REPORTING GUIDELINES

Preliminary Inquiries:

After the discovery of a spillage and the initial reporting, designated security officials must conduct a preliminary inquiry (who, what, when, where, why, how, etc.) into the incident. A preliminary inquiry, at a minimum, answers the following questions:

- When did the spillage occur?
- What information was spilled?
- What was the classification (sensitivity level) of the information?
- Was it properly identified?
- What caused the spillage?
- Who was responsible?
- What steps were taken to identify the person responsible?
- Where is the information now (current disposition) and what (if any) mitigation or containment methods have been utilized?
- What individuals had and have access to the information?
- What computer systems were affected? Identify each and type.

NOTE: As determined by the SSE, additional inquiries or a formal investigation may be necessary.

Preliminary Inquiries must NOT contain classified information and should be categorized as For Official Use Only (FOUO).

REPORTING REQUIREMENTS

FAA personnel are required to report all actual or suspected incidents of spillage to:

Servicing Security Elements (SSE)

System Owner/Administrator

SSE will notify the Information Owner/Originator !!

NOTE: Follow-up (status) reports are issued as needed or if mitigation/containment efforts exceed 72 HOURS from the initial reporting of the incident.

Who are the Servicing Security Elements (SSE)?

- *In regions the SSE is the Security and Hazardous Materials Division, AXX-700.*
- *At Washington Headquarters, the SSE is the Internal Security Division, AIN-100.*

Federal Aviation Administration
Assistant Administrator for Security
and Hazardous Materials (ASH-1)
Office of Security
Internal Security Division (AIN-100)
800 Independence Ave, SW
Room 315
Washington, DC 20591
202-493-5405

HQ-09782.INDD

Federal Aviation Administration

Classified/Sensitive Information and How to Handle Data Spills (Spillage)

SPILLAGE AND THE CAUSES

What is a Data Spill (Spillage)?

A data spill occurs when classified or sensitive information is transferred to a non-accredited or unauthorized computer system.

Regardless of who discovers the incident, immediate action is required.

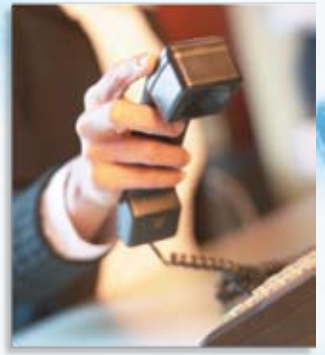
Causes of Data Spillage include, but are not limited to:

- Electronic receipt from an outside entity
- Inadequate classification guidance or identification markings
- User Error
  - Personnel who do not know the rules or choose not to follow them
  - Fatigue
  - Honest mistakes and/or oversights (data entry errors)
  - Lack of sufficient training
  - General indifference

INITIAL STEPS/CONSIDERATIONS

Initial Steps

- **Immediately report the incident to the Servicing Security Element (SSE). The SSE will provide guidance on the appropriate containment and mitigation measures.**
- **Maintain mission/operations unless or until otherwise directed**
- **Take steps to prevent additional spillage**
- **Conduct an inquiry**



Considerations

Should operations/mission continue?

Consider:

The classification/sensitivity level of the information

Amount/volume/nature of information

Criticality necessity of current operations

Perishability of the information

Possible impact to ongoing investigations (Preservation of evidence)

Prior to Mitigation Consider:

The impact to operations and mission

Financial concerns, including the cost of media replacement and the resources required to mitigate

Requirements of the information owner and any pre-existing agreements regarding the information

Assessment of the effectiveness of the mitigation methods and acceptance of residual risk by the information owner

MITIGATION METHODS

With coordination and approval from the SSE, steps could include:

Using the existing operating system to delete the spilled information

Re-labeling the media or system and storing appropriately in approved areas (Confiscating the media or hardware)

Approved technical means
- National Security Agency Approved methods (e.g. degaussing)

Approved agency methods
- Consult with your SSE