# ADMINISTRATIVE COMMUNICATIONS SYSTEM
## U.S. DEPARTMENT OF EDUCATION

# DEPARTMENTAL DIRECTIVE



*Distribution*:
All Department of Education Employees

*Signed by:* Andrew Jackson
Assistant Secretary for Management

# External Breach Notification Policy and Plan

Table of Contents



For technical questions concerning information found in this ACS document, please contact (202) 401-1269 or via e-mail privacysafeguards@ed.gov.

Supersedes OM: 6-107 “External Breach Notification Policy and Plan”, dated 04/15/2008.

# I. Purpose

This Directive establishes an external breach notification policy and plan for the United States Department of Education (ED). Based on this Directive, when a data breach involving Personally Identifiable Information (PII)[1] occurs, ED will conduct a risk analysis. Based on this risk analysis, ED will determine whether to notify individuals whose PII may have been involved in the breach and what steps, if any, ED will take to mitigate actual or potential harm to the data subjects, the Department, or anyone else who might be harmed by a breach.

The procedures in this Directive supplement the procedures already stated in:

A. Handbook for Information Assurance/Cybersecurity Policy, OCIO-01;

B. Handbook for Information Security Incident Response and Reporting Procedures, OCIO-14; and

C. Handbook for Protection of Sensitive but Unclassified Information, OCIO-15.

# II. Policy

A. Notification Policy

It is ED's policy that:

1. ED shall assess all actual or suspected data breaches involving PII that are processed or maintained by ED when the entity experiencing the data breach is ED or third parties, such as contractors or subcontractors, who are provided access to ED data and who have agreed to, or are otherwise required to, abide by this Directive. ED shall make a determination as to whether and how to provide external notification or any other remediation, consistent with all applicable legal requirements.

2. The determination of whether external notification is required shall be based on a risk assessment performed by the Privacy Incident Response Team ("PIRT"), or the PIRT Advisory Group ("PAG"), as discussed in Section VII. D.

3. The risk analysis shall consider, among other things, the likelihood that the information will be used to harm the data subject(s).

[1] Personally Identifiable Information (PII), in accordance with the definition prescribed by the Office of Management and Budget (OMB) M-07-16, is any information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc. alone, or when combined with other personal information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

4. The PAG or PIRT, as appropriate, shall apply the five risk factors described in Section VII.D.2. of this document, within the fact-specific context of a reported actual or suspected breach of PII. Using this methodology, notification shall be given in instances where there is reasonable risk of harm to the data subjects or anyone else who might be harmed by a breach.

5. If ED determines that the data breach meets the established criteria for notification, the notification shall be made as expeditiously as practicable and without unreasonable delay, after the data breach.

6. If ED determines that the incident meets the established criteria for notification, the PAG or PIRT will notify the Office of Communications and Outreach (OCO) to alert them to the breach so that they can be prepared to answer any questions from the press or the general public. The PAG or PIRT will also notify the Office of Legislation and Congressional Affairs (OLCA) if it is a "major incident" (see Section VI.N.), so they can notify Congress.

B. Administrative Policy

1. Annual Meeting and Directive Review

   The PIRT shall meet regularly, usually annually, to review this Directive, any changes in circumstances that would require amendment of this Directive, and to assess the handling of any breaches that occurred during the year, incident trends, and to consider whether any process improvements are warranted.

   The PAG will analyze incident response after all major incidents to identify opportunities for process improvement, and will submit them to the PIRT for action, as appropriate.

2. Reporting

   The Senior Privacy Specialist will track and monitor the life-cycle of breaches, based on information received by ED's Computer Incident Response Capability (EDCIRC) Coordinator, the PIRT, and the Information Systems Security Officer (ISSO) of the system(s) involved and/or any other designee of the Principal Office experiencing the breach.

   All ED employees and contractors with authorized access to ED data, who know about or suspect a breach of PII, or who otherwise might be involved with an incident involving PII, must report the breach to their EDCIRC and ISSO per OCIO-14 "Handbook for Information Security Incident Response and Reporting Procedures."

3. Incidents Involving Contractors or Other Third Parties

   a. All contractors that have an incident involving ED PII data must comply with the reporting requirements in OCIO-14 "Handbook for Information Security Incident Response and Reporting Procedures," as well as the policies and procedures set forth in this document. Contractor requirements can be found at: http://www2.ed.gov/fund/contract/about/bsp.html.

      All incidents involving contractors are also governed by the contract and the statement of work.

      All incidents involving other third parties with access to ED data are governed by their agreements or other requirements requiring their compliance with this Directive.

   b. When the breach is caused by a contractor or another third party with access to ED data, the contractor or other third party has agreed to or is otherwise required to comply with this Directive, and the data is ED data (for example, when a contractor is processing data that ED provided from one of ED's systems), the determination regarding notification will be determined according to Section VII.G.2 of this document. In some cases, the PIRT or PAG may require that a contractor or third party notify the data subjects. In other cases, due to state law, the contractor or third party will determine that they must notify.

   c. When an incident involves a contractor, the Contracting Officer shall provide direction to the contractor.

## III. Authorization

A. Office of Management and Budget (OMB) Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007.

B. The President's Identity Theft Task Force, Memorandum [not numbered] "Recommendations for Identity Theft Related Data Breach Notification," September 20, 2006.

C. Title III of the E-Government Act of 2002, Pub. L. 107-347, Federal Information Security Management Act of 2002 (FISMA 2002).

D. Privacy Act of 1974, as amended (5 U.S.C. § 552a) (Privacy Act).

E. Federal Information Security Modernization Act of 2014, Pub. L. 113–283, (FISMA 2014).

F. Office of Management and Budget (OMB) Memorandum M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements, October 30, 2015.

## IV. Applicability

This Directive applies to all ED employees, and third parties, including contractors and subcontractors, with access to ED data who have agreed to, or are otherwise required to, abide by this Directive.

## V. Definitions

A. Availability means ensuring timely and reliable access to and use of information.

B. Breach or Data Breach is an incident that includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic.

C. Confidentiality means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

D. Data Breach Analysis is the process used to determine the extent and impact of a data breach resulting from an actual or suspected breach of personally identifiable information.

E. ED means the United States Department of Education.

F. External Notification is the notice provided to those individuals affected, or potentially affected, after a data breach involving PII has occurred. External notification may also include notification to the general public through the news media, ED's webpage or notice to Members of Congress. External notification does not include notification of the Inspector General (IG) or other law enforcement.[2] External notification to other Federal entities required under other authority is not covered by this Directive.

[2] These entities will be notified in accordance with the Handbook for Information Security Incident Response and Reporting Procedures, Handbook OCIO-14

G. Incident is defined in FISMA 2014 and means an occurrence that--(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

   Note: Data Breaches are a subset of incidents.

H. Identity Theft means a fraud committed or attempted using the identifying information of another person without authority, subject to such further definition as the Federal Trade Commission may prescribe by regulation. Identity theft is a crime under 18 U.S.C. § 1028.

I. Information System, as defined by OMB Circular A-130, means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

J. Integrity means guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

K. Personally Identifiable Information (“PII”), in accordance with the definition prescribed by OMB M-07-16, is any information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc. alone, or when combined with other personal information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

L. Processed or Maintained by ED means collected, received, stored, used, or manipulated by ED personnel or by a person acting on behalf of ED, including a contractor or other third party with authorized access to ED data.

M. Secretary means the Secretary of Education. Under Section 412 of the Department of Education Organization Act, 20 U.S.C. § 3472, the Secretary generally may delegate any function to other ED employees or officers.

N. Suspected Breach means a breach, as defined in B. above that may have occurred, but is not yet confirmed.

O. Third Party includes an entity with access to ED data, such as a contractor or subcontractor, who has agreed to, or is otherwise required to, abide by this Directive.

P. Unauthorized Access is when a person gains logical or physical access without permission to PII, or to a network, system, application, data, or other

resource containing PII. Logical access means being able to interact with data through access control procedures such as identification, authentication, and authorization. Physical access means being able to physically touch and interact with the computers and network devices.

## VI. Responsibilities

A. Secretary

The Secretary has the ultimate authority to make final decisions about breach notification and remediation of incidents. It is expected, however, that the Secretary will not be involved in incident response decisions in the majority of cases, but will instead rely for decision-making on incidents involving PII on the PIRT, and, if appropriate in the context of an incident involving a law enforcement issue, the IG.

B. Senior Agency Official for Privacy (SAOP)

The SAOP is the Assistant Secretary for Management and is a core member of the PIRT. The SAOP shall provide overall management, oversight, and resources for responding to data breaches and compliance with OMB M-07-16 and this ACS Directive. For specific breaches, the SAOP shall appoint as necessary additional core members, including in consultation with the Office of the Deputy Secretary, including the Single Point of Contact as defined below.

C. Chief Privacy Officer (CPO)

The CPO chairs the PIRT. The CPO is responsible for:

1. convening and chairing meetings of the PIRT when a data breach requiring the PIRT's involvement has occurred;

2. providing to the PIRT information about data breaches;

3. providing insight and guidance regarding breach risk analysis, external notification, and information on current issues, trends, best practices and requirements regarding privacy safeguards;

4. reporting the PIRT's significant findings and recommendations to the Secretary, as appropriate;

5. being accountable to the Secretary and the SAOP for the appropriate handling of any breach, and for the continuing review and improvement of the breach notification policy; and

6. overseeing preparation for the PIRT's annual meeting.

D. Contracting Officer (CO) or Contracting Officer Representative (COR)

For contracts involving PII, contracting officers will provide this Directive to contractors to ensure that they are aware of ED's breach policy and where appropriate, incorporate provisions into the contract to ensure the contractor and all covered subcontractors comply with this policy.

When an incident involves a contractor, the CO, in collaboration with the COR, shall provide direction to the contractor on behalf of the Department.

E. EDCIRC Coordinator (EDCIRC)

The EDCIRC Coordinator, within the Office of the Chief Information Officer (OCIO), Information Assurance, is ED's chief point of contact for Principal Offices to report all actual and suspected incidents. The EDCIRC Coordinator is a member of the PAG, but may delegate that responsibility. The EDCIRC Coordinator is responsible for:

1. notifying United States Computer Emergency Readiness Team (US-CERT), the Senior Privacy Specialist, and designated contacts from the POC that experienced the breach, of an information security incident that involves PII, or is suspected to have involved PII;

2. notifying the IG of an information security incident of PII that may involve criminal activity, and updating the PAG regarding these incidents, to the extent that the EDCIRC may do so under direction from the IG;

3. notifying OCO for possible communication with the press and the general public;

4. providing any relevant incident information collected during the investigation of the security incident for the risk analysis;

5. attending PAG meetings and providing input on the incident; and

6. working with the PAG to perform the initial risk analysis and either resolve the incident, or determine if the incident should be referred to the PIRT.

F. Privacy Incident Response Team (PIRT)

The PIRT is chaired by the CPO. The team consists of two groups: core members and ancillary members. Core members serve as the permanent team for all PIRT purposes including annual meetings to review this Directive, as well as meetings convened to address a breach. Ancillary members are

officials from other key POs who serve on an as needed basis to provide essential expertise. The CPO determines if ancillary members are needed for a PIRT meeting on an as needed basis. Core members are: the SAOP, the CIO, the CPO, the Senior Official of the PO experiencing the breach, the General Counsel, and the Assistant Secretary for OCO, or their designees. If the data are lost by a different PO than that which owns the data, the senior official from the PO that owns the data will also be asked to participate on the PIRT. Additionally, the Deputy Secretary may appoint additional core members for specific breaches.

The Ancillary members are the Assistant Secretary of the Office of Legislation and Congressional Affairs (OLCA), the IG, the Deputy Assistant Secretary for Management, the Chief Financial Officer, and senior officials from Federal Student Aid (FSA) and Institute of Education Sciences (IES), or their designees.

The PIRT's responsibilities are as follows:

1. When the PAG refers a breach to the PIRT, the Chair shall convene the PIRT to review the PAG's risk analysis to determine the likelihood that the breach might result in identity theft, consumer fraud, or other harm.

2. Based on its findings, the PIRT shall determine what action, if any, is appropriate, including, but not limited to, whether to issue external notification to affected data subjects.

3. Both core and ancillary PIRT members shall designate an alternate to serve when the member is unable to participate in PIRT activities. It is the responsibility of each PIRT member to ensure that he or she is represented at each PIRT meeting, and that alternates are authorized to speak on behalf of PIRT members.

4. The PIRT shall meet regularly, generally annually, to review this Directive, any changes in circumstances that would require amendment of this Directive, the handling of any breaches that occurred during the year, incident trends, and proposed process improvements. The PIRT may also implement process changes on an ad hoc basis, based on recommendation by the PAG after a major incident.

5. The PIRT may convene in person, by teleconference, or by email, as appropriate, depending on the sensitivity of the breach.

G. PIRT Advisory Group (PAG)

The PAG consists of ED's Senior Privacy Specialist, the EDCIRC Coordinator, the FSA Chief Information Security Officer, or designee, and the

ISSO of the PO experiencing the breach, as needed. Where legal counsel is needed, an attorney from OGC will also be a member. The PAG is responsible for:

1. generally meeting weekly and as needed to review incidents and incident status;

2. gathering incident information and making the initial risk analysis determination about any security incidents;

3. when a risk analysis shows low-moderate risk of harm or lower, determining ED action;

4. referring incidents with a risk of harm of moderate or higher to the PIRT;

5. analyzing incident response after all major incidents to identify opportunities for process improvement, and submitting them to the PIRT or appropriate PO for action, as appropriate;

6. referring incidents to the PIRT where the PAG is not unanimous; and

7. providing input on notices.

H. Chief Information Officer (CIO)

The CIO, or designee, is a core member of the PIRT. The CIO shall participate in PIRT activities, and shall provide guidance on issues relating to information technology and cyber-security.

I. Senior Privacy Specialist

ED's Senior Privacy Specialist (SPS) is a member of the PAG. The SPS is located in the Office of the Chief Privacy Officer, in the Office of Management. Working closely with the affected Principal Office designee, the SPS is responsible for:

1. receiving notification from the EDCIRC Coordinator that a suspected or actual breach involving PII has occurred;

2. consulting with the EDCIRC coordinator to monitor initial fact finding;

3. working with the PAG to perform the initial risk analysis;

4. notifying the CPO of incidents that the PAG refers to the PIRT for a determination;

5. notifying the senior official and ISSO of the PO experiencing the incident of the determination made regarding notification, and providing that PO with the tools and templates needed to promptly implement the decision, as needed;

6. maintaining a record of actions regarding data breaches, including open and closed incidents, determinations, and mitigation;

7. tracking and monitoring the life-cycle of the incident, based on information received by the EDCIRC Coordinator, the PIRT, and the ISSO of the PO experiencing the breach;

8. determining when a data breach is closed and notifying the appropriate parties; and

9. keeping the CPO apprised of breach activity and PAG determinations.

J. Senior Official of the Principal Office Experiencing the Breach

The Senior Official of the Principal Office experiencing the breach, or designee, is a member of the PIRT. The Senior Official, or designee, shall:

1. provide to the PAG, PIRT, and CPO any necessary program information, and shall participate in the PIRT review and decision-making process;

2. if ED will provide external notification and ED is responsible for the data breach, the Senior Official will be responsible for developing the external notification letter, signing the letters, developing the list of the names and addresses of those being notified, and overseeing dispatch of the notice to the individual(s) involved;

3. monitor the process of any mitigation directed at his or her Principal Office, and will ensure a prompt implementation or notification, as expeditiously as practicable and without unreasonable delay;

4. if the incident involved a contractor, the Senior Official will work with the CO or COR for the affected contractor, to oversee and monitor the contractor and its actions and ensure that the contractor is doing what ED has directed it to do;

5. be authorized to represent the interests of the PO for the purposes of decision-making regarding mitigation activities and funding issues;

6. notify the Senior Privacy Specialist when the final notification action has been taken; and

7. if ED is responsible for the breach, ensure that the PO is responsible for any costs associated with external notification and mitigation activities. If a third party, is responsible for the breach, work with, as may be applicable, the PO's contracting representative, Contracts and Acquisitions Management, OGC, and the third party to determine the responsible party for any such costs, based on the contract, statement of work, and other relevant documents.

K. Information Systems Security Officer(s) for the PO or System(s) affected by the breach or other person primarily responsible for security within the Principal Office, such as a Chief Information Security Officer, or for a specific system (called an ISSO throughout this document).

The PO's ISSO is a member of the PAG when a breach occurs in his or her PO. The ISSO is responsible for:

1. developing the facts of an incident occurring in the ISSO's system;

2. participating in the activities of the PAG regarding incidents occurring in that system;

3. with the PAG, conducting a risk analysis and making a recommendation regarding further action;

4. working with the Senior Official of that PO to implement a decision of the PIRT; and

5. keeping the Senior Privacy Specialist informed as to the status and progress of those actions directed by the PIRT to that system.

I. Assistant Secretary for Communications and Outreach

The Assistant Secretary, or designee, is a core member of the PIRT. The Assistant Secretary for OCO is responsible for participating in all PIRT activities, recommending a public notification strategy, and developing outreach materials, e.g., news releases, webpage postings.

M. General Counsel (GC)

The General Counsel, or designee, is a core member of the PIRT and shall participate in all PIRT activities in order to provide advice and legal counsel regarding breach issues and activities, as well as external notification.

N. Assistant Secretary for Legislation and Congressional Affairs

The Assistant Secretary, or designee, is an ancillary member of the PIRT and shall participate in PIRT activities, as needed, to provide assistance with communicating with Congress, and in responding to Congressional inquiries. The Assistant Secretary will also notify Congress in the event of a major incident, in compliance with FISMA 2014, and in accordance with current OMB guidance[3].

O. Inspector General (IG)

The Office of Inspector General is the law enforcement component of ED and has primary responsibility for criminal investigations related to ED's programs and operations. The IG is an ancillary member of the PIRT. The IG, or designee, is responsible for:

1. coordinating any law enforcement response to an incident;

2. participating in PIRT activities, as needed, and subject to the requirements of the Inspector General Act;

3. providing consultative advice to the CPO and the SAOP, as needed; and

4. conducting independent and objective audits, investigations, and inspections of ED's programs and operations.

After a breach is referred to the OIG because of possible criminal activity, the IG is responsible for reporting back to the PAG, when appropriate, so that notification can be made to the data subjects, or for the PAG to better understand the breach and modify processes to avoid future breaches or develop improved response procedures.

P. Deputy Assistant Secretary for Management

The Deputy Assistant Secretary for Management, or designee, is an ancillary member of the PIRT and is responsible for:

1. participating in PIRT activities in order to provide expertise on Office of Management matters;

2. providing input regarding external notification, as needed; and

[3] OMB was tasked with defining "major incident" in FISMA 2014 and defined the term in OMB M-16-03 available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf. This definition is subject to change based upon incidents, risks, recovery activities, or other relevant factors, and will be updated on MAX.gov: https://community.max.gov/x/eQPENw.

3. acting as the Senior Official of the PO experiencing the breach if OM is the PO experiencing the breach.

Q. Chief Financial Officer (CFO)

The CFO, or designee, is an ancillary member of the PIRT and shall participate in PIRT activities and provide input regarding external notification and contract issues, as needed.

R. FSA and IES Officials

FSA and IES Officials are ancillary members of the PIRT, unless an incident has occurred in their PO, and shall participate at annual meetings and other PIRT discussions, as needed, in order to provide expertise from their roles as the major collectors and users of PII within ED.

S. Single Point of Contact (SPOC)

If there is a major incident as defined under current OMB guidance[4], the SAOP will, in consultation with the Office of the Deputy Secretary, appoint a SPOC for communications with OMB, the Department of Homeland Security (DHS), and other Federal agencies as appropriate. The SPOC will coordinate with OMB and DHS throughout the incident response process. The SPOC will have the authority to direct actions required in all phases of the incident response process.

## VII. Procedures

A. External Breach Response Procedures

Upon notice that a breach involving PII, or suspected to involve PII, has been reported to the EDCIRC Coordinator, ED must determine the course of action regarding external notification and mitigation-related actions using the procedures described below.

All ED employees and contractors who know about or suspect a breach of PII, or who otherwise might be involved with an incident involving PII, shall report the breach to their ISSO per OCIO-14 “Handbook for Information Security Incident Response and Reporting Procedures.”

Contractors shall notify their Point of Contact or ISSO. For contractors, this information is found in the contract or Statement of Work.

B. Initial Analysis of an Incident

[4] See footnote 3.

1. Incidents, including those involving PII, are required to be reported to the OCIO[5] by the PO experiencing the breach. When a breach or suspected breach involving FSA data occurs, the FSA Chief Information Security Officer will also be notified.

2. When a breach or suspected breach involving PII processed or maintained by ED has been reported to the EDCIRC Coordinator, the Coordinator works with the ISSO of that PO, and the PAG, to develop a complete understanding of all of the facts, including type of PII lost, how it was lost, the nature of loss, potential for harm, number of individuals affected, and other key information. During this time, the affected PO and/or OCIO are working to contain potential harm in the event of a system-related breach, in accordance with OCIO-14. The EDCIRC Coordinator provides initial and follow-up facts describing the incident to the Senior Privacy Specialist.

3. Once the breach has been reported to US-CERT, the internal incident investigation is complete, and there is sufficient information to make a determination as to ED action, the Senior Privacy Specialist will convene the PAG to perform the initial risk analysis methodology as described in Subsection D below.

4. The PAG will then either make a determination on the matter, or will refer the matter to the CPO to convene the PIRT.

5. The Senior Privacy Specialist will provide the risk analysis results and the recommendation to the PIRT for further action.

C. Determination of Action

1. The PIRT Advisory Group

   The PAG is convened when the EDCIRC Coordinator determines that a breach involving PII processed or maintained by ED has occurred. The PAG shall assess breaches involving PII that are processed or maintained by ED when the entity experiencing the breach is ED or a third party who has agreed to, or is otherwise required to, abide by this Directive. The PAG may, but is not required to, assess breaches involving PII that are processed or maintained by ED when the entity experiencing the breach is not covered by this Directive. When a breach or suspected breach

[5] All security incidents are immediately reported to the EDCIRC Coordinator, in accordance with *the Handbook for Information Security Incident Response and Reporting Procedures*, Handbook OCIO-14, or replacement publication. The EDCIRC Coordinator reports the incident as required, including to the Incident Handler, who will conduct a review of the incident. A security risk assessment is performed.

involving FSA data occurs, the FSA Chief Information Security Officer will work closely with the PIRT and PAG.

The PAG will conduct the initial risk analysis. If they unanimously agree that the risk of harm is low-moderate or lower, no further action is required and that decision is considered to be a final decision. The Senior Privacy Specialist shall keep the CPO informed of any such determinations made by the PAG.

If the PAG decides that the risk of harm is moderate or higher, pursuant to the risk analysis methodology described in Subsection D below, or if they are not unanimous, the incident is referred to the CPO to convene the PIRT. The PAG may also recommend other non-notification mitigation, such as an email from the CPO to a PO reminding them of a privacy or security policy, or repeating security training.

If the PAG notifies the CPO that the breach was intentional and the data were the target, where the incident has been reported in the media or on social networking sites, or where circumstances otherwise require urgency, the PAG will expedite the notification to the CPO, who will immediately convene the PIRT. In the case of possible criminal activity, the incident will have been reported to the IG and the CPO will coordinate with the IG.

If it appears that the incident may be a “major incident” as discussed in footnote 3 of this document, the PAG will note this in referring the incident to the PIRT, so that the Assistant Secretary of OLCA may notify Congress, as appropriate.

2. The PIRT

   If the PAG refers the incident to the CPO, the CPO shall convene a meeting of the PIRT as soon as reasonably possible. For the purposes of conducting PIRT meetings, the CPO may convene the PIRT via email, conference call, or on-site, as appropriate, depending on the sensitivity of the breach, and in order to accommodate the schedules of the members and the urgency of the agenda item(s). The CPO shall determine, as appropriate, whether to include ancillary members of the PIRT in such convening.

3. Summary Variation in Determination of Action According to Risk Analysis

   As stated above, if the PAG determines that the risk of harm is low-moderate or lower, no notification will be provided and the breach is closed.

If the PAG determines that the risk of harm is moderate or higher, they will refer the breach to the PIRT using the process described above.

The PIRT shall apply the five risk factors identified below in Subsection D below within the fact-specific context of a reported actual or suspected breach of PII.

Using this methodology, and consistent with all applicable legal requirements, the PIRT will decide what mitigation to provide pursuant to the procedures outlined in Subsection E below. Once the PIRT has made the determination about what mitigation to provide, the Senior Official of the PO experiencing the breach is responsible for ensuring that external notification is made promptly and according to the PIRT's determination.

Notification shall be provided pursuant to the procedures outlined in Subsections E-O below, in instances where required by law, or where there is a moderate or higher risk of harm that can be mitigated with notification.

D. Risk Analysis Methodology

1. The PAG shall assess the likely risk of harm caused by the breach, using the five factors described below, and then assess the level of risk as low, low-moderate, moderate, moderate-high or high. The PIRT may adopt this risk assessment, or the PIRT may conduct its own assessment using the same five factors.

    a. In determining the risk of harm, a wide variety of harms shall be considered, including harm to reputation and the potential for harassment or prejudice, particularly when health or financial information is involved in the breach.

    b. When notification could increase a risk of harm, notification shall be delayed while appropriate safeguards are put in place.

2. The five factors that shall be considered in assessing the likely risk of harm[6] are:

    a. Nature of the Data Elements Breached

        The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals. In assessing the levels of risk and harm, the

[6] OMB M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information,

PAG shall consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.[7]

b. Number of Individuals Affected

The magnitude of the number of affected individuals impacts the scope of likely harm and may dictate the method that is chosen for providing notification, but should not be the determining factor for whether ED provides notification.

c. Likelihood the Information is Accessible and Usable

The PAG or PIRT shall assess the likelihood that compromised PII will be, or has been, used by unauthorized individuals. An increased risk that unauthorized individuals will use the information increases the risk of harm. The PAG or PIRT shall consider any physical, technological, and procedural safeguards that were in place that could affect the likelihood of unauthorized use, such as properly implemented encryption. The PAG or PIRT shall also consider whether or not the safeguards provided make the PII inaccessible or unusable, and determine whether the PII is at a low, moderate, or high risk of compromise. Other considerations may include the likelihood that any unauthorized individual will know the value of the information and will either use the information or sell it to others. The assessment shall be guided by the ED-CIRC Coordinator and shall comply with National Institute of Standards and Technology (NIST) security standards and guidance.

d. Likelihood the Breach May Lead to Harm

1) Broad Reach of Potential Harm

The PAG or PIRT shall consider whether the breach could result in substantial harm, embarrassment, inconvenience, or unfairness to any of the subject individuals. The PAG or PIRT shall also consider a number of possible harms associated with the loss or compromise of information. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse,

[7] An example provided in OMB M-07-16, page 14, Footnote 41 states “theft of a database containing individuals’ names in conjunction with Social Security numbers, and/or dates of birth may pose a high level of risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context.”

the potential for secondary uses of the information that could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

2) Likelihood Harm Will Occur

The likelihood that a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. Social Security numbers and account information are useful for committing identity theft, as are dates of birth, passwords, and mother's maiden names. If the information involved is a name and address or other personally identifying information, the loss may also pose a significant risk of harm if, for example, it appears on a list of patients at a clinic for treatment of a contagious disease. In considering whether the loss of information could result in identity theft or fraud, the PAG should consult guidance from the Identity Theft Task Force.[8]

e. Ability of the Agency to Mitigate the Risk of Harm

Within an information system, the risk of harm will depend on how ED is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken. Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and difficult to determine.

3. Risk of Harm

After evaluating each of these factors, the PAG or PIRT shall assess the level of impact using the impact levels below. The impact levels – low, low-moderate, moderate, moderate-high, and high – describe the potential impact(s) on an organization or individual if a breach occurs. The impact levels will help determine the risk of harm.

a. **Low:** The risk of harm is low if the breach could result in limited or no harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; or could have a limited or no adverse effect on organizational operations or organizational assets.

[8] Memorandum [not numbered] "Recommendations for Identity Theft Related Data Breach Notification," September 20, 2006.

b. **Moderate:** The risk of harm is moderate if the breach could result in significant harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; or could have a serious adverse effect on organizational operations or organizational assets.

c. **High**: The risk of harm is high if the breach could result in severe or catastrophic harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained; or could have a severe or catastrophic adverse effect on organizational operations or organizational assets.

E. Mitigation and Related Actions

The PIRT's decision about mitigation should also include the method of notification, consideration of appropriate mitigation options, as well as notice of whether the data subject is already aware of the breach. Such options may include:

1. **External Notification** – This process is described in detail below.

2. **Credit Monitoring** – If it is determined that credit monitoring services are appropriate, the PO experiencing the breach shall utilize one of the government-wide Blanket Purchase Agreements that the General Services Administration (GSA) has established to provide these services.[9]

3. **Law Enforcement Notification** – The Office of Inspector General, as the primary law enforcement component of ED, shall determine the appropriate steps, if needed, for coordination with any other law enforcement agencies.

4. **Other Mitigation** – ED may also set up a toll-free number or webpage to handle inquiries from the affected individuals and the public, remove subject PII if no longer needed for documented agency need, send a broadcast email to the affected PO that reminds employees about their responsibilities, recommend that the PO change policies or practices, and/or recommend disciplinary action toward an employee under existing PMI guidelines.

F. Timeliness of the Notification

The Federal Information Security Management Act of 2002 (FISMA 2002), established a federal information security incident center to, among other

[9] See OMB M-07-04, "Use of Credit Monitoring Services Blanket Purchase Agreements (BPA)" dated December 22, 2006. For guidance in obtaining credit monitoring for data subjects, see GSA's Center for Innovative Acquisition Development, and the GSA list of data breach contractors.

things, provide timely technical assistance to agencies regarding cyber incidents. Established in 2003, US-CERT serves as the federal information security incident center authorized under FISMA. Pursuant to OMB Memoranda M-06-19 and M-07-16, incidents that involve PII must be reported to the Federal Incident Response Center (US-CERT) within one hour of discovery. New guidance issued by US-CERT requires reporting to US-CERT within one hour after the highest level incident response team confirms an actual breach.

OCIO requires that any incidents at ED shall be reported to EDCIRC Coordinator as soon as an incident is suspected, so that the incident response team can confirm the breach, so that the US-CERT deadline may be met.

Upon notification that a breach involving PII has occurred or is suspected to have occurred, and a risk analysis supports external notification, ED shall provide notification as expeditiously as practicable and without unreasonable delay. The PO where the breach occurred is responsible for prompt notification. This may vary depending on the circumstances, but in most cases, within 10 days of the determination that notification will be provided. Such notification shall be consistent with the needs of law enforcement and national security, and any measures necessary to restore the reasonable integrity of any computerized data system compromised. Decisions to delay notification shall be made by CPO or the SAOP. In some circumstances, law enforcement or national security considerations may require a delay if notification would impede the investigation of the breach or the affected individual(s).

G. Source of the Notification

1. Principal Office Experiencing the Breach

   Generally, the PO where the data breach occurred will draft, sign, and distribute all notifications if ED is responsible for the data breach, with input from the body that determined the notification is appropriate, either the PAG or the PIRT, and OCO (see role of OCO Assistant Secretary). In situations that have been determined to be a “major incident” as defined above, prior to distribution, the CPO and OGC will review and approve the notifications.

2. Third Parties

   a. There are situations where the breach is caused by a third party and the data is ED data (for example, when a contractor is processing data that ED provided from one of ED’s systems). The PAG should conduct the risk analysis.

1) If the risk of harm is low-moderate or low risk, and the PO or the third party determines that the individuals should or must be notified for legal or other reasons, the PO or the third party may do so only with the coordination, review, and approval of the PAG, with input from OGC and OCO, as needed.

2) If the risk of harm is moderate or higher risk, or the breach was referred to the PIRT for any reason, ED will determine the source of the notification.

   a) The third party may not issue notification unless explicitly allow to do so by the PIRT.

   b) If the PIRT determines that the third party must notify the data subjects, the third party must notify with the coordination, review, and approval of the PIRT. The PIRT may request input on the notification from OCO, OGC, or other relevant office. The third party may be asked to draft the notice, assist in developing the notification list, and sending out the notification.

b. When a breach involves a contractor, the Contracting Officer shall provide direction to the contractor.

c. All incidents involving contractors are governed by procurement law and regulation as well as the provisions of the contract, including the statement of work.

d. If the breach involves data that is strictly contractor data, such as its own human resources data, then the contractor does not need to consult with ED.

e. If the breach involved a contractor, the CO, in collaboration with the COR will oversee and monitor the contractor and its actions and ensure that the contractor is doing what the PIRT or PO directed the contractor to do in accordance with contract requirements.

H. Contents of the Notification

The notification shall be provided in writing, with few exceptions, as described in Subsection J below – “Means of Providing Notification”, and shall be concise, conspicuous, and in plain language. If it is known that the affected individual(s) are not English proficient, notice shall also be provided in the appropriate language(s).

The notice shall include the following elements:

1. A brief description of what happened, including the date(s) of the breach and of its discovery;

2. To the extent possible, a description of the types of personal information involved in the breach (*e.g.*, full name, Social Security number, date of birth, home address, account number, or disability code);

3. A statement clarifying whether the information was encrypted or protected by other means, if such information would be beneficial and would not compromise the security of the system;

4. What steps individuals should take to protect themselves from potential harm, if any;

5. What ED is doing, if anything, to investigate the breach, mitigate losses, and protect against any further breaches; and

6. The points of contact at ED for more information, which may include a toll-free telephone number, e-mail address, or postal address.

It is recommended that the most current information be attached to the external breach notification letter to help breach subjects understand their options and where they can go for more information.

I. Internal Review

After a letter is developed for external notification, it should be reviewed at the staff level by OGC, CIO, OCO, and the Senior Privacy Specialist. If a form letter has already been drafted and pre-approved for distribution for a common type of breach, and it has not been substantially altered, it need only be reviewed by the PAG. It should then be forwarded to the appropriate entity for signature.

For major incidents, the PIRT, and others at a senior level, as determined by the SAOP, will review and approve the letter.

J. Means of Providing Notification

1. First-class mail

   a. Notification to the last known mailing address of the individual(s) in ED's records is the primary means of external notification.

   b. If there is reason to believe the address is no longer current, ED shall take reasonable steps to update the address by consulting with other agencies such as the U.S. Postal Service.

c. The notice shall be sent separately from any other mailing so that it is conspicuous to the recipient.

d. If ED is using another agency to facilitate mailing (for example, consulting the Internal Revenue Service for current mailing addresses of affected individuals), ED, and not the facilitating agency, must be identified as the sender.

e. The front of the envelope shall be labeled to alert the recipient to the importance of its contents, *e.g.*, "Data Breach Information Enclosed" and shall be marked with the U.S. Department of Education as the sender in order to reduce the likelihood that the recipient thinks it is advertising mail.

2. Telephone

In cases where the impact is not widespread (100 data subjects or fewer), but where the harm may be great, and the issue is urgent, the telephone may be the most appropriate means of notification. In these cases, written notification by first-class mail shall follow as soon as practicable.

3. E-mail

a. The notification will usually not be provided by e-mail, unless an individual has provided an e-mail address, and has expressly consented to use e-mail as the primary means of communication with ED.

b. E-mail notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. For example, if the matter is urgent, the risk of harm is high, and there are large numbers of people affected, ED might use both regular mail and e-mail to reach an individual.

c. If a decision is made to use e-mail, such notification may include links to ED's website and USA Services web sites, where the notice may be "layered" so that the most important summary facts are up front with additional information provided under link headings.

K. Existing Government-Wide Services

In addition to the means discussed above, ED will use Government-wide services already in place to provide support services needed, such as USA Services, including the toll free number 1-800-FedInfo.

L. Newspapers or other Public Media Outlets

In matters that have been referred to the PIRT, the PIRT shall determine whether supplementing individual notification, such as with notification in newspapers or other public media outlets, is appropriate. The PIRT should work with the AS of OCO, the Senior Official of the Principal Office Experiencing the Breach, and the third party involved with the incident, if any, to make and implement this determination.

M. Substitute Notice

If ED does not have sufficient contact information to provide individual notification, substitute notice may be used. Substitute notice shall be coordinated through OCO and consist of a conspicuous posting of the notice on www.ed.gov and social media outlets, and notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media should include a toll-free phone number where an individual can learn whether or not his or her personal information is included in the breach.

N. Accommodations

Special consideration must be given to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973. Accommodations may include establishing a telephone number for those who use a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on ED's website.

O. Who Receives Notification: Public Outreach in Response to a Breach

1. Notification of Individuals. The PIRT shall determine to whom notice shall be provided. The PIRT should work with the Senior Official of the Principal Office Experiencing the Breach, and the Contracting Officer or COR, if any, to make and implement this determination. Parties may include the affected individuals, the public media, and/or other third parties (such as Members of Congress, academic institutions, financial partners, etc.) affected by the breach or the notification. This shall be done in accordance with the Privacy Act and any applicable exceptions to consent, such as if the disclosure is permissible pursuant to a published routine use. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, once it has been determined to provide notice regarding the breach, affected individuals must be notified promptly.

2. Notification of External Entities including the Media and Social Media Outlets

If it is determined that an external entity will be notified regarding a breach, the PIRT shall consider the following:

a. *Careful Planning.* ED's decision whether to notify the public media and/or social media, will require careful planning and execution so that it does not unnecessarily alarm the public when the risk of harm is, in fact, minimized. OCO, working in collaboration with the Principal Office Experiences the Breach, shall manage disclosure to the media or social media wherever a decision is made to provide such notification. OCO, working in collaboration with the Principal Office Experiencing the Breach, shall develop the notification and focus on providing information, including links to resources, to aid the public in its response to the breach. Notification may be delayed upon the request of law enforcement or national security agencies as described above.

b. *Web Posting.* OCO, working in collaboration with the Principal Office Experiencing the Breach, shall develop and post information about the breach and notification in a clearly identifiable location on ED's home page and social media outlets, as appropriate, as soon as possible after a decision is made to provide notification to the affected individuals. The posting shall also include a link to Frequently Asked Questions (FAQs) and other information to assist the public's understanding of the breach and the notification process. The PIRT shall also consider posting the information to the www.USA.gov web site. The PIRT shall also consult with GSA's USA Services regarding using that agency's call center. The PIRT should work with the AS of OCO, the Senior Official of the Principal Office Experiencing the Breach, and the third party involved with the incident, if any, to make and implement this determination.

c. *Notification of other Public and Private Sector Agencies.* The PIRT may determine that other public and private sector agencies should be notified on a need-to-know basis, particularly those agencies that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach. The PIRT should work with the AS of OCO, the Senior Official of the Principal Office Experiencing the Breach, and the third party involved with the incident, if any, to make and implement this determination.

d. *Congress.* The Office of Legislation and Congressional Affairs will lead efforts to notify Congress in the event of a major incident, in compliance with FISMA 2014, and in accordance with current OMB guidance. OLCA shall take the lead in developing responses to potential inquiries from Members of Congress.

e. For FSA breaches, the FSA Communications Office will collaborate with ED OCO for all outreach and communications.

## Appendix 1 – Acronym Table

| | |
|---|---|
| **AS** | **Assistant Secretary** |
| **CFO** | **Chief Financial Officer** |
| **CIO** | **Chief Information Officer** |
| **CO** | **Contracting Officer** |
| **COR** | **Contracting Officer Representative** |
| **CPO** | **Chief Privacy Officer** |
| **DHS** | **Department of Homeland Security** |
| **ED** | **Department of Education** |
| **EDCIRC** | **ED's Computer Incident Response Capability Coordinator** |
| **FAQ** | **Frequently Asked Questions** |
| **FISMA 2002** | **Federal Information Security Management Act of 2002** |
| **FISMA 2014** | **Federal Information Security Management Act of 2014** |
| **FSA** | **Federal Student Aid** |
| **GC** | **General Counsel** |
| **GSA** | **General Services Administration** |
| **IES** | **Institute of Education Sciences** |
| **IG** | **Inspector General** |
| **ISSO** | **Information Systems Security Officer** |
| **NIST** | **National Institute of Standards and Technology** |
| **OCIO** | **Office of the Chief Information Officer** |
| **OCO** | **Office of Communications and Outreach** |
| **OGC** | **Office of General Counsel** |
| **OLCA** | **Office of Legislation and Congressional Affairs** |
| **OMB** | **Office of Management and Budget** |
| **PAG** | **PIRT Advisory Group** |
| **PII** | **Personally Identifiable Information** |
| **PIRT** | **Privacy Incident Response Team** |
| **POC** | **Principal Office** |
| **SAOP** | **Senior Agency Official for Privacy** |
| **SPOC** | **Single Point of Contact** |
| **SPS** | **Senior Privacy Specialist** |
| **TDD** | **Telecommunications Device for the Deaf** |
| **US-CERT** | **United States Computer Emergency Readiness Team** |