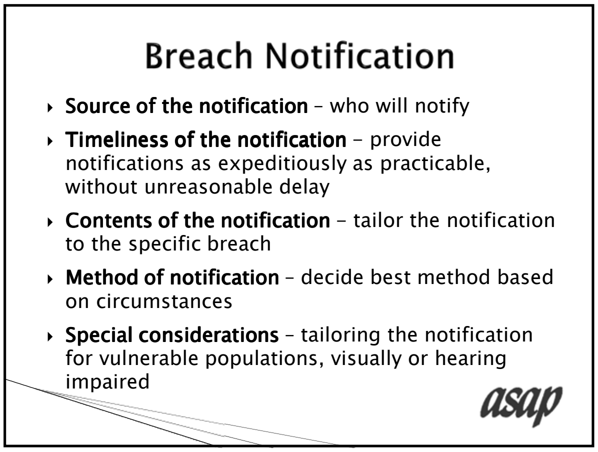
asap



Is Notification Required?

- The assessed risk of harm to individuals will inform the agency's decision to notify
- Head of the agency will make the determination in coordination with the breach response team
- Agencies should balance the need for transparency with concerns about over-notifying
- Certain Federal information systems my be subject to other breach notification requirements, such as those subject to HIPAA

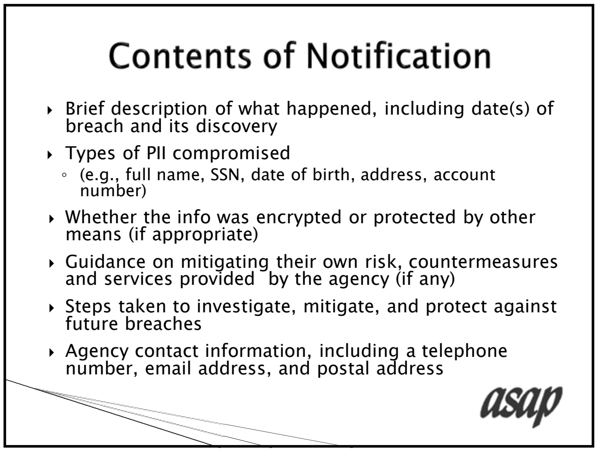
asap



Breach Notification

- **Source of the notification** – who will notify
- **Timeliness of the notification** – provide notifications as expeditiously as practicable, without unreasonable delay
- **Contents of the notification** – tailor the notification to the specific breach
- **Method of notification** – decide best method based on circumstances
- **Special considerations** – tailoring the notification for vulnerable populations, visually or hearing impaired

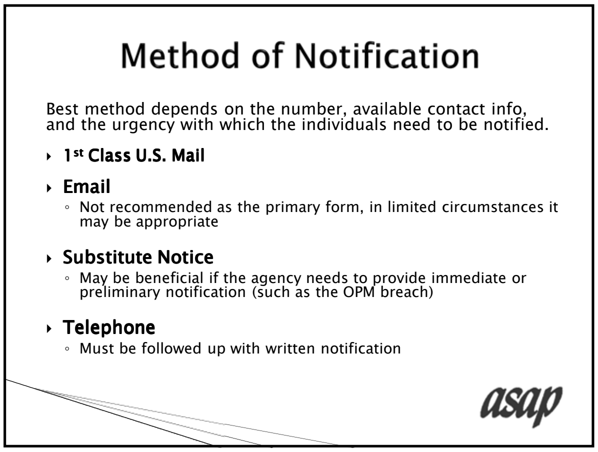
asap



Contents of Notification

- Brief description of what happened, including date(s) of breach and its discovery
- Types of PII compromised
  - (e.g., full name, SSN, date of birth, address, account number)
- Whether the info was encrypted or protected by other means (if appropriate)
- Guidance on mitigating their own risk, countermeasures and services provided by the agency (if any)
- Steps taken to investigate, mitigate, and protect against future breaches
- Agency contact information, including a telephone number, email address, and postal address

asap

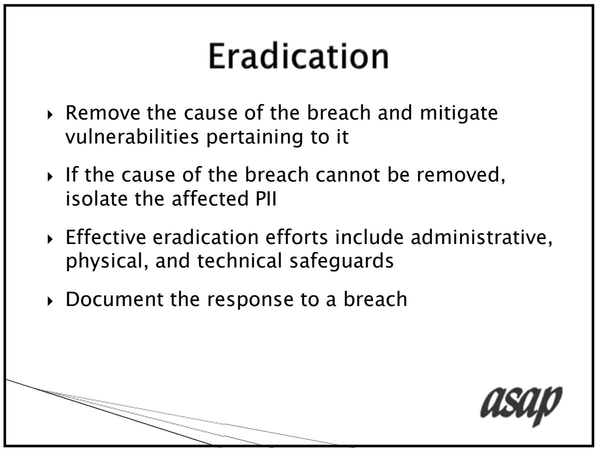


Method of Notification

Best method depends on the number, available contact info, and the urgency with which the individuals need to be notified.

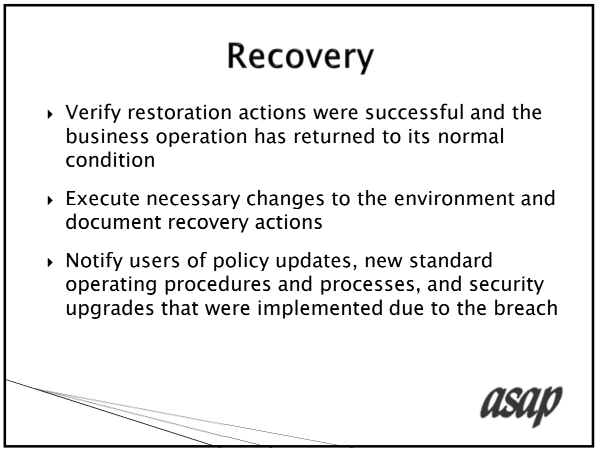
- **1st Class U.S. Mail**
- **Email**
  - Not recommended as the primary form, in limited circumstances it may be appropriate
- **Substitute Notice**
  - May be beneficial if the agency needs to provide immediate or preliminary notification (such as the OPM breach)
- **Telephone**
  - Must be followed up with written notification

asap



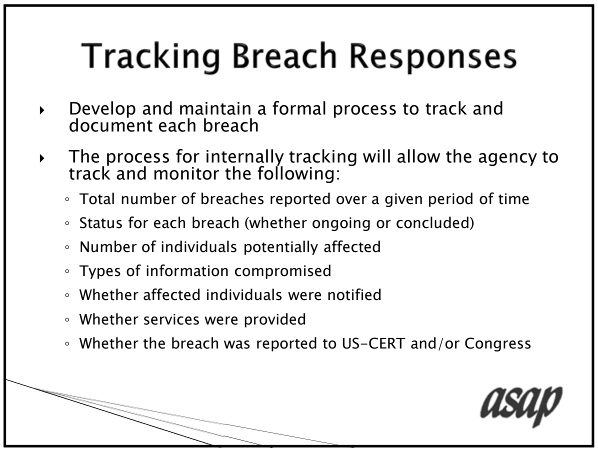
Eradication

- Remove the cause of the breach and mitigate vulnerabilities pertaining to it
- If the cause of the breach cannot be removed, isolate the affected PII
- Effective eradication efforts include administrative, physical, and technical safeguards
- Document the response to a breach



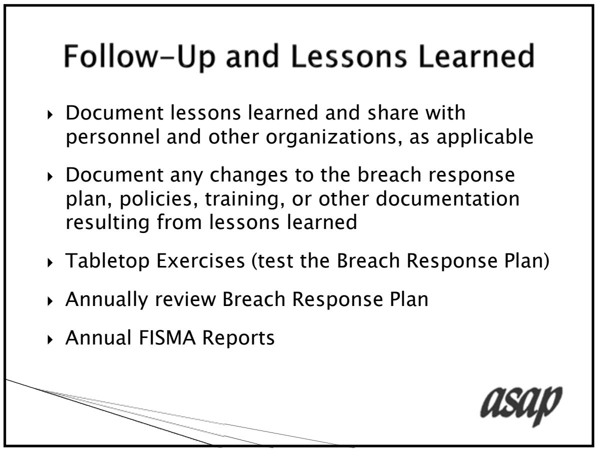
Recovery

- Verify restoration actions were successful and the business operation has returned to its normal condition
- Execute necessary changes to the environment and document recovery actions
- Notify users of policy updates, new standard operating procedures and processes, and security upgrades that were implemented due to the breach



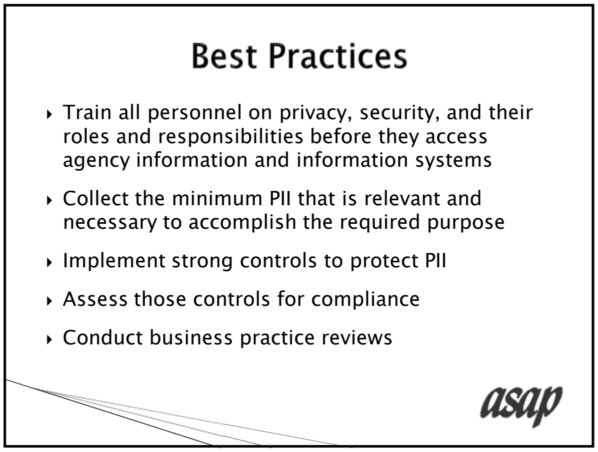
Tracking Breach Responses

- Develop and maintain a formal process to track and document each breach
- The process for internally tracking will allow the agency to track and monitor the following:
  - Total number of breaches reported over a given period of time
  - Status for each breach (whether ongoing or concluded)
  - Number of individuals potentially affected
  - Types of information compromised
  - Whether affected individuals were notified
  - Whether services were provided
  - Whether the breach was reported to US-CERT and/or Congress



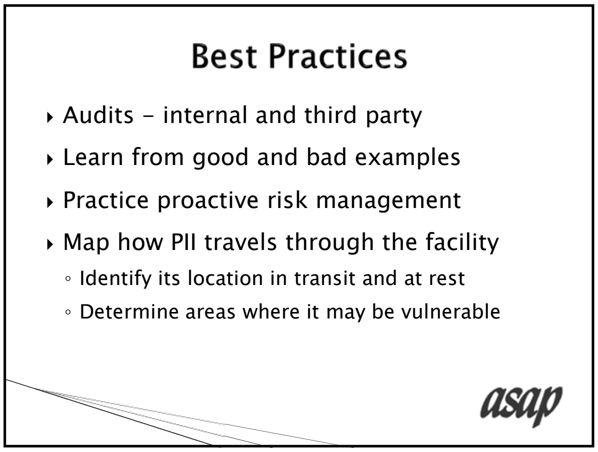
Follow-Up and Lessons Learned

- Document lessons learned and share with personnel and other organizations, as applicable
- Document any changes to the breach response plan, policies, training, or other documentation resulting from lessons learned
- Tabletop Exercises (test the Breach Response Plan)
- Annually review Breach Response Plan
- Annual FISMA Reports



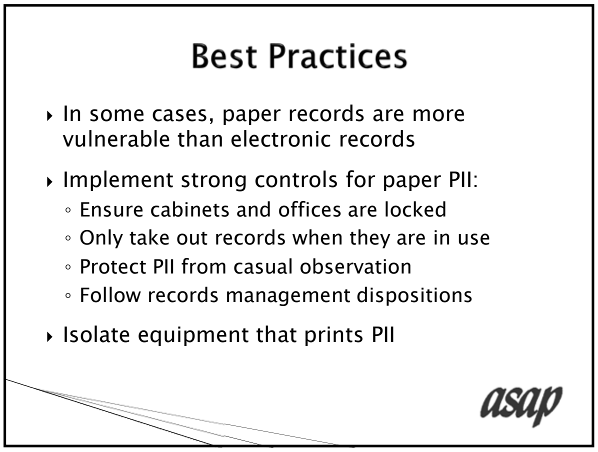
Best Practices

- Train all personnel on privacy, security, and their roles and responsibilities before they access agency information and information systems
- Collect the minimum PII that is relevant and necessary to accomplish the required purpose
- Implement strong controls to protect PII
- Assess those controls for compliance
- Conduct business practice reviews



Best Practices

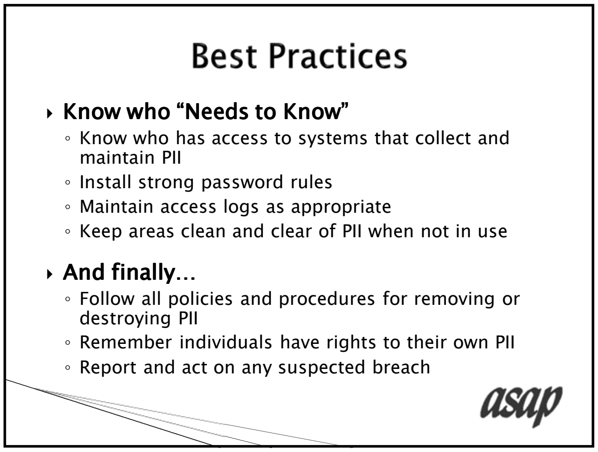
- Audits - internal and third party
- Learn from good and bad examples
- Practice proactive risk management
- Map how PII travels through the facility
  - Identify its location in transit and at rest
  - Determine areas where it may be vulnerable



Best Practices

- In some cases, paper records are more vulnerable than electronic records
- Implement strong controls for paper PII:
  - Ensure cabinets and offices are locked
  - Only take out records when they are in use
  - Protect PII from casual observation
  - Follow records management dispositions
- Isolate equipment that prints PII

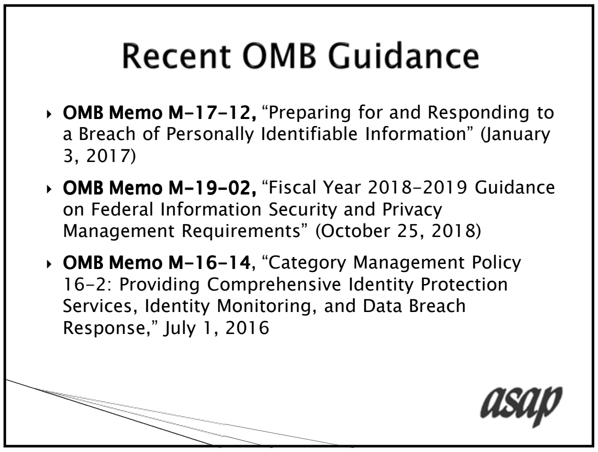
asap



Best Practices

- **Know who “Needs to Know”**
  - Know who has access to systems that collect and maintain PII
  - Install strong password rules
  - Maintain access logs as appropriate
  - Keep areas clean and clear of PII when not in use
- **And finally…**
  - Follow all policies and procedures for removing or destroying PII
  - Remember individuals have rights to their own PII
  - Report and act on any suspected breach

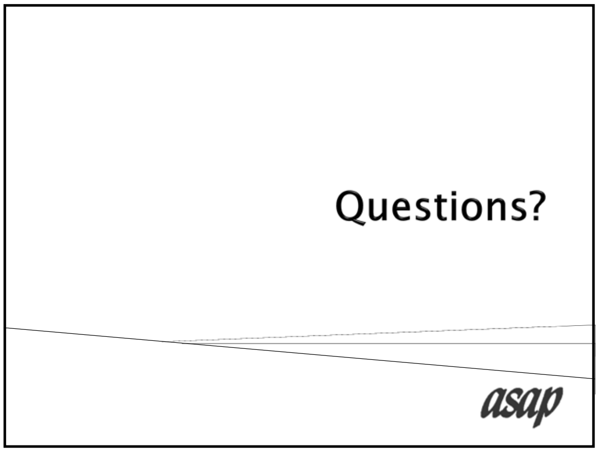
asap



Recent OMB Guidance

- **OMB Memo M-17-12,** “Preparing for and Responding to a Breach of Personally Identifiable Information” (January 3, 2017)
- **OMB Memo M-19-02,** “Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements” (October 25, 2018)
- **OMB Memo M-16-14**, “Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response,” July 1, 2016

asap



Questions?