U.S. Department of Justice **0900.00.01**

Approved On: August 6, 2013

DOJ Instruction

INCIDENT RESPONSE PROCEDURES FOR DATA BREACHES

PURPOSE:	This instruction establishes Department of Justice (DOJ) notification procedures and plans for responding to actual or suspected data breaches involving personally identifiable information (PII), company or business identifiable information, significant breaches of National Security Information (NSI) and significant cybersecurity incidents. It also identifies the DOJ Core Management Team (CMT) as the primary advisor to the Attorney General in making determinations regarding breach notification and as the review and oversight body for significant breaches of national security information and significant cybersecurity incidents.
SCOPE:	This Instruction applies to all DOJ components and contractors who operate systems supporting DOJ.
ORIGINATOR:	Justice Management Division (JMD), Office of the Chief Information Officer (OCIO)
CATEGORY:	(I) Administrative, (II) Information Technology
AUTHORITY:	DOJ Order 2880.1C, DOJ Order 2640.2F, and OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.*
CANCELLATION:	DOJ Incident Response Procedures for Data Breaches Involving Personally Identifiable Information, dated August 7, 2008.
DISTRIBUTION:	This Instruction is distributed electronically to those components referenced in the 'SCOPE' section as well as posted to the DOJ Directives electronic repository (SharePoint).
APPROVED BY:	*Luke J. McCormack* *Chief Information Officer (CIO)*

ACTION LOG

All DOJ directives are reviewed, at minimum, every five years and revisions are made as necessary. The action log records dates of approval, recertification, and cancellation, as well as major and minor revisions to this directive. A brief summary of all revisions will be noted. In the event this directive is cancelled, superseded, or supersedes another directive, that will also be noted in the action log.

Action	Authorized by	Date	Summary
Initial Approval	Luke J. McCormack	8/6/2013	Summary of Action

TABLE OF CONTENTS

GLOSSARY OF TERMS

Term	Definition
Breach	The term "breach" is used to include 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 information, whether physical or electronic. It includes both intrusions (from outside the organization) and misuse (from within the organization).
Classified National Security Information	''Classified national security information'' or ''classified information'' or NSI means information that has been determined pursuant to Executive Order 13526, Classified National Security Information," or any predecessor or successor order, to require protection against unauthorized disclosure and is required to be marked to indicate its classified status when in documentary form.
Company or business identifiable information	Identifying information about a company or other business entity that could be used to commit or facilitate the commission of fraud, deceptive practices or other crimes (for example, bank account information, trade secrets, confidential or proprietary business information).
Component	An Office, Board, Division, or Bureau of the Department of Justice as defined in 28 C.F.R. Part 0 Subpart A, Paragraph 0.1.
Cybersecurity incident	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.
Harm	For the purposes of this document, harm means any adverse effects that would be experienced by an individual or organization (e.g., that may be socially, physically, or financially damaging) whose information was breached, as well as any adverse effects experienced by the organization that maintains the information.
Identity Theft	The act of obtaining or using an individual's identifying information without authorization in an attempt to commit or facilitate the commission of fraud or other crimes. The resulting crimes usually occur in one of the following ways. Identity thieves may attempt to: • Gain unauthorized access to existing bank, investment, or credit accounts using information associated with the person • Withdraw or borrow money from existing accounts or charge purchases to the accounts • Open new accounts with a person's identifiable information without that person's knowledge

Term	Definition
	• Obtain driver's licenses, social security cards, passports, or other identification documents using the stolen identity
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, acceptable use policies or standard computer security practices.
National Security System	Has the meaning given it in the Federal Information Security Management Act of 2002 (FISMA, Title III, Public Law 107-347, December 17, 2002), codified at 44 U.S.C. 3542(b)(2). Components shall use National Institute of Standards and Technology Special Publication 800-59, "Guideline for Identifying an Information System as a National Security System," to identify National Security Systems.
Personally Identifiable Information (PII)	PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[1] Information that standing alone is not generally considered personally identifiable, because many people share the same trait, includes: • First or last name, if common (For example: Smith or Brown) • Country, state, city or Zip code of residence • Age, especially if non-specific (such as age in years, without a birth date) • Gender or race • Workplace or school • Grades, salary, or job position Sometimes multiple pieces of information, none of which alone may be considered personally identifiable, may uniquely identify a person when brought together.

[1] *National Institute of Standards and Technology Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010, footnote 6 "This definition is the GAO expression of an amalgam of the definitions of PII from OMB Memorandums 07-16 and 06-19. GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008.*

ACRONYMS

Acronym	Meaning
AAG/A	Assistant Attorney General for Administration
CIO	Chief Information Officer
CPCLO	Chief Privacy and Civil Liberties Officer
CCIPS	Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division
CO	Contracting Officer
COR	Contracting Officer's Representative
CMT	Core Management Team
DOJ	Department of Justice
DOJCERT	DOJ Computer Emergency Readiness Team
DSO	Department Security Officer
FTC	Federal Trade Commission
JSOC	Justice Security Operations Center
NSI	National Security Information
OLC	Office of Legal Counsel
OLA	Office of Legislative Affairs
OPA	Office of Public Affairs
OPCL	Office of Privacy and Civil Liberties
PII	Personally Identifiable Information
SSN	Social Security Number
US-CERT	United States Computer Emergency Readiness Team

I. Background

In September 2006, Office of Management and Budget (OMB) issued a Memorandum for the Heads of Departments and Agencies entitled "Recommendations for Identity Theft Related Data Breach Notification." In February 2007, DOJ issued the *U.S. Department of Justice Incident Response Procedures for Data Breaches Involving Personally Identifiable Information* implementing the recommendations in OMB's Memorandum. In May 2007, OMB issued Memorandum 07-16 entitled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," which requires agencies to develop and implement a notification policy for breaches of personally identifiable information (PII), including the establishment of an agency response team. DOJ subsequently modified its procedures to create the DOJ Core Management Team.

In October 2012, the Assistant Attorney General for Administration (AAG/A) expanded the responsibility of the DOJ Core Management Team (CMT) to include breaches of company or business identifiable information, significant breaches of classified national security information (NSI) and significant cybersecurity incidents.

This Instruction applies to all DOJ components, contractors that operate systems supporting DOJ, and all information regardless of format (e.g., paper, electronic, etc.). It defines the responsibilities of:

- DOJ Core Management Team (CMT)
- DOJ Computer Emergency Readiness Team (DOJ-CERT)
- All DOJ personnel, contractors, and others who process, store, or possess PII or NSI on behalf of DOJ, or are involved in cybersecurity incidents

This Instruction also establishes DOJ's notification policy and response plan for breaches of PII, company or business identifiable information, significant breaches of NSI and significant cybersecurity incidents. It supplements, but does not replace, the security and privacy requirements contained in the DOJ Security Program Operating Manual (SPOM); DOJ Order 2640.2F, *Information Technology Security* and DOJ Information Technology Security Standards; the DOJ Computer System Incident Response Plan; the Privacy Act of 1974, and DOJ Order 3011.1A, *Compliance with the Privacy Requirements of the Privacy Act, the E-Government Act and the FISMA*.

Procedures to respond to information security incidents involving the Department's information systems are located in the DOJ Computer System Incident Response Plan. This Plan focuses on protection and defense of DOJ systems and network against data loss and intrusive, abusive, and destructive behavior from both internal and external sources. For a description of computer security incidents, refer to National Institute of Standards and Technology (NIST) Special Publication 800-61, *Computer Security Incident Handling Guide*. Guidelines for a risk-based approach to protecting the confidentiality of PII are provided in NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. The SPOM prescribes requirements and procedures for the classification, safeguarding and

declassification of classified national security information (NSI), including reporting of any incident involving a possible loss, compromise, or suspected compromise of sensitive or classified information.

II. DOJ Core Management Team

The DOJ Core Management Team (CMT) is the organizational backbone for the DOJ response to an actual or suspected data breach involving PII, company or business identifiable information, significant breaches of NSI and significant cybersecurity incidents. The CMT is the primary advisor to the Attorney General in making determinations regarding breach notification.

As discussed in Section V, the CMT convenes in the event of certain significant data breaches or cybersecurity incidents. The CMT is responsible for:

- Determining the extent to which the incident poses problems related to identity theft, loss of individuals', companies', or businesses' privacy or confidentiality, or the security of DOJ information and systems

- Managing activities to recover from the breach and mitigate the resulting damage, including decisions relating to external breach notification

The DOJ CMT is chaired by the Chief Information Officer and Chief Privacy and Civil Liberties Officer and is supported by the staff members of each of the offices represented and reports to the Assistant Attorney General for Administration. The DOJ CMT consists of the following members:

- Representative from the Office of Attorney General

- Principal Associate Deputy Attorney General

- Associate Attorney General

- Assistant Attorney General, Office of Legal Counsel

- Assistant Attorney General, Office of Legislative Affairs

- Assistant Attorney General, Administration

- Assistant Attorney General, Civil Division

- Chief Information Officer

- Chief Privacy and Civil Liberties Officer

- Director, Office of Privacy and Civil Liberties

- Department Security Officer

- Inspector General
- Director, Office of Public Affairs

Program Manager and Senior Component Official for Privacy, Executive Officer, and legal counsel from component experiencing breach or incident

The DOJ CMT should convene at least annually to review these procedures and discuss likely actions should an incident occur.

III. Incident Detection and Reporting

A. Requirement for Reporting

Components must report actual or suspected data breaches, significant breaches of NSI and significant cybersecurity incidents to DOJCERT within one hour of discovery[2].

1. Additional Component Requirements

   The following individuals should be notified of the incident within their component; should support the investigation, mitigation and recovery efforts of the DOJ CMT; and should meet, as appropriate.

   - Component Head or designee
   - Component Chief Information Officer
   - Senior Component Official for Privacy, Executive Officer, and legal counsel
   - Component Security Program Manager[3]
   - Incident response team representative
   - Owner or manager of the system from which the loss occurred

2. Additional Contractor Requirements

   Contractors must notify the Contracting Officer (CO), the Contracting Officer's Representative (COR) and DOJCERT within one hour of discovery of any data breach, significant breaches of NSI or significant cybersecurity incident. Contractors shall cooperate with all aspects of DOJ's investigation, assessment, mitigation, and recovery activities.

[2] *Components must also report incidents falling under SPOM Section 1-302,* ***Incident and Vulnerability Reporting,*** *to the Department Security Officer through their Security Program Manager.*
[3] *Pursuant to SPOM Section 1-303, the SPM will initiate a preliminary inquiry to ascertain all the circumstances surrounding the incident.*

B. Incident Record

DOJCERT will work with the reporting Component to record the incident information in the DOJCERT Incident Tracking System. The record should contain the following:

- Description of the data lost, including the amount and its sensitivity or classification level
- For cybersecurity incidents, the nature of the cyber threat (e.g., Advanced Persistent Threat, Zero Day Threat, data exfiltration)
- Nature and number of persons affected (e.g., employees, outside individuals)
- Likelihood data is accessible and usable
    - Likelihood the data was intentionally targeted
    - Evidence that the compromised information is actually being used to commit identity theft
    - Strength and effectiveness of security technologies protecting data
- Likelihood the breach may lead to harm and the type of harm
- Ability to mitigate the risk of harm

DOJCERT will notify the DSO and OIG of all reported breaches and incidents.

C. Initial Assessment

The DSO will assess data breaches and incidents involving classified information with support from DOJCERT. DOJCERT will assess all other data breaches and incidents. The assessment will be based on the details included in the incident report and will assign an initial potential impact level of Low, Moderate, or High[4]. The potential impact levels describe the worst case potential impact on a component, person, company or business of the breach or incident.

- Low: the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
- Moderate: the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

[4] *National Institute of Standards and Technologies Federal Information Processing Standards Publication (FIPS PUB) 199, "Standards for Security Categorization of Federal Information and Information Systems."*

- High: the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

D. Criminal Investigation

DOJCERT will also work with the Criminal Division, Computer Crime and Intellectual Property Section (CCIPS), to determine whether further investigation is warranted by law enforcement. As appropriate, CCIPS will notify the Federal Bureau of Investigation.

E. Incident Notification

DOJCERT will notify US-CERT within the OMB-mandated one hour timeframe for incidents involving PII and within US-CERT established timeframes for other incidents, and will start the internal alerting and notification process.

IV. Internal Notification Process

A. Requirement for Initial Notification

For incidents with an initial risk rating of either Moderate or High, or that may receive particular notoriety, DOJCERT will, within 72 hours of the incident being reported to DOJCERT, send an initial e-mail notification to the following:

- Office of the Inspector General
- Office of Privacy and Civil Liberties
- Office of the Chief Information Officer
- Civil Division
- Security and Emergency Planning Staff
- Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division
- Office of Public Affairs

B. Contents of the Notification

The e-mail shall contain the known details of the incident, DOJCERT's initial risk rating, as well as the actions that have been taken to respond to the incident thus far.

V. Risk Assessment

A. Incident Analysis

After initial notification, DOJCERT will perform a more thorough analysis of the incident, using the factors used in the initial assessment (section III.B. above) and additional information that becomes available, including reassessing the risk rating.

B. Summary of Facts with Recommendations

Following the analysis, DOJCERT will prepare a *Summary of Facts with Recommendations* for Moderate or High risk incidents and forward it to the CIO and CPCLO, in their capacity as co-chairs of the DOJ CMT. The CIO and CPCLO will then notify the members of the DOJ CMT.

C. AAG/A Notification and Meeting Determination

If the risk is high, the CIO and CPCLO will also notify the Assistant Attorney General for Administration (AAG/A), who will decide whether to convene a meeting of the DOJ CMT.

D. Other Meeting Determination

The CIO, CPCLO or the AAG/A may also, at their discretion, convene a meeting of the DOJ CMT to address specific incidents assessed at a low or moderate risk level.

VI. Incident Handling and Response

A. Course of Action

The component experiencing the breach or incident, or the CMT for breaches and incidents handled by the CMT, will determine the appropriate course of action, including notification to affected individuals (discussed in the next section), the resources needed, and any appropriate remedy options. The component experiencing the breach or incident may consult with the CMT in developing an appropriate course of action.

B. Risk Mitigation

The component experiencing the breach or incident, or the CMT for breaches and incidents handled by the CMT, will simultaneously consider options for mitigating the risk. The component experiencing the breach or incident may consult with the CMT in developing appropriate mitigation options. The following are actions that can be taken by DOJ or the contractor to mitigate the risk from loss of PII, and actions that individuals can routinely take to mitigate their risk:

1. Actions that Can Be Taken to Mitigate the Risk from Loss of PII

    - If the breach involves individuals' banking, credit card, or other financial PII, DOJ or the contractor should notify the individuals and inform them of steps that they should take to mitigate the risk. Written notification

procedures are contained in Appendix A. Where necessary, the Department or contractor should assist the individuals' mitigation efforts.

- If the breach involves a large volume of users, DOJ or the contractor should consider establishing a Help Line that allows affected users to call in to DOJ or the contractor to learn information. Appendix B contains more information regarding the procedures for establishing a Help Line.

- If the breach of PII has the potential to compromise the physical safety of the individuals involved, DOJ should ensure that the appropriate law enforcement agencies are notified and that the agencies take appropriate protective action.

- If the breach involves government-authorized credit cards (such as a loss of a card or card number), DOJ should notify the issuing bank promptly. If the breach involves individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit payment, DOJ should notify the bank or other entity that handles that particular transaction for DOJ.

- DOJ or the contractor may take two other significant steps that can offer additional measures of protection but which will involve DOJ or contractor expense. They are:

    - Data Breach Analysis – Using available technology or services, analyze whether a particular data loss appears to be resulting in identity theft. DOJ or the contractor may consider using this measure if it is uncertain about whether the identity-theft risk warrants implementing more costly additional steps or if it wishes to do more than rely on individual actions.

    - Credit Monitoring – In deciding whether to offer credit monitoring services and of what type and length, DOJ should consider the seriousness of the risk of identity theft arising from the data breach involving PII. A particularly important consideration is whether any identity theft incidents have already been detected. The cost of the service should also be considered. To assist the timely implementation of either data breach analysis or credit monitoring, the General Services Administration (GSA) is putting in place several government-wide contracting methods to provide these services if needed. If a contractor is responsible for the data breach involving PII, the contractor may provide credit monitoring and/or other corrective action in coordination with the Department.

2. Actions that Individuals Can Routinely Take to Mitigate the Risk

    - Contact their financial institution to determine whether their account(s) should be monitored or closed. This option is relevant only when financial account information Monitor their financial account statements and immediately report any suspicious or unusual activity to their financial institution.

    - Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. It may take a few months for most signs of fraudulent account activity to appear on the credit report. This option is most useful when the data breach involves information that can be used to open new accounts.

    - Contact the three major credit bureaus and place an initial fraud alert on credit reports maintained by each of the credit bureaus. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs.

    - For residents of states in which state law authorizes a credit freeze, consider placing a credit freeze on their credit file. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs.

    - For deployed members of the military, consider placing an active duty alert on their credit file. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs.

    - Review resources provided on the Federal Trade Commission (FTC) Identity Theft Website.

    - Complete a Federal Trade Commission ID Theft Affidavit at the above FTC Website. This will allow an individual to legally notify their creditors that their identity has been compromised. Any debts incurred after that date will not be assigned to them.

    - Be aware that the public announcement of the breach could itself cause criminals engaged in fraud to use various techniques to deceive individuals affected by the breach into disclosing their personal information.

3. Congressional Notification

    The CMT will also determine whether Congress should be notified.

VII. External Breach Notification

Components and the CMT will consider the following six elements when considering external notification:

- Whether breach notification is required
- Timeliness of the notification
- Source of the notification
- Contents of the notification
- Means of providing the notification
- Who receives notification: public outreach in response to a breach

A more detailed description of these elements is set forth below:

A. Whether Breach Notification is Required

To determine whether notification of a breach is required, the likely risk of harm caused by the breach and then the level of risk must be assessed. A wide range of harms should be considered, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach.[5] Notification when there is little or no risk of harm might create unnecessary concern and confusion[6]. Additionally, under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.

Five factors should be considered to assess the likely risk of harm:

1. 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.[7] It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A

[5] *For reference, the express language of the Privacy Act requires agencies to consider a wide range of harms: agencies shall "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." 5 U.S.C. § 552a (e)(10).*

[6] *Another consideration is a surfeit of notices, resulting from notification criteria which are too strict, could render all such notices less effective, because consumers could become numb to them and fail to act when risks are truly significant.*

[7] *For example, 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.*

name in one context may be less sensitive than in another context.[8] In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

2. Number of Individuals Affected. The number of affected individuals may dictate the method(s) the component chooses for providing notification, but should not be the determining factor for whether a notification should be provided.

3. Likelihood the Information is Accessible and Usable. Assess the likelihood information will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the decision to provide notification.

   The fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals, however, depending upon a number of physical, technological, and procedural safeguards employed by the component. If the information is properly protected by encryption that has been validated by NIST, for example, the risk of compromise may be low to non-existent.

4. Likelihood the Breach May Lead to Harm.

   a. *Broad Reach of Potential Harm.* The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained" (5 USC 552a(e)(10)). Additionally, the analysis should 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, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

   b. *Likelihood Harm Will Occur.* The likelihood 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 to committing identity theft, as are date of birth, passwords, and mother's maiden name. If the information involved, however, 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.

[8] *For example, breach of a database of names of individuals receiving treatment for contagious disease may pose a higher risk of harm, whereas a database of names of subscribers to agency media alerts may pose a lower risk of harm.*

5. Ability to Mitigate the Risk of Harm. Within an information system, the risk of harm will depend on how the component 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.[9] 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 may be difficult to determine.

B. Timeliness of the Notification

Components should provide notification without unreasonable delay following the discovery of a breach, consistent with the needs of public or national security; official inquiries, investigations or proceedings; the prevention, detection, investigation, or prosecution of criminal offenses; the rights and freedoms of others, in particular the protection of victims and witnesses; and any measures necessary for the component to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized data system compromised.

Decisions to delay notification should be made by the component head or a senior-level individual he/she may designate in writing. In some circumstances, law enforcement or national security considerations may require a delay if it would seriously impede the investigation of the breach or the affected parties. However, any delay should not exacerbate risk or harm to any affected individual(s).

In cases where a contractor processes, stores, possesses, or otherwise handles the PII that is the subject of a data breach, any notification to individuals affected by the data breach must be coordinated with the Department. No notification by the contractor may proceed until the Department has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by the contractor must be coordinated with, and is subject to the approval of, the Department.

C. Source of the Notification

In general, notification to parties affected by the breach should be issued by the Component Head, or senior-level individual he/she may designate in writing. This demonstrates it has the attention of the chief executive of the organization. Notification involving only a limited number of persons (*e.g.*, under 50) may also be issued jointly under the auspices of the Chief Information Officer and the Chief Privacy Officer or Senior Agency Official for Privacy. This approach signals the component recognizes both the security and privacy concerns raised by the breach.

[9] *For example, if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address may signal fraudulent activity.*

When the breach involves a Federal contractor or a public-private partnership operating a system of records on behalf of a component, the component is responsible for ensuring any notification and corrective actions are taken. The roles, responsibilities, and relationships with contractors or partners must be reflected in contracts and other documents.

D. Contents of the Notification

The notification should be provided in writing and should use concise, conspicuous, plain language. The notice should include the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery
- 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, disability code, etc.)
- A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise the security of the system
- What steps affected parties should take to protect themselves from potential harm, if any
- What is being done, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches
- Who affected parties should contact for more information, including a toll-free telephone number, e-mail address, and postal address

Given the amount of information required above, the component may want to consider layering the information, providing the most important information up front, with the additional details in a Frequently Asked Questions (FAQ) format or on the component's web site. If the component has knowledge that the affected parties are not English speaking, notice should also be provided in the appropriate language(s). See Appendix A for samples of written notifications.

E. Means of Providing Notification

The best means for providing notification will depend on the number of persons affected and what contact information is available about the affected parties. Notice provided to persons affected by a breach should be commensurate with the number of persons affected and the urgency with which they need to receive notice. The following examples are types of notice which may be considered.

- Telephone. Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification and/or when a

limited number of persons are affected. Telephone notification, however, should be contemporaneous with written notification by first-class mail.

- First-Class Mail. First-class mail notification to the last known mailing address of the persons in the component's records should be the primary means notification is provided. Where the component has reason to believe the address is no longer current, it should take reasonable steps to update the address by consulting with other agencies such as the US Postal Service. The notice should be sent separately from any other mailing so that it is conspicuous to the recipient. If the component which experienced the breach uses another agency to facilitate mailing (for example, if the component which suffered the loss consults the Internal Revenue Service for current mailing addresses of affected persons), care should be taken to ensure the component which suffered the loss is identified as the sender, and not the facilitating agency. The front of the envelope should be labeled to alert the recipient to the importance of its contents, *e.g.*, "Data Breach Information Enclosed" and should be marked with the name of the component as the sender to reduce the likelihood the recipient thinks it is advertising mail.

- E-Mail. E-mail notification is problematic, because individuals change their e-mail addresses and often do not notify third parties of the change. Notification by postal mail is preferable. However, where an individual has provided an e-mail address and has expressly given consent to e-mail as the primary means of communication with the component, and no known mailing address is available, notification by e-mail may be appropriate. E-mail notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. E-mail notification may include links to the component and www.USA.gov web sites, where the notice may be "layered" so the most important summary facts are up front with additional information provided under link headings.

- Existing Government Wide Services. Agencies should use Government wide services already in place to provide support services needed, such as USA Services, including toll free number of 1-800-FedInfo and www.USA.gov.

- Newspapers or other Public Media Outlets. Additionally, the component may supplement individual notification with placing notifications in newspapers or other public media outlets. The component should also set up toll-free call centers staffed by trained personnel to handle inquiries from the affected parties and the public.

- Substitute Notice. Substitute notice in those instances where the component does not have sufficient contact information to provide notification. Substitute notice should consist of a conspicuous posting of the notice on the home page of the component's web site and notification to major print and broadcast media, including major media in areas where the affected parties 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.

- Accommodations. Special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973 should be given. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on the component web site.

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

- Notification of Individuals. The final consideration in the notification process when providing notice is who should receive notification: the affected individuals, the public media, and/or other third parties affected by the breach or the notification. 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 should receive prompt notification.

- Notification of Third Parties including the Media. If communicating with third parties regarding a breach, agencies should consider the following.

    - *Careful Planning.* A component's decision to notify the public media will require careful planning and execution so that it does not unnecessarily alarm the public. When appropriate, the component should notify public media as soon as possible after the discovery of a breach and the response plan, including the notification, has been developed. Notification should 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 in Section VII.B. To the extent possible, prompt public media disclosure is generally preferable because delayed notification may erode public trust.

    - *Web Posting.* Agencies should post information about the breach and notification in a clearly identifiable location on the home page of the component web site as soon as possible after the discovery of a breach and the decision to provide notification to the affected parties. The posting should include a link to Frequently Asked Questions (FAQ) and other talking points to assist the public's understanding of the breach and the notification process. The information should also appear on the www.USA.gov web site. The component may also consult with the General Services Administration's USA Services regarding using their call center.

- *Notification of other Public and Private Sector Agencies.* Other public and private sector agencies may need to be notified on a need-to-know basis, particularly those that may be affected by the breach or may play a role in mitigating the potential harm stemming from the breach.[10]

- *Congressional Inquiries.* Agencies should be prepared to respond to inquiries from other governmental agencies such as the Government Accountability Office and Congress.

- Reassess the Level of Impact Assigned to the Information. After evaluating each of these factors, the component should review and reassess the level of impact it has already assigned to the information using the impact levels defined by the NIST.

[10] *For example, a breach involving medical information may warrant notification of the breach to health care providers and insurers through the public or specialized health media, and a breach of financial information may warrant notification to financial institutions through the federal banking agencies.*

APPENDIX A

Sample Written Notifications

DATA ACQUIRED: Social Security Number (SSN)
(Note: Do not insert actual SSN)

Dear :

We are writing to you because of a recent security incident at [DOJ or name of Component]. [Describe what happened in general terms, what kind of PII was involved, and what you are doing in response.]

To protect yourself from the possibility of identity theft, we recommend that you complete a Federal Trade Commission ID Threat Affidavit. This will allow you to legally notify your creditors that your identity may have been compromised. Any debts incurred after that date will not be assigned to you.

We also recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289

Look your credit reports over carefully when you receive them. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personally identifiable information, such as home address or Social Security Number that is not accurate.

If you see anything you do not understand, call the credit reporting agency at the telephone number on your report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [Or, if appropriate, give contact number for law enforcement agency investigating the incident.] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you visit the Identity Theft Website of the Federal Trade Commission. If there is anything [DOJ or name of Component] can do to assist you, please call [toll-free telephone number].

[Closing]

DATA ACQUIRED: Credit Card Number or Financial Account Number Only
(Note: Do not insert actual credit card or financial account numbers)

Dear :

We are writing to you because of a recent security incident at [DOJ or name of Component]. [Describe what happened in general terms, what type of PII was involved, and what DOJ is doing in response.]

To protect yourself from the possibility of identity theft, we recommend that you immediately contact [credit card or financial account issuer] at [phone number] and close your account. Tell them that your account may have been compromised.

We also recommend that you complete a Federal Trade Commission ID Threat Affidavit. This will allow you to legally notify your creditors that your identity has been compromised. Any debts incurred after that date will not be assigned to you.

In addition, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289

Look your credit reports over carefully when you receive them. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personally identifiable information, such as home address or Social Security Number that is not accurate.

If you see anything you do not understand, call the credit reporting agency at the telephone number on your report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [Or, if appropriate, give contact number for law enforcement agency investigating the incident.] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you visit the Identity Theft Website of the Federal Trade Commission. If there is anything [DOJ or name of Component] can do to assist you, please call [toll-free telephone number].

[Closing]

APPENDIX B

General Guidance for the Establishment of a Call Center in the Event of a Significant Data Breach

In the event of a significant data breach involving PII, the following guidance is provided to help with the determination of whether to establish a call center. The purpose of a call center is to provide individuals a number to call to obtain further information regarding the data loss and possible action they may want to take to lessen the incident's impact on their personal lives.

The decision to establish a call center should be based on several considerations:

- If a data breach does not extend outside of a Component (i.e., those affected by the breach are known and can be contacted), the establishment of a call center would not normally be necessary

- If the breach affects a large number of individuals and those individuals are not easily identifiable or easily contacted, establishment of a call center should be considered to allow those potentially impacted to call and obtain additional information regarding the breach

- Each situation will be unique and the decision to establish a call center must be based on individual circumstances. The main concern should be sharing of information with those affected and how they may obtain assistance.

Once a decision is made to establish a call center, there are several options:

- Contact the National Business Center to obtain a toll-free number. This option is likely the least expensive, since DOJ would provide its own personnel to support the call center.

- Contact General Service Administration's (GSA) USA Contact to establish a fully supported and staffed call center. A thorough description of the incident and set of frequently asked questions (FAQs) will also be required for call center to refer to when fielding calls.

Suggested items to consider based on the nature of the breach would include, but are not limited to, the following:

- Using existing DOJ personnel to staff the call center and the number of individuals required

- Training of call center operators

- Pre-stage FAQs

- Ability to adjust staffing in response to call volume

- Daily hours of operations

- Cost of service
- Call logging
- DOJ reporting requirements
- Advertising call center numbers and making data breach information readily available to those affected
- Quality assurance checks of call center effectiveness

Sample call center FAQs are as follows:

1. How can I tell if my information was compromised?

   At this point, there is no evidence that any missing data has been used illegally. However, the DOJ/Component is asking each individual to be extra vigilant and to carefully monitor bank statements, credit card statements, and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved.

2. What is the earliest date at which suspicious activity might have occurred due to this data breach?

   The information was stolen from an employee of the DOJ/Component during the month of _____. If the data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that individuals may notice suspicious activity during the month of _____.

3. I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself from being victimized by credit card fraud or identity theft?

   The DOJ/Component strongly recommends that individuals closely monitor their financial statements and visit the DOJ/Component special Website at www._____.gov.

4. Should I reach out to my financial institutions or will the DOJ/Component do this for me?

   The DOJ/Component does not believe that it is necessary to contact financial institutions or cancel credit cards and bank accounts, unless you detect suspicious activity.

5. Where should I report suspicious or unusual activity?

   The Federal Trade Commission (FTC) Identity Theft web site (http://www.consumer.ftc.gov/features/feature-0014-identity-theft) recommends the following steps if you detect suspicious activity:

- Immediate Steps
  - Place an Initial Fraud Alert

    Contact the fraud department of one of the three major credit bureaus:

    - Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
    - Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
    - TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
  - Order Your Credit Report from the three major credit bureaus above
  - Create an Identity Theft Report
    - Submit a report about the theft to the FTC online or call the FTC at 1-877-438-4338 (1-866-653-4261 – TTY). When you finish writing all the details, print a copy of the report. It will be called an Identity Theft Affidavit. Bring your FTC Identity Theft Affidavit when you file a police report.
    - File a police report with your local police department or the police department where the theft occurred, and get a copy of the police report or the report number. Your FTC Identity Theft Affidavit and your police report make an Identity Theft Report.
- Extended Fraud Alerts and Credit Freezes
  - Extended Fraud Alerts. If you've created an Identity Theft Report, you can get an extended fraud alert on your credit file. When you place an extended alert, you can get 2 free credit reports within 12 months from each of the 3 nationwide credit reporting companies, and the credit reporting companies must take your name off marketing lists for prescreened credit offers for 5 years, unless you ask them to put your name back on the list. The extended alert lasts for 7 years.
  - Credit Freezes. You may choose to put a credit freeze on your file. But a credit freeze may not stop misuse of your existing accounts or some other types of identity theft. Also, companies that you do business with would still have access to your credit report for some purposes. A fraud alert will allow some creditors to get your report as long as they verify your identity.
- Close any accounts that have been tampered with or opened fraudulently

FTC also has a printed publication called Taking Charge, What To Do If Your Identity Is Stolen

6. What is the DOJ/Component doing to ensure that this does not happen again?

   The DOJ/Component is working with the FTC to investigate the data breach and to develop safeguard against similar incidents. The DOJ/Component has directed all employees to complete the DOJ "Computer Security Awareness and Training (CSAT)" course. In addition, the DOJ/Component will immediately be conducting an inventory and review of all current positions requiring access to PII and require all employees needing access to PII to undergo an updated National Agency Check and Inquiries (NACI) and/or a Minimum Background Investigation (MBI), depending on the level of access required by the responsibilities associated with their position. Appropriate law enforcement agencies, including the Federal Bureau of Investigation and the DOJ Office of the Inspector General have launched full-scale investigations into this matter.

7. Where can I get further, up-to-date information?

   The DOJ/Component has set up a special Website which features up-to-date news and information. Please visit www._____.gov.

8. Does the data breach affect only certain individuals?

   It potentially affects a large population of individuals. We urge everyone possibly affected to be extra vigilant and monitor their financial accounts.

APPENDIX C

References

The following references are applicable to this Instruction. Unless otherwise stated, all references to publications are to the most recent version of the referenced publication.

1. Congressional Mandates

a. Clinger Cohen Act of 1996, (Pub. L. 104-106, 110 Stat. 186); and (Pub. L. 104-208, 110 Stat. 3009).
b. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511.
c. E-Government Act of 2002, PL 107-347, 44 U.S.C. Ch 35.
d. Federal Information Security Management Act of 2002 (FISMA), Pub. L. 107-347, 116 Stat. 2899.
e. Freedom of Information Act (FOIA), 5 U.S.C. § 552.
f. Privacy Act of 1974, 5 U.S.C. § 552a.

2. Federal/Departmental Regulations/Guidance

a. DOJ Order 2880.1B, Information Resources Management.
b. DOJ Order 2640.2F, Information Technology Security.
c. DOJ Order 3011.1A, Compliance with the Privacy Requirements of the Privacy Act, the E-Government Act and the FISMA.
d. DOJ Computer System Incident Response Plan.
e. DOJ Information Technology Security Standards.
f. DOJ Security Program Operating Manual (SPOM).

3. Presidential and Office of Management and Budget Guidance

a. OMB Circular A-130, Management of Federal Information Resources (with Appendices and periodic revisions).
b. OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.