EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

January 3, 2017

M-17-12

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director

SUBJECT: Preparing for and Responding to a Breach of Personally Identifiable Information

I. Introduction

This Memorandum sets forth the policy for Federal agencies to prepare for and respond to a breach of personally identifiable information (PII). It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. This Memorandum is intended to promote consistency in the way agencies prepare for and respond to a breach by requiring common standards and processes. While promoting consistency, this Memorandum also provides agencies with the flexibility to tailor their response to a breach based upon the specific facts and circumstances of each breach and the analysis of the risk of harm to potentially affected individuals.

This Memorandum reflects certain changes to laws, policies, and best practices that have emerged since the Office of Management and Budget (OMB) first required agencies to develop plans to respond to a breach. In particular, this Memorandum updates existing OMB breach notification policies and guidelines in accordance with the Federal Information Security Modernization Act of 2014 (FISMA)[1] and implements recommendations included in OMB Memorandum M-16-04.[2]

The primary audience for this Memorandum is the agency's Senior Agency Official for Privacy (SAOP) as well as other senior agency officials, managers, and staff who help evaluate the risk of harm to individuals potentially affected by a breach. In addition, sections of this Memorandum are relevant for an agency's Chief Information Officer (CIO), Senior Agency Information Security Officer[3] (*e.g.*, Chief Information Security Officer (CISO)), and other information technology (IT) and cybersecurity staff who participate in breach response activities. This Memorandum does not provide a comprehensive account of all the statutory and policy

---

[1] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073 (Dec. 18, 2014) (primarily codified at 44 U.S.C. chapter 35, subchapter II).
[2] OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for Federal Civilian Government* (Oct. 30, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.
[3] *See* 44 U.S.C. § 3554(a)(3).

requirements associated with preparing for and responding to an incident or a breach. Moreover, this Memorandum does not set policy related to information security, protecting against malicious cyber activities, technical methods and controls to detect incidents, or activities related to the management of cyber incidents more generally such as threat mitigation, threat response, collecting evidence from computing resources, containment strategies, identifying adversaries, and maintaining operational continuity or intelligence activities. Agencies shall consult law, regulation, and policy, including OMB guidance, National Institute of Standards and Technology (NIST) standards and guidelines, and Department of Homeland Security (DHS) binding operational directives to understand all applicable requirements for responding to a breach. At a minimum, agencies should consider the government-wide incident and breach response resources included as Appendix IV to this Memorandum when responding to an incident or a breach.

The policies set forth in this Memorandum are the minimum requirements that agencies shall follow when responding to a breach. Agencies may impose stricter standards consistent with their missions, authorities, circumstances, and identified risks.

This Memorandum rescinds and replaces the following previously issued OMB memoranda:

- OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007);
- *Recommendations for Identity Theft Related Data Breach Notification* (Sept. 20, 2006);
- OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 12, 2006); and
- OMB M-06-15, *Safeguarding Personally Identifiable Information* (May 22, 2006).

Table of Contents

I. Introduction 1
II. The Evolving Threat and Risk Landscape 5
III. Scope 8
A. Agency Federal Information and Information Systems 8
B. Personally Identifiable Information 8
C. Definition of a Breach 9
IV. Training and Awareness Campaigns 10
V. Preparing for a Breach 10
A. Privacy Act Routine Uses Required to Respond to a Breach 10
B. Contracts and Contractor Requirements for Breach Response 11
C. Grants and Grantee Requirements for Breach Response 13
D. Identifying Logistical and Technical Support to Respond to a Breach 13
VI. Reporting a Suspected or Confirmed Breach 14
VII. Breach Response Plan 15
A. Breach Response Team 16
B. Identifying Applicable Privacy Compliance Documentation 18
C. Information Sharing to Respond to a Breach 18
D. Reporting Requirements 19
1. Reporting to US-CERT 19
2. Reporting to Law Enforcement, the Inspector General, and General Counsel 19
3. Reporting to Congress 20
E. Assessing the Risk of Harm to Individuals Potentially Affected by a Breach 20
1. Risk of Harm to Individuals 20
2. Factors for Assessing the Risk of Harm to Potentially Affected Individuals 21
a. Nature and Sensitivity of PII 21
b. Likelihood of Access and Use of PII 23
c. Type of Breach 26
F. Mitigating the Risk of Harm to Individuals Potentially Affected by a Breach 27
1. Countermeasures 28
2. Guidance 28
3. Services 28

G. Notifying Individuals Potentially Affected by a Breach 29
1. Source of the Notification 30
2. Timeliness of the Notification 31
3. Contents of the Notification 31
4. Method of Notification 32
5. Special Considerations 33
VIII. Tracking and Documenting the Response to a Breach 34
IX. Lessons Learned 35
X. Tabletop Exercises and Annual Plan Reviews 35
A. Tabletop Exercises 35
B. Annual Breach Response Plan Reviews 35
XI. Annual FISMA Reports 36
XII. Implementation 36
Appendix I: Model Breach Reporting Template 38
Appendix II: Examples of Guidance an Agency May Offer 42
Appendix III: Examples of Services an Agency May Provide 44
Appendix IV: Government-wide Incident and Breach Response Resources 45
Glossary 47

II. The Evolving Threat and Risk Landscape

In today's information-driven economy, Federal agencies create, collect, use, process, store, maintain, disseminate, disclose, and dispose of unprecedented volumes of PII. Agencies increasingly depend on their ability to interact with the public through myriad digital services, leverage cutting-edge technologies to more efficiently collect and process information, and employ big data analytics to make informed decisions.[4] Beyond collecting greater volumes of PII, advancements in technology enable agencies to generate and maintain increasingly diverse and sensitive datasets about individuals. The PII may range from common data elements such as names, addresses, dates of birth, and places of employment, to identity documents, Social Security numbers (SSNs) or other government-issued identifiers, precise location information, medical history, and biometrics.

The Federal Government is expected to protect the information entrusted to it by the American people and one of the most important and pressing challenges for Federal agencies is protecting their IT systems, networks, and information from sophisticated and persistent cyber threats.[5] Today, Federal information and information systems are increasingly the targets of sophisticated attacks by actors who want to sell or trade stolen PII on criminal exchanges or use the information for other malicious purposes. Between Fiscal Years (FYs) 2013 and 2015, there was a 27 percent increase in the number of incidents reported by Federal agencies to the DHS United States Computer Emergency Readiness Team (US-CERT). These incidents have the potential to place sensitive information at risk and to pose serious threats to individuals and Federal operations and assets.[6]

Over the past decade, discussions about the risk of harm to individuals resulting from a breach have generally focused on financial- or credit-related identity theft such as using a stolen credit card number, opening a new bank account, or applying for credit in another person's name. Today, however, malicious actors use stolen PII, modern technology, and forged identity documents to:

- seek employment;[7]

---

[4] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), *available at* https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[5] *Strengthening the Federal Cybersecurity Workforce*, WHITE HOUSE, *available at* https://www.whitehouse.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce (accessed Dec. 28, 2016).

[6] OFFICE OF MGMT. & BUDGET, ANNUAL REPORT TO CONGRESS: FEDERAL INFORMATION SECURITY MODERNIZATION ACT (2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf.

[7] *See Document Fraud in Employment Authorization: How an E-Verify Requirement Can Help: Hearing Before the Subcomm. on Immigration Policy and Enforcement of the H. Comm. on the Judiciary*, 112th Cong. (2012) (statement of Waldemar Rodriguez, Deputy Assistant Director, Transnational Crime and Public Safety Division), *available at* https://www.ice.gov/doclib/news/library/speeches/120418rodriguez.pdf ("Fraudulent documents are often used to obtain genuine government issued documents for employment purposes.").

- travel across international borders;[8]
- obtain prescription drugs;[9]
- receive medical treatment;[10]
- claim benefits;[11]
- file false tax returns;[12] and
- aid in other criminal activities.[13]

Additionally, identity theft — the harm most often associated with a breach — remains a significant problem in the United States. Identity theft represented 16 percent (490,220) of the over 3 million complaints received by the Federal Trade Commission (FTC) in 2015.[14] In 2014, the Department of Justice reported that 17.6 million individuals, or 7 percent of all U.S. residents age 16 or older, were victims of one or more occurrences of identity theft.[15] Moreover, new types of identity theft are emerging, such as synthetic identity theft, which occurs when a malicious actor constructs a new identity using a composite of multiple individuals' legitimate information along with fabricated information.[16]

---

[8] *See Passport and Visa Fraud: A Quick Course*, U.S. DEP'T OF STATE, *available at* http://www.state.gov/m/ds/investigat/c10714.htm (accessed Sept. 15, 2016) ("In Fiscal Year 2012, DS investigated over 3,900 new cases of passport and visa fraud, and made more than 440 arrests.").

[9] *Medical Identity Theft*, FED. TRADE COMM'N, *available at* https://www.consumer.ftc.gov/articles/0171-medical-identity-theft (accessed Sept. 15, 2016) ("A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care.").

[10] THE DEP'T OF HEALTH & HUMAN SERVIC. & THE DEP'T OF J. HEALTH CARE FRAUD & ABUSE CONTROL PROGRAM ANN. REP. FOR FISCAL YEAR 2014 (2015), *available at* https://oig.hhs.gov/publications/docs/hcfac/FY2014-hcfac.pdf (reporting a defendant used the victim's stolen identity to obtain health care benefits, Social Security disability benefits, and medical services including a liver transplant).

[11] *See* FED. TRADE COMM'N, THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATTING IDENTITY THEFT: A STRATEGIC PLAN (2007), [hereinafter IDENTITY THEFT TASK FORCE], *available at* https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf ("In addition, identity thieves sometimes use stolen personal information to obtain government, medical, or other benefits to which the criminal is not entitled.").

[12] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-508, IDENTITY THEFT AND TAX FRAUD: IRS NEEDS TO UPDATE ITS RISK ASSESSMENT FOR THE TAXPAYER PROTECTION PROGRAM (2016), *available at* http://www.gao.gov/assets/680/677406.pdf, ("Identity theft (IDT) refund fraud is an evolving and costly problem that causes hardship for legitimate taxpayers who are victims of the crime and demands an increasing amount of the Internal Revenue Service's (IRS) resources.").

[13] *IDENTITY THEFT: Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain: Testimony Before the Subcomm. on Info. Policy, Census and National Archives, H. R. Comm. on Oversight and Gov't Reform*, 111th Cong. (2009) (statement of Daniel Bertoni, Director, Education, Workforce, and Income Security Issues), *available at* http://www.gao.gov/assets/130/122769.pdf ("[I]dentity theft is not a 'stand alone' crime, but rather a component of one or more complex crimes, such as computer fraud, credit card fraud, or mail fraud.").

[14] FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK 2-3 (2015), *available at* https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf.

[15] U.S. DEPT. OF JUSTICE, VICTIMS OF IDENTITY THEFT (2014), *available at* http://www.bjs.gov/content/pub/pdf/vit14.pdf.

[16] FED. TRADE COMM'N, GUIDE FOR ASSISTING IDENTITY THEFT VICTIMS (2013), *available at* https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf ("In some cases the thief does not steal the victim's entire identity, but rather uses only the victim's Social Security number, in combination with another person's name and birth date, to create a new, fictitious identity. As a result, the victim may experience

As the ways in which criminals can exploit PII have evolved, so too have the ensuing types of harm to potentially affected individuals. Identity theft can result in embarrassment,[17] inconvenience, reputational harm,[18] emotional harm,[19] financial loss, unfairness, and, in rare cases, risk to personal safety. Individuals can be arrested and charged for crimes they did not commit,[20] professionals such as pharmacists and doctors can suffer irreparable reputational harm, and individuals can have benefits suspended or terminated.

The unprecedented volume of PII maintained by the Federal Government today, coupled with the rapidly evolving threat and risk landscape, necessitate that agencies take an aggressive approach to protecting Federal information resources. As a result, the Federal Government has invested significant resources and efforts to ensure that protecting information resources remains a top priority.[21] These efforts have included strengthening government-wide processes for developing, implementing, and institutionalizing best practices;[22] leveraging cutting-edge technologies;[23] and proposing a significant budget to start the overhaul of antiquated IT systems.[24]

At the same time that the Federal Government is investing in protecting Federal information resources, it is critically important that Federal agencies remain vigilant and prepare for and understand how to respond to a breach in today's threat landscape. An agency's

---

problems when the new identity tracks back to the victim's credit or tax records. Because this type of fraud may not be reflected on a consumer's credit report, it may not be discovered by the victim for many years.").

[17] National Institute of Standards and Technology, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, Special Publication 800-122 (Apr. 2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf ("Unauthorized access, use, or disclosure of PII can seriously harm both individuals, by contributing to identity theft, blackmail, or embarrassment.").

[18] *Identity Theft*, U.S. DEPT. OF JUSTICE, *available at* https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud (accessed Sept. 15, 2016) ("In many cases, a victim's losses may include not only out-of-pocket financial losses, but substantial additional financial costs associated with trying to restore his reputation in the community.").

[19] *See* IDENTITY THEFT TASK FORCE, *supra* note 11 ("Beyond tangible forms of harm, statistics cannot adequately convey the emotional toll that identity theft often exacts on its victims, who frequently report feelings of violation, anger, anxiety, betrayal of trust, and even self-blame or hopelessness.").

[20] *Id.* ("In addition to losing time and money, some identity theft victims suffer the indignity of being mistaken for the criminal who stole their identities, and have been wrongfully arrested. In one case, a victim's driver's license was stolen, and the information from the license was used to open a fraudulent bank account and to write more than $10,000 in bad checks. The victim herself was arrested when local authorities thought she was the criminal. In addition to the resulting feelings of trauma, this type of harm is a particularly difficult one for an identity theft victim to resolve.").

[21] *See* OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* (Oct. 30, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

[22] *See id.*

[23] *Laying the Foundation for a More Secure, Modern Government*, WHITE HOUSE, *available at* https://www.whitehouse.gov/blog/2016/10/26/laying-foundation-more-secure-modern-government (accessed Oct. 27, 2016).

[24] *See id.* (stating that the proposed IT Modernization Fund is intended to kick-start an overhaul of antiquated Federal Government IT systems and transition to new, more secure, efficient, and modern systems).

effective detection and expeditious response to a breach is important to reduce the risk of harm to potentially affected individuals and to keep the public's trust in the ability of the Federal Government to safeguard PII.

III. Scope

A. Agency Federal Information and Information Systems

This Memorandum applies to Federal information and information systems[25] of an agency, as defined in FISMA.[26] This Memorandum does not apply to national security systems.[27] However, agencies operating national security systems are encouraged to apply this Memorandum to those systems.

B. Personally Identifiable Information

The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available — in any medium or from any source — that would make it possible to identify an individual.[28]

---

[25] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[26] When an agency acts as a service provider, the ultimate responsibility for compliance with applicable requirements is not shifted (to the service provider). Agencies shall describe the responsibilities of service providers in relevant agreements with the service providers. OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf; FISMA, 44 U.S.C. § 3554, provides the following:

"Federal agency responsibilities

(a) IN GENERAL.—The head of each agency shall—

(1) be responsible for—

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency; [. . .]."

[27] *See* 44 U.S.C. § 3552.

[28] *See* OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

C. Definition of a Breach

The guidance set forth in this Memorandum applies to a breach, which is a type of incident.[29]

Definition of an Incident:

An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Definition of a Breach:

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII for an other than authorized purpose. Often, an occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves PII, as is often the case with a lost or stolen laptop or electronic storage device.

Some common examples of a breach include:

- A laptop or portable storage device storing PII is lost or stolen;
- An email containing PII is inadvertently sent to the wrong person;
- A box of documents with PII is lost or stolen during shipping;

[29] *See* 44 U.S.C. § 3552(b)(2).

- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or Federal benefits;

- A user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual;

- An IT system that maintains PII is accessed by a malicious actor; or

- PII that should not be widely disseminated is posted inadvertently on a public website.

IV. Training and Awareness Campaigns

Each agency shall develop training for all individuals with access to the agency's Federal information and information systems on how to identify and respond to a breach, including the internal process at the agency for reporting a breach.[30] Such training is required prior to any individual accessing Federal information or information systems and should also be included in the agency's annual privacy and security awareness training. This includes individuals with temporary access to Federal information or information systems, such as detailees, contractors, grantees, volunteers, and interns. The training should emphasize the individual's obligation to report to the agency not only a confirmed breach, but also a suspected breach, involving information in any medium or form, including paper, oral, and electronic.

Agencies should not limit training on how to identify, report, and respond to a suspected or confirmed breach to annual security and privacy training. Rather, agencies should consider annual security and privacy training as the baseline and consider specialized training for specific groups, such as supervisors and employees who have access to or responsibility for High Value Assets.[31] Additionally, agencies should consider promoting awareness throughout the year, such as by sending periodic reminders through email and conducting awareness campaigns.

V. Preparing for a Breach

A. Privacy Act Routine Uses Required to Respond to a Breach

The SAOP has agency-wide responsibility and accountability for the agency's privacy program and is responsible for overseeing, coordinating, and facilitating the agency's privacy compliance efforts, including those related to the Privacy Act of 1974.[32] The SAOP shall ensure that all agency Privacy Act system of records notices (SORNs) include routine uses for the disclosure of information necessary to respond to a breach either of the agency's PII or, as

---

[30] *See* 44 U.S.C. § 3554(b).
[31] *See* OMB Memorandum M-17-09, *Management of Federal High Value Assets* (Dec. 9, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2017/m-17-09.pdf.
[32] *See* OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Sept. 15, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m_16_24_0.pdf.

appropriate, to assist another agency in its response to a breach.[33] The SAOP should include the following routine use in each of the agency's SORNs to facilitate the agency's response to a breach of its own records:

> *To appropriate agencies, entities, and persons when (1) [the agency] suspects or has confirmed that there has been a breach of the system of records; (2) [the agency] has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, [the agency] (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with [the agency's] efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.*

Additionally, agencies may have records in their systems of records that could assist another agency in its efforts to respond to a breach. For example, this may include information that would assist the other agency in locating or contacting individuals potentially affected by a breach, or information that is related to the other agency's programs or information. To ensure that agencies are able to disclose records in their systems of records that may reasonably be needed by another agency in responding to a breach, the SAOP shall incorporate the following routine use into each of the agency's SORNs:

> *To another Federal agency or Federal entity, when [the agency] determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.*

B. Contracts and Contractor Requirements for Breach Response

Agencies shall ensure that contract terms necessary for the agency to respond to a breach are included in contracts when a contractor collects or maintains Federal information on behalf of the agency or uses or operates an information system on behalf of the agency.[34] To the extent that a cooperative agreement[35] or other such instrument requires another organization or entity to perform such functions on behalf of the agency, the agency must similarly ensure that such cooperative agreements and instruments include the following terms.

---

[33] 5 U.S.C. § 552a(b)(3). The publication of appropriate routine uses is required under the Privacy Act and thus would be necessary in order to disclose information for the purpose of executing an agency's obligations to effectively manage and report a breach under FISMA. Disclosures pursuant to a routine use are permissive, not mandatory. *See* Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948 (July 9, 1975), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf.
[34] *See* 44 U.S.C. § 3553(a)(1)(A).
[35] *See* 31 U.S.C. § 6305.

Thus, at a minimum, contracts should include terms that:

- Require the contractor to cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.

- Require contractors and subcontractors (at any tier) to properly encrypt PII in accordance with OMB Circular A-130[36] and other applicable policies and to comply with any agency-specific policies for protecting PII;

- Require regular training for contractors and subcontractors (at any tier) on how to identify and report a breach;

- Require contractors and subcontractors (at any tier) to report a suspected or confirmed breach in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy and US-CERT notification guidelines;

- Require contractors and subcontractors (at any tier) to maintain capabilities to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector;

- Allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with this Memorandum, the agency's breach response plan, and to assist with responding to a breach;

- Identify roles and responsibilities, in accordance with this Memorandum and the agency's breach response plan; and,

- Explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor (at any tier) failed to provide adequate safeguards for PII.

The Chief Acquisition Officer (CAO), in coordination with the SAOP, should ensure that contract provisions to assist with the response to a breach are uniform and consistently included in agency contracts. Lack of uniformity in agency contracts is likely to complicate an agency's response to a breach and may create unnecessary implementation challenges that could have been avoided. In addition, the SAOP and CIO shall ensure that the agency's breach response plan and system security authorization documentation clearly define the roles and responsibilities of contractors that operate Federal information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII on behalf of the agency. Any such roles and

[36] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

responsibilities should be further defined in the contract so as to ensure contractor compliance with agency requirements.

An agency may also require the contractor to notify any individuals potentially affected by a breach, as explained in this Memorandum. In those instances, the agency may require the contractor to take countermeasures to mitigate the risk of harm to potentially affected individuals or to protect PII on behalf of the agency, including operating call centers and providing resources for potentially affected individuals.

The agency shall ensure that any required countermeasures are consistent with OMB Memorandum M-16-14, which, except under limited circumstances, requires the use of General Services Administration's (GSA) identity protection services (IPS) blanket purchase agreements (BPAs).[37] GSA has awarded government-wide Federal Supply Schedule BPAs for identity monitoring, credit monitoring, and other related services. These BPAs, the requirements for which were developed jointly with officials from the Office of Personnel Management, the Department of Defense, and other agencies, give Federal agencies access to a vetted pool of well-qualified contractors capable of providing the comprehensive services needed to mitigate the risk of harm to individuals potentially affected by a breach, as well as other personnel security matters.

The head of the agency is ultimately responsible for deciding whether to provide notification on behalf of the agency, offer guidance, and provide services to individuals potentially affected by a breach. When a contractor provides notification on behalf of an agency, such activities shall be in accordance with OMB guidance and the agency's breach response plan and shall be coordinated with and subject to prior written approval by the head of the agency.

C. Grants and Grantee Requirements for Breach Response

When a grant recipient uses or operates a Federal information system or creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of PII within the scope of a Federal award, the agency shall ensure that the grant recipient has procedures in place to respond to a breach and include terms and conditions requiring the recipient to notify the Federal awarding agency in the event of a breach. The procedures should promote cooperation and the free exchange of information with Federal awarding agency officials, as needed, to properly escalate, refer, and respond to a breach.

D. Identifying Logistical and Technical Support to Respond to a Breach

Logistical and technical support are often essential to effectively and efficiently respond to a breach. For example, logistical support may be required to prepare and deliver notification and to staff call centers, and technical support is often required to confirm which PII in a given IT system or on a particular device was exposed, accessed, or removed. When a breach

---

[37] OMB Memorandum M-16-14, *Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response* (July 1, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-14.pdf.

potentially affects a large number of individuals or implicates multiple IT systems, this can be a resource-intensive and challenging undertaking and can require hundreds of hours to complete.

When identifying logistical support to respond to a breach, the SAOP should identify the logistical capabilities that exist within the agency and which offices are responsible for maintaining those capabilities. The SAOP should understand the ability of the agency to support any resource-intensive activities that may be necessary to provide notification, offer guidance, and provide services to individuals potentially affected by a breach, such as call center services, updating websites, and providing translation services.

When identifying technical support to respond to a breach, the CIO shall identify technical remediation and forensic analysis capabilities that exist within the agency and which offices are responsible for maintaining those capabilities. Depending on the size, missions, and structure of each agency, the CIO may find the necessary expertise and technical support within the agency. As a part of this process, however, the CIO may identify gaps in the agency's technical capabilities and therefore should communicate with the CAO and other agency officials on the need to enter into contracts or to explore other options for ensuring that certain functions are immediately available during a time-sensitive response. Additionally, while the SAOP might not lead the technical team, the SAOP should understand the ability of the agency to gather, analyze, and preserve the evidence necessary to support an investigation and identify and assess the risk of harm to potentially affected individuals.

The CIO, in coordination with the SAOP, should also consider whether other Federal agencies can support the agency in the event of a breach. Agencies may request technical assistance from US-CERT. In addition, GSA may have BPAs and other guidance for agencies to procure technical services to assist with responding to a breach.[38]

VI. Reporting a Suspected or Confirmed Breach

Each agency shall require all individuals with access to the agency's Federal information and information systems to report a suspected or confirmed breach to the agency as soon as possible and without unreasonable delay, consistent with the agency's incident management policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines.[39] This includes a breach in any medium or form, including paper, oral, and electronic.

Individuals with access to the agency's Federal information and information systems shall not wait for confirmation that a breach has in fact occurred before reporting to the agency, as such a delay may undermine the agency's ability to apply preventative and remedial measures to protect the PII or reduce the risk of harm to potentially affected individuals. In addition, any delay may reduce the likelihood that the agency can recover a lost or stolen device or physical document. For example, if an agency employee loses a mobile device that contains PII, the

---

[38] GSA Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN) includes 132-45B: Incident Response services help organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their IT systems, and restore their networks to a more secure state.
[39] *See* 44 U.S.C § 3556(b)(7).

employee shall report the loss of the device even if the employee believes he or she may be able to locate the device in the future. This is critical because the agency may have the ability to wipe information remotely from the device, thereby reducing or eliminating the risk that the PII may be accessed without authorization or used for malicious purposes. In other cases, the immediate involvement of law enforcement may lead to the retrieval of lost or stolen equipment and PII.

Individuals with access to the agency's Federal information and information systems shall also be able to report a suspected or confirmed breach quickly and easily while in the office, teleworking, or from any remote location, including during domestic and international travel. In order to make it easy for individuals to report a suspected or confirmed breach quickly, agencies should consider establishing a memorable email address and/or toll free telephone number dedicated to incident response (*e.g.*, breach@[agency].gov).

Agencies shall establish rules of behavior, including consequences for violating such rules, for employees, contractors, and others who have access to Federal information or information systems.[40] Agencies shall include in the rules of behavior the consequences for failing to comply with the reporting requirements in this Memorandum. In addition, agencies shall ensure that employees and contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access.

The SAOP should also provide guidance to individuals on the limited circumstances under which the requirement to report a suspected or confirmed breach to the agency is not triggered. In such circumstances, the risk of harm to the potentially affected individuals must be negligible and the failure to report the occurrences must not violate law or regulation. The SAOP shall also conduct an assessment of the risk of harm for any such circumstances prior to issuing any guidance or training (see Section VII.E. of this Memorandum). The agency shall document any such circumstances that the agency finds do not require reporting a suspected or confirmed breach in the agency's incident management policy.

VII. Breach Response Plan

In order to effectively and efficiently respond to a breach, the SAOP shall develop and implement a breach response plan. A breach response plan is critically important to ensuring that an agency is prepared to respond to a breach. A breach response plan is a formal document that includes the agency's policies and procedures for reporting, investigating, and managing a breach, and it should be specifically tailored to the agency and address the agency's missions, size, structure, and functions. An agency's breach response plan shall be part of an agency's formal incident response plan.[41]

At a minimum, a breach response plan shall include the following elements:

---

[40] *See* 5 U.S.C. § 552a(e)(9); *see also* 44 U.S.C. § 3554(b)(4).

[41] *See* National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 Rev. 2, (Aug. 2012), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

- ***Breach Response Team***, including the specific agency officials who comprise the breach response team, as well as their respective roles and responsibilities when responding to a breach.

- ***Identifying Applicable Privacy Compliance Documentation***, including the responsibility to identify any applicable Privacy Act SORNs, privacy impact assessments (PIAs), and privacy notices that may apply to the potentially compromised information.

- ***Information Sharing to Respond to a Breach***, including the potential information sharing within the agency, between agencies, or with a non-Federal entity that may arise following a breach to reconcile or eliminate duplicate records, to identify potentially affected individuals, or to obtain contact information to notify potentially affected individuals.

- ***Reporting Requirements***, including the specific agency officials responsible for reporting a breach to US-CERT, law enforcement and oversight entities, and Congress, when appropriate.

- ***Assessing the Risk of Harm to Individuals Potentially Affected by a Breach***, including the factors the agency shall consider when assessing the risk of harm to potentially affected individuals.

- ***Mitigating the Risk of Harm to Individuals Potentially Affected by a Breach***, including whether the agency should provide guidance to potentially affected individuals, purchase identity theft services for potentially affected individuals, and offer methods for acquiring such services.

- ***Notifying Individuals Potentially Affected by a Breach***, including if, when, and how to provide notification to potentially affected individuals and other relevant entities.

With SAOP approval, a sub-agency or component may develop and implement a sub-agency- or component-specific breach response plan. In those instances, the plan shall be approved by the SAOP and be consistent with the requirements of the agency's breach response plan, OMB guidance, and applicable law. The SAOP shall ensure that sub-agency or component breach response plans are reviewed no less than annually, updated if necessary, and that the date of the review is properly documented in the plan. Sub-agency and component plans shall clearly detail the relationship between the sub-agency or component plan and the agency-level breach response plan.

A. Breach Response Team

An agency's breach response team is the group of agency officials designated by the head of the agency that may be convened to respond to a breach. Once convened, the SAOP is responsible for leading the breach response team. The criteria for convening the breach response team shall be documented in the agency's breach response plan. The criteria for when to

convene the breach response team may be different for each agency according to its individual missions, specific authorities, circumstances, and risks.

When the SAOP is made aware of a report of a suspected or confirmed breach (See section VIII of this Memorandum), the SAOP shall first determine whether the agency's response can be conducted at the staff level or whether the agency must convene the breach response team. If the response can be conducted at the staff level, the agency may choose not to convene the breach response team. At a minimum, the breach response team shall always be convened when a breach constitutes a major incident, as defined in OMB guidance (see Section VII.D.3. of this Memorandum).

When designating agency officials to serve on the agency's breach response team, the head of the agency shall consider the skills and expertise that may be required to effectively and efficiently respond to a breach. The breach response team is responsible for advising the head of the agency on effectively and efficiently responding to a breach.

At a minimum, the agency's breach response team shall include:

- The SAOP;
- The CIO or the CIO's designee;
- The Senior Agency Information Security Officer;[42]
- Legal counsel;
- Legislative affairs official; and
- Communications official.

In order to effectively and efficiently respond to a breach, the breach response team may need to consult with the following personnel:

- Budget and procurement personnel who can provide expertise when a breach involves contractors or an acquisition, or who may help procure services such as computer forensics, cybersecurity experts, services, or call center support;

- Human resources personnel who may assist when employee misconduct results in a breach or when an employee is suspected of intentionally causing a breach or violating agency policy;

- Law enforcement personnel who may assist when a breach involves the violation or suspected violation of law or when a breach is the subject of a law enforcement investigation;

- Physical security personnel who may investigate a breach involving unauthorized physical access to a facility or when additional information regarding physical access to a facility is required; and,

[42] *See* 44 U.S.C. § 3554(a)(3).

- Other agency personnel who may be necessary according to specific agency missions, authorities, circumstances, and identified risks.

B. Identifying Applicable Privacy Compliance Documentation

When responding to a breach, the SAOP shall identify all the applicable privacy compliance documentation. The compliance documentation will help identify what information was potentially compromised, the population of individuals potentially affected, as well as the purpose for which the information had originally been collected, the permitted uses and disclosures of the information, and other information that may be useful when developing the agency's response.

When reviewing privacy compliance documentation in response to a breach, the agency's breach response plan shall, at a minimum, require the SAOP to consider the following:

- Which SORNs, PIAs, and privacy notices apply to the potentially compromised information?

- If PII maintained as part of a system of records needs to be disclosed as part of the breach response, is the disclosure permissible under the Privacy Act and how will the agency account for the disclosure?

- If additional PII is necessary to contact or verify the identity of individuals potentially affected by the breach, does that information require new or revised SORNs or PIAs?

- Are the relevant SORNs, PIAs, and privacy notices accurate and up-to-date?

C. Information Sharing to Respond to a Breach

When responding to a breach, agencies often need additional information to reconcile or eliminate duplicate records, identify potentially affected individuals, or obtain contact information in order to provide notification. Accordingly, the agency may need to combine information maintained in different information systems within the agency, share information between agencies, or share information with a non-Federal entity.

When contemplating the potential information sharing that may be required in response to a breach, the agency's breach response plan shall, at a minimum, require the SAOP to consider the following:

- Would the information sharing be consistent with existing or require new data use agreements, information exchange agreements, or memoranda of understanding?

- How will PII be transmitted and protected when in transmission, for how long will it be retained, and may it be shared with third parties?

D. Reporting Requirements

1. Reporting to US-CERT

OMB Memorandum M-16-03 requires each Federal agency to designate a principal security operation center (SOC) to be accountable for all incident response activities for the respective agency.[43] The agency's breach response plan shall identify the agency's principal SOC. The SAOP shall ensure that employees and contractors staffing the agency's principal SOC are properly trained to identify a breach.

The principal SOC shall notify US-CERT of a breach consistent with the agency's incident management policy and US-CERT notification guidelines.[44] In addition, agencies shall assess whether a breach constitutes a major incident, as defined by OMB guidance, and report that designation to US-CERT as soon as the agency has a reasonable basis to conclude that such a breach has occurred.[45] US-CERT may help the agency assess the circumstances that contributed to the breach and take corrective actions on technical remediation within its scope. However, it is ultimately the agency's responsibility to respond to the breach, including full logistical and technical remediation and forensic analysis.

2. Reporting to Law Enforcement, the Inspector General, and General Counsel

An agency's breach response plan shall identify the agency officials responsible for notifying and consulting with law enforcement and Offices of Inspectors General and General Counsel on behalf of the agency.[46] When responding to a breach, the SAOP shall coordinate with the identified agency officials to ensure that law enforcement and Offices of Inspectors General and General Counsel receive timely notification when notification is appropriate. The SAOP shall also consider and advise appropriate officials on whether the specific circumstances and type of PII potentially compromised by a breach require the involvement of other oversight entities.

When a breach warrants a report to law enforcement, the agency shall ensure that the report occurs promptly, even if the breach is unconfirmed or the circumstances are still unclear. Prompt referral to law enforcement can prevent PII from being further compromised and in some cases can reduce the risk of harm to potentially affected individuals.

---

[43] OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements* (Oct. 30, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf.

[44] *US-CERT Federal Incident Notification Guidelines*, UNITED STATES COMPUTER EMERGENCY READINESS TEAM, available at https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf (accessed Nov. 18, 2016).

[45] *See* OMB Memorandum M-17-05, *Fiscal Year 2016 – 2017 Guidance on Federal Information Security and Privacy Management Requirements* (Nov. 4, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2017/m-17-05.pdf.

[46] 44 U.S.C. § 3554(b)(7)(c).

3. Reporting to Congress

Agencies shall notify the appropriate Congressional Committees pursuant to FISMA[47] no later than seven days after the date on which there is a reasonable basis to conclude that a breach that constitutes a "major incident" has occurred.[48] In addition, agencies shall also supplement their initial seven day notification to Congress with a report no later than 30 days after the agency discovers the breach.[49] This notification shall be consistent with FISMA and OMB guidance on reporting a breach to Congress.[50] The breach response plan shall identify the agency officials responsible for notifying Congress.

Certain information and information systems may be subject to other reporting requirements. The SAOP shall ensure that appropriate subject matter experts who can identify those requirements are part of the breach response team.

E. Assessing the Risk of Harm to Individuals Potentially Affected by a Breach

In order to properly escalate and tailor breach response activities, the SAOP, in coordination with the breach response team when applicable, shall conduct and document an assessment of the risk of harm to individuals potentially affected by a breach. Agencies shall include in their respective breach response plans the requirement to conduct and document an assessment of the risk of harm to potentially affected individuals, including the factors the agency shall consider when assessing the risk.

1. Risk of Harm to Individuals

When assessing the risk of harm to individuals potentially affected by a breach, the SAOP shall consider the potential harms that could result from the loss or compromise of PII. 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, financial harm, the disclosure of contact 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.

---

[47] The committees are the Committee on Oversight and Government Reform, Committee on Homeland Security, and the Committee on Science, Space, and Technology, of the House of Representatives; the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate; the appropriate authorization and appropriations committees of Congress; the Committee on the Judiciary of the Senate; and the Committee on the Judiciary of the House of Representatives. *See* 44 U.S.C. § 3553, note ("Breaches"); 44 U.S.C. § 3554 (b)(7)(C)(III)(aa)-(bb).

[48] 44 U.S.C. § 3554 (b)(7)(C)(III)(aa)-(bb).

[49] 44 U.S.C. § 3553, note ("Breaches").

[50] Detailed guidance on meeting FISMA's Congressional reporting requirements for a breach is provided in OMB Memorandum M-17-05, *Fiscal Year 2016 – 2017 Guidance on Federal Information Security and Privacy Management Requirements* (Nov. 4, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2017/m-17-05.pdf. OMB updates this guidance annually and the most current guidance can be located at https://www.whitehouse.gov/omb/memoranda_default.

Additionally, 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."[51]

Agencies must consider any and all risks relevant to the breach, which may include risks to the agency, agency information systems, agency programs and operations, the Federal Government, or national security. Those additional risks may properly influence an agency's overall response to a breach and the steps the agency should take to notify individuals.

2. Factors for Assessing the Risk of Harm to Potentially Affected Individuals

At a minimum, the SAOP shall consider the following factors when assessing the risk of harm to individuals potentially affected by a breach:

- ***Nature and sensitivity of the PII potentially compromised by the Breach***, including the potential harms that an individual could experience from the compromise of that type of PII;
- ***Likelihood of Access and Use of PII***, including whether the PII was properly encrypted or rendered partially or completely inaccessible by other means; and
- ***Type of Breach***, including the circumstances of the breach, as well as the actors involved and their intent.

a. Nature and Sensitivity of PII

At a minimum, the SAOP shall consider the following when assessing the nature and sensitivity of PII potentially compromised by a breach:

- ***Data Elements***, including an analysis of the sensitivity of each individual data element as well as the sensitivity of all the data elements together;
- ***Context***, including the purpose for which the PII was collected, maintained, and used;
- ***Private Information***, including the extent to which the PII, in a given context, may reveal particularly private information about an individual;
- ***Vulnerable Populations***, including the extent to which the PII identifies or disproportionately impacts a particularly vulnerable population; and
- ***Permanence***, including the continued relevance and utility of the PII over time and whether it is easily replaced or substituted.

[51] *See* 5 U.S.C. § 522a(e)(10).

i. Data Elements

When assessing the nature and sensitivity of PII potentially compromised by a breach, the SAOP shall evaluate the sensitivity of each individual data element. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual. These data elements include, but are not limited to, SSNs, passport numbers, driver's license numbers, state identification numbers, bank account numbers, passwords, and biometric identifiers.

In addition to evaluating the sensitivity of each data element, the SAOP shall also evaluate the sensitivity of all the data elements together. Sometimes multiple pieces of information, none of which are particularly sensitive in isolation and would not present a risk of harm to the individual, may present an increased risk of harm to the individual when combined. For example, date of birth, place of birth, address, and gender may not be particularly sensitive alone, but when combined would pose a greater risk of harm to the individual.

When assessing the nature and sensitivity of potentially compromised PII, the SAOP should not limit the scope of the evaluation to the sensitivity of the information involved in the breach. The SAOP should also consider information that may have been potentially compromised in a previous breach, as well as any other available information that when combined with the information may result in an increased risk of harm to the individuals.

ii. Context

When assessing the nature and sensitivity of PII potentially compromised by a breach, the SAOP shall consider the context. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individuals. For example, a list of personnel and their associated office phone numbers may not be particularly sensitive. However, the same list of personnel and their associated office phone numbers on a list of personnel who hold sensitive positions within a law enforcement agency is sensitive information. Similarly, the same list of names and associated phone numbers on a list of individuals along with information about a medical condition is also sensitive.

iii. Private Information

When assessing the nature and sensitivity of PII potentially compromised by a breach, the SAOP shall evaluate the extent to which the PII constitutes information that an individual would generally keep private. Such "private information" may not present a risk of identity theft or other criminal conduct, but may pose a risk of harm such as embarrassment, blackmail, or emotional distress. Examples of private information include: derogatory personnel or criminal information, personal debt and finances, medical conditions, treatment for mental health, pregnancy related information including pregnancy termination, sexual history or sexual orientation, adoption or surrogacy information, and immigration status. Passwords are another example of private information that if involved in a breach may present a risk of harm.

iv. Vulnerable Populations

When assessing the nature and sensitivity of PII potentially compromised by a breach, the SAOP shall consider whether the potentially affected individuals are from a particularly vulnerable population that may be at greater risk of harm than the general population. Potentially vulnerable populations include, but are not limited to: children; active duty military; government officials in sensitive positions; senior citizens; individuals with disabilities; confidential informants; witnesses; certain populations of immigrants; non-English speakers; and victims of certain crimes such as identity theft, child abuse, trafficking, domestic violence, or stalking. This is not a comprehensive list and other populations may also be considered vulnerable.

v. Permanence

When assessing the nature and sensitivity of PII potentially compromised by a breach, the SAOP shall consider the permanence of the PII. This includes an assessment of the relevancy and utility of the information over time and whether the information will permanently identify an individual. Some information loses its relevancy or utility as it ages, while other information is likely to apply to an individual throughout his or her life. For example, an individual's health insurance ID number can be replaced. However, information about an individual's health, such as family health history or chronic illness, may remain relevant for an individual's entire life, as well as the lives of his or her family members.

Special consideration is warranted when a breach involves biometric information including fingerprints, hand geometry, retina or iris scans, and DNA or other genetic information. When considering the nature and sensitivity of biometric information, an agency should factor in the known current uses of the information and consider that, with future advancements in science and technology, biometric information could have many additional uses not yet contemplated.

b. Likelihood of Access and Use of PII

The agency shall consider the following when assessing the likelihood of access and use of PII potentially compromised by a breach:

- ***Security Safeguards***, including whether the PII was properly encrypted or rendered partially or completely inaccessible by other means;
- ***Format and Media***, including whether the format of the PII may make it difficult and resource-intensive to use;
- ***Duration of Exposure***, including how long the PII was exposed; and

- ***Evidence of Misuse***, including any evidence confirming that the PII is being misused or that it was never accessed.

i. Security Safeguards

When assessing the likelihood of access and use of PII potentially compromised by a breach, the CIO shall evaluate the implementation and effectiveness of security safeguards protecting the information. Security safeguards may significantly reduce the risk of harm to potentially affected individuals, even when the PII is particularly sensitive. The CIO shall consider each of the employed security safeguards on a case-by-case basis and take into account whether the type, value, or sensitivity of the information might motivate a malicious actor to put time and resources towards overcoming those safeguards.

Encryption:

When evaluating the likelihood of access and use of encrypted PII potentially compromised by a breach, the CIO, in coordination with the SAOP and CISO, shall confirm:

- *whether encryption was in effect;*
- *the degree of encryption;*
- *at which level the encryption was applied; and,*
- *whether decryption keys were controlled, managed, and used.*

There are many ways to encrypt information and different technologies provide varying degrees of protection. Encryption can be applied at the:

- *device-level;*
- *file-level; and,*
- *to information at rest or in transmission.*

The protection provided by encryption may be undermined if keys, credentials, or authenticators used to access encrypted information are compromised.

Federal agencies are required to use a NIST-validated encryption method.[52] *The SAOP shall consult with the agency's CISO and other technical experts, as appropriate, to ascertain whether information was properly encrypted. For additional information, refer to National Institute of Standards and Technology Federal Information Processing Standards Publication 140, Security Requirements for Cryptographic Modules at: http://csrc.nist.gov/publications.*

[52] OMB Circular A-130 requires agencies to encrypt all FIPS 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information is technically infeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations; and the risk of not encrypting is accepted by the authorizing official and approved by the agency CIO, in consultation with the SAOP (as appropriate).

The PII potentially compromised by a breach also may be rendered partially or completely inaccessible by security safeguards other than encryption. This may include redaction, data masking, and remote wiping[53] of a connected device. Physical security safeguards such as a locked case securing documents or devices may also reduce the likelihood of access and use of PII. For example, PII in a briefcase left temporarily unattended is less likely to have been accessed and used if the briefcase was securely locked.

ii. Format and Media

When assessing the likelihood of access and use of PII potentially compromised by a breach, the SAOP, in coordination with the CIO, shall evaluate whether the format or media of the PII may make its use difficult and resource-intensive. The format of the PII or the media on which it is maintained may make the PII more susceptible to a crime of opportunity. For example, a spreadsheet on a portable USB flash drive does not require any special skill or knowledge to access and an unauthorized user could quickly search for specific data fields such as a nine-digit SSN. Conversely, a magnetic tape cartridge used for backing up servers that is one of a set of 30 and contains a large volume of unstructured PII would require special expertise and equipment to access and use the information.

The SAOP shall also consider the type, value, or sensitivity of the PII. If the PII is particularly valuable, it may increase the likelihood of access and use regardless of its format or media. This is because the value of the information may outweigh the difficulty and resources needed to access the information.

iii. Duration of Exposure

When assessing the likelihood of access and use of PII potentially compromised by a breach, the SAOP shall consider the amount of time that the PII was exposed. PII that was exposed for an extended period of time is more likely to have been accessed or used by unauthorized users. For example, a briefcase containing PII left in a hotel lobby for an hour before being recovered is less likely to have been accessed by an unauthorized user than if it had been left for three days prior to being recovered. Similarly, PII inadvertently published to a public Internet page for an hour before being removed is less likely to have been accessed by an unauthorized user than if it had been available on the public Internet page for a week.

iv. Evidence of Misuse

When assessing the likelihood of access and use of PII potentially compromised by a breach, the SAOP shall determine whether there is evidence of misuse. In some situations, an agency may be able to determine with a high degree of certainty that PII has been or is being misused. Evidence may indicate that identity theft has already occurred as a result of a specific breach or that the PII is appearing in unauthorized external contexts. For example, law

---

[53] *See* National Institute of Standards and Technology, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, Special Publication 800-124 Rev. 1 (June 2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

enforcement may confirm that PII is appearing on a website dedicated to the sale of stolen PII and may determine that there is strong evidence of misuse. Conversely, agencies may determine with reasonable certainty that the PII will not be misused. For example, a forensic analysis of a recovered device may reveal that the PII was not accessed.

c. Type of Breach

The SAOP shall consider the following when determining the type of breach:

- ***Intent***, including whether the PII was compromised intentionally, unintentionally, or whether the intent is unknown; and,

- ***Recipient***, including whether the PII was disclosed to a known or unknown recipient, and the trustworthiness of a known recipient.

i. Intent

When assessing the risk of harm to individuals potentially affected by a breach, the SAOP shall consider whether the breach was intentional, unintentional, or whether the intent is unknown. If a breach was intentional, the SAOP should determine whether the information was the target, or whether the target was the device itself, like a mobile phone or laptop, and whether the compromise of the information was incidental. Examples of an intentional breach include the theft of a device storing PII from a car or office, the unauthorized intrusion into a Government network that maintains PII, or an employee looking up a celebrity's file in an agency database out of curiosity. While the risk of harm to individuals may often be lower when the information was not the target, the potential for a significant risk of harm to individuals may still exist.

The risk of harm to individuals may be lower when a breach is unintentional, either by user error or sometimes by failure to comply with agency policy. However, that is not always the case, and breach response officials must conduct a case-by-case assessment to determine the risk of harm. Examples of an unintentional breach include an employee accidentally emailing another individual's PII to the wrong email address or a contractor storing personnel files in a shared folder that the contractor thought was access-controlled but that actually was not.

In many circumstances, the SAOP may be unable to determine whether a breach was intentional or unintentional. In these instances, the SAOP shall consider the possibility that the breach was intentional. For example, if an employee realizes her mobile device is missing, it may be that it was stolen intentionally or that she dropped it accidentally. Similarly, a shipment of files containing PII that never arrives at its destination may have been unintentionally lost or may have been targeted by a malicious actor and intercepted.

In circumstances where an agency has notified law enforcement of a breach (see Section VII.D. of this Memorandum), the SAOP shall consider any relevant information provided to the agency by law enforcement that may help inform whether the breach was intentional or unintentional.

ii. Recipient

In some cases, the agency may know who received the compromised PII. This information, when available, may help the SAOP assess the likely risk of harm to individuals. For example, a breach is often reported by a recipient who receives information he or she should not have. This may be an indication of a low risk of harm to individuals, particularly when the recipient is another employee within the agency's IT network. One common type of low-risk breach is when an employee sends an individual's PII via email to another employee at the same agency who does not need to know that PII for his or her duties. In many such cases it may be reasonable to conclude that there is a negligible risk of harm. Even where PII is inadvertently sent to an individual outside an agency, the risk of harm may be minimal if it is confirmed that, for example, the individual is known to the agency, acknowledged receipt of the PII, did not forward or otherwise use the PII and the PII was properly, completely, and permanently deleted by the recipient. This is a breach that must be reported within the agency and appropriately responded to, but the risk of harm is low enough that the response often does not necessitate that the agency notify or provide services to the individual whose PII was compromised.

Conversely, if analysis reveals that the PII is under control of a group or person who is either untrustworthy or known to exploit compromised information, the risk of harm to the individual is considerably higher. In many cases an agency will not have any information indicating that compromised or lost PII was ever received or acquired by anyone. In such circumstances, the SAOP shall rely upon the other factors set forth in this section.

F. Mitigating the Risk of Harm to Individuals Potentially Affected by a Breach

Once the SAOP assesses the risk of harm to individuals potentially affected by a breach, the SAOP, in coordination with the breach response team when applicable, shall consider how best to mitigate the identified risks. The SAOP, in coordination with the breach response team when applicable, is responsible for advising the head of the agency on whether to take countermeasures, offer guidance, or provide services to individuals potentially affected by a breach. Because each breach is fact-specific, the decision of whether or not to offer guidance or provide services to individuals will depend on the circumstances of the breach. When deciding whether or not to offer guidance or provide services to potentially affected individuals, agencies shall consider the assessed risk of harm conducted in accordance with Section VII.E. of this Memorandum. The assessed risk of harm to individuals shall inform the agency's decision of whether or not to offer guidance or provide services. The head of the agency is ultimately responsible for making final decisions regarding whether to offer guidance or provide services to individuals potentially affected by a breach.

The SAOP shall determine and document the actions that the agency will take to mitigate the risk of harm. These actions can include:

- ***Countermeasures***, such as expiring potentially compromised passwords or placing an alert in a database containing potentially compromised PII;

- ***Guidance***, such as how individuals may obtain a free credit report and whether they should consider closing certain accounts; and,

- ***Services***, such as identity and/or credit monitoring.

1. Countermeasures

When determining how to mitigate the risk of harm to individuals potentially affected by a breach, the agency shall consider what countermeasures it can take. Countermeasures may not always prevent harm to potentially affected individuals but may limit or reduce the risk of harm. For example, if credit card information is potentially compromised, the agency may proactively notify appropriate banks so they can monitor the associated accounts or reissue the lines of credit using new accounts. If the information is only useful in a specific context, there may be context-specific countermeasures that can be taken to limit the risk of harm. For example, if information related to disability beneficiaries is potentially compromised, the agency may consider monitoring beneficiary databases for unusual activity that may signal fraudulent activity, such as a sudden request for a change of address. Similarly, if individuals' passwords are potentially compromised in a breach, the agency should require those users to change their passwords.

2. Guidance

When determining how to mitigate the risk of harm to individuals potentially affected by a breach, the SAOP shall consider what guidance to provide to those individuals about how they may mitigate their own risk of harm. There are several steps individuals can take to mitigate their own risk of harm resulting from a breach. These steps include setting up fraud alerts or credit freezes, changing or closing accounts, and taking advantage of services made available by the FTC. The guidance will necessarily depend on the potentially compromised information. Agencies should use the information available at www.IdentityTheft.gov/databreach as the baseline when drafting guidance. The FTC provides specific guidance for when a breach involves SSNs, payment card information, bank accounts, driver's licenses, children's information, and account credentials. Additionally, the agency may advise individuals to change passwords and encourage the use of multi-factor authentication for account access. When choosing guidance to mitigate the risk of harm, the SAOP should consider the guidance options included in Appendix II of this Memorandum.

3. Services

When determining how to mitigate the risk of harm to individuals potentially affected by a breach, the SAOP shall determine if there are services the agency can provide. Many of the services currently available in today's marketplace only mitigate risks of financial identity theft, and even the most comprehensive services are unable to mitigate the potential harms resulting from the evolving threat and risk landscape (see Section II of this Memorandum). When selecting services, the SAOP shall identify those services that best mitigate the specific risk of harm resulting from the particular breach. If the SAOP determines that no service currently available mitigates a specific risk of harm, the agency may choose not to provide services to potentially affected individuals. Choosing not to provide services is a decision separate from the

decision to provide notification and there may be circumstances where potentially affected individuals are notified but not provided services. This Memorandum does not set a specific threshold for providing services to individuals.

When choosing identity monitoring, credit monitoring, and other related services to mitigate the risk of harm to individuals potentially affected by a breach, the SAOP shall take advantage of GSA BPAs in accordance with OMB Memorandum M-16-14.[54] In addition, the SAOP should consider the services included in Appendix III of this memorandum as well as additional services available in the future.

G. Notifying Individuals Potentially Affected by a Breach

The SAOP, in coordination with the breach response team when applicable, is responsible for advising the head of the agency on whether and when to notify individuals potentially affected by a breach. Because each breach is fact-specific, the decision of whether or not to notify individuals will depend on the circumstances of the breach. When deciding whether or not to notify individuals potentially affected by a breach, agencies shall consider the assessed risk of harm conducted in accordance with Section VII.E. of this Memorandum. The assessed risk of harm to individuals shall inform the agency's decision of whether or not to notify individuals. The head of the agency is ultimately responsible for making a final decision regarding whether to provide notification.

The agency's decision to offer guidance, take countermeasures, or provide services to individuals potentially affected by a breach may necessarily require the agency to notify those individuals both of the breach and of those steps taken to mitigate any identified risks. For example, if an agency decides to provide identity and credit monitoring to individuals potentially affected by a particular breach, the agency would need to notify those individuals so that they can use the service. However, agencies may also choose to notify individuals even when the agency is not providing a specific service. For example, an agency may notify individuals that their passwords were potentially compromised by a breach and offer guidance but no services.

Agencies should balance the need for transparency with concerns about over-notifying individuals. Notification may not always be helpful to the potentially affected individuals, and agencies should exercise care to evaluate the benefit of providing notice to individuals or notifying the public (see Section VII.G.4. of this Memorandum).

Certain Federal information systems may be subject to other breach notification requirements, such as those subject to the Health Insurance Portability and Accountability Act.[55] The SAOP shall ensure that appropriate subject matter experts who can identify those requirements are part of the breach response team. In circumstances where multiple notification requirements apply to a breach, agencies should provide a single notice to potentially affected

---

[54] *See id.* For details on the Identity Protection Services BPA, including task order instructions, offered services, authorized users, order dollar value limitations, the inclusion of agency specific terms, and ordering periods, visit www.gsa.gov/ipsbpa.

[55] 45 C.F.R. §§ 164.400-414.

individuals that complies with the guidance in this Memorandum as well as any other notification requirements.

When the head of the agency determines that it is necessary to notify individuals potentially affected by a breach, the SAOP, in coordination with the breach response team when applicable, shall consider the following:

- ***Source of the Notification***, including whom from the agency shall notify individuals potentially affected by a breach;
- ***Timeliness of the Notification***, including the requirement to provide notification as expeditiously as practicable, without unreasonable delay;
- ***Contents of the Notification***, including whether to draft different notifications for different populations potentially affected by a breach;
- ***Method of Notification***, including the best method for providing notification depending on the circumstances of a breach; and,
- ***Special Considerations***, including tailoring the notification for vulnerable populations, whether to provide notification to individuals other than those whose PII was potentially compromised, and how to notify individuals who are visually or hearing impaired.

1. Source of the Notification

When notification is necessary, helpful, or otherwise required, the head of the agency or a senior-level individual he or she may designate in writing, shall be the source of the notification to potentially affected individuals. When a breach involves a well-known component or bureau of an agency, such as the Food and Drug Administration or the Transportation Security Administration, the component or bureau head should issue the notification. Notification from this level demonstrates that the breach has the attention of the head of the agency.

In instances where a small number of individuals potentially are affected by a breach, and when the SAOP determines that there is a low risk of harm to the potentially affected individuals, the SAOP may issue the notification.

When PII created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of by a contractor, or by a subcontractor (at any tier), on behalf of an agency is involved in a breach, the agency may require the contractor to notify any potentially affected individuals (see Section V.B. of this Memorandum).

2. Timeliness of the Notification

Agencies shall notify individuals potentially affected by a breach as expeditiously as practicable and without unreasonable delay.[56] As a practical matter, agencies should avoid providing multiple notifications for a single breach and should balance the timeliness of the notification with the need to gather and confirm information about a breach and assess the risk of harm to potentially affected individuals. If a technical issue contributed to the breach, the head of the agency may also consider whether the issue has been corrected or resolved prior to providing notification.

The Attorney General, the head of an element of the Intelligence Community, or the Secretary of DHS may delay notifying individuals potentially affected by a breach if the notification would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions.[57] Any instruction to delay notification shall be sent to the head of the agency.

3. Contents of the Notification

Agencies shall provide individuals potentially affected by a breach with notification that is concise and uses plain language. Agencies should avoid using generic or repetitive language and should tailor the notification to the specific breach. In some instances, it may be necessary for the agency to draft different notifications for different populations affected by the same breach.

At a minimum, notifications shall include the following:

- 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 PII compromised by the breach (*e.g.*, full name, SSN, date of birth, home address, account number, and disability code);
- A statement of whether the information was encrypted or protected by other means, when it is determined that disclosing such information would be beneficial to potentially affected individuals and would not compromise the security of the information system;

[56] 44 U.S.C. § 3553, note ("Breaches").
[57] 44 U.S.C. § 3553, note ("National Security; Law Enforcement; Remediation.—The Attorney General, the head of an element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. § 3003(4)), or the Secretary of Homeland Security may delay the notice to affected individuals…if the notice would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions.").

- Guidance to potentially affected individuals on how they can mitigate their own risk of harm, countermeasures the agency is taking, and services the agency is providing to potentially affected individuals, if any;

- Steps the agency is taking, if any, to investigate the breach, to mitigate losses, and to protect against a future breach; and,

- Whom potentially affected individuals should contact at the agency for more information, including a telephone number (preferably toll-free), email address, and postal address.

Agencies may want to provide additional details in a Frequently Asked Questions (FAQ) format on the agency website or via an enclosure. The FAQs on an agency website may be beneficial because they can be easily updated, contain links to more information, provide more tailored information than the formal notification, and can be easily translated into multiple languages. For a breach that potentially affects a large number of individuals, or as otherwise appropriate, agencies should establish toll-free call centers staffed by trained personnel to handle inquiries from the potentially affected individuals. If agencies have knowledge that the potentially affected individuals are not English speaking, or require translation services, notification should also be provided in the appropriate languages to the extent feasible. Agencies may seek additional guidance on how to draft a notification from the FTC, which is a leader in providing clear and understandable notifications to consumers, as well as from communication experts.

4. Method of Notification

The SAOP shall select the method for providing notification. The best method for providing notification will potentially depend on the number of individuals affected, the available contact information for the potentially affected individuals, and the urgency with which the individuals need to receive the notification.

- **First-Class Mail**: First-class mail notification to the last known mailing address of the individual in agency records should be the primary means by which notification is provided. Where the agency has reason to believe the address is no longer current, the agency should take reasonable steps to update the address by consulting with other agencies such as the U.S. Postal Service. The notification should be sent separately from any other mailing so that it is conspicuous to the recipient. If the agency that experienced the breach uses another agency to facilitate mailing, care should be taken to ensure that the agency that 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 and should be marked with the name of the agency as the sender to reduce the likelihood the recipient thinks it is advertising mail. Agencies should anticipate mail returned as undeliverable and should have procedures in place for how to provide a secondary notification.

- **Telephone**: Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification or when a small number of individuals are affected. Telephone notification, however, should be contemporaneous with written notification by first-class mail.

- **Email**: Email notification, especially to or from a non-government email address, is not recommended due to the high risk of malicious email attacks that are often launched when attackers hear about a breach. Emails often do not reach individuals because they are automatically routed to spam or junk mail folders. Individuals who receive notifications via email are often uncertain of the legitimacy of the email and will not open the notification. While email is not recommended as the primary form of notification, in limited circumstances it may appropriate. For example, if the individuals potentially affected by a breach are internal to the agency, it may be appropriate for an agency to use an official email address to notify a small number of employees, contractors, detailees, or interns via their official email addresses. A ".gov" or ".mil" email may be used to notify an individual on his or her ".gov" or ".mil" email that his or her PII was potentially compromised by a breach.

- **Substitute Notification**: Agencies may provide substitute notification if the agency does not have sufficient contact information to provide notification, and also as supplemental notification for any breach to keep potentially affected individuals informed. This type of notice may also be beneficial if the agency needs to provide an immediate or preliminary notification in the wake of a high-profile breach when notification is particularly time-sensitive. A substitute notification should consist of a conspicuous posting of the notification on the home page of the agency's website and/or notification to major print and broadcast media, including major media in areas where the potentially affected individuals reside. Notification to media should include a toll-free phone number and/or an email address that an individual can use to learn whether or not his or her personal information is affected by the breach. In instances where there is an ongoing investigation and the facts and circumstances of a breach are evolving, agencies should consider whether it is appropriate to establish an ongoing communication method for interested individuals to automatically receive updates. Depending on the individuals potentially affected and the specific circumstance of a breach, it may be necessary for agencies to provide notifications in more than one language.

5. Special Considerations

When a breach potentially affects a vulnerable population, the agency may need to provide a different type of notification to that population, or provide a notification when it would not otherwise be necessary.

There may be instances when an agency provides notification to individuals other than those whose PII was potentially compromised. For example, when the individual whose information was potentially compromised is a child, the agency may provide notification to the

child's legal guardian(s). Special care may be required to determine the appropriate recipient in these cases.

Agencies should give special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973, as amended.[58] Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the agency website.

VIII. Tracking and Documenting the Response to a Breach

The agency's principal SOC shall develop and maintain a formal process to track and document each breach reported to the agency. The process shall ensure that the SAOP is made aware in a timely manner of each report of a suspected or confirmed breach. The SAOP is responsible for keeping the principal SOC informed of the status of an ongoing response and for determining when the response to a breach has concluded. When the SAOP determines that the agency's response to a breach has concluded, the SAOP shall report that status to the principal SOC along with the outcome of the response.

As a part of the agency's formal process for internally tracking and documenting a response to a breach, each agency shall create a standard internal reporting template that reflects its missions and functions. Appendix I of this Memorandum provides a model breach reporting template that includes examples of data elements and information types that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. In creating a standard internal reporting template, the agency should include as many of the data elements and information types as are relevant to its missions and functions.

The process for internally tracking each reported breach shall allow the agency to track and monitor the following:

- The total number of breaches reported over a given period of time;
- The status for each reported breach, including whether the agency's response to a breach is ongoing or has concluded;
- The number of individuals potentially affected by each reported breach;
- The types of information potentially compromised by each reported breach (see Appendix I of this Memorandum);
- Whether the agency, after assessing the risk of harm, provided notification to the individuals potentially affected by a breach;

[58] 29 U.S.C. § 794(d). For additional information about accessibility aids, refer to www.section508.gov.

- Whether the agency, after considering how best to mitigate the identified risks, provided services to the individuals potentially affected by a breach; and,

- Whether a breach was reported to US-CERT and/or Congress.

IX. Lessons Learned

At the end of each quarter of the fiscal year, the agency's principal SOC shall provide a report to the SAOP detailing the status of each breach reported to the principal SOC during the fiscal year. The SAOP shall review the report and validate that the report accurately reflects the status of each reported breach.

When an agency reports a breach to Congress, the SAOP shall convene the agency's breach response team to formally review the agency's response to the breach and identify any lessons learned. The agency shall use lessons learned to implement specific, preventative actions. Agencies shall document any changes to its breach response plan, policies, training, or other documentation resulting from lessons learned. If there are specific challenges preventing agencies from instituting remedial measures, agencies shall also document those challenges.

X. Tabletop Exercises and Annual Plan Reviews

A. Tabletop Exercises

The SAOP shall periodically, but not less than annually, convene the agency's breach response team to hold a tabletop exercise. The purpose of the tabletop exercise is to test the breach response plan and to help ensure that members of the team are familiar with the plan and understand their specific roles. Testing breach response plans is an essential part of risk management and breach response preparation. Tabletop exercises should be used to practice a coordinated response to a breach, to further refine and validate the breach response plan, and to identify potential weaknesses in an agency's response capabilities.

B. Annual Breach Response Plan Reviews

At the end of each fiscal year, the SAOP shall review the reports from the principal SOC, described in Section VIII of this Memorandum, detailing the status of each breach reported during the fiscal year and consider whether the agency should undertake any of the following actions:

- Update its breach response plan;
- Develop and implement new policies to protect the agency's PII holdings;
- Revise existing policies to protect the agency's PII holdings;
- Reinforce or improve training and awareness;
- Modify information sharing arrangements; and,
- Develop or revise documentation such as SORNs, PIAs, or privacy policies.

As part of the review, the SAOP shall review the agency's breach response plan to confirm that the plan is current, accurate, and reflects any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology. The SAOP is responsible for documenting the date of the most recent review and submitting the updated version of the plan to OMB when requested as part of annual FISMA reporting.

XI. Annual FISMA Reports

FISMA requires agencies to submit an annual report on the adequacy and effectiveness of information security policies, procedures, and practices, to include a description of major information security incidents and major incidents that involved a breach.[59] In addition to those reporting requirements, agencies are required to include in their annual report descriptions of the agency's implementation of the requirements in this Memorandum.[60] At a minimum, agencies shall:

- Confirm that the agency satisfied all requirements in this Memorandum for training and awareness with respect to breach reporting, or if not, explain why the agency did not satisfy those requirements in the Memorandum and what steps the agency will take to satisfy those requirements in the next reporting period;

- Submit the number of breaches reported within the agency during the reporting period, the number of breaches reported by the principal SOC to US-CERT, the number of breaches reported by the agency to Congress, as well as the number of potentially affected individuals;

- Submit the agency's breach response plan and certify that the plan has been reviewed and updated over the past 12 months, as appropriate;

- Submit the names and titles of the individuals on the agency's breach response team and identify those individuals who were removed from the team or added to the team over the past 12 months; and,

- Confirm that the members of the breach response team participated in at least one tabletop exercise during the reporting period or, if not, explain why and what steps the agency will take to ensure that the breach response team participates in a tabletop exercise during the next reporting period.

XII. Implementation

Within 180 days of the issuance of this Memorandum, the SAOP of each agency shall update the agency's breach response plan and provide it to OMB at privacy-oira@omb.eop.gov.[61]

---

[59] 44 U.S.C. § 3554(c)(1)(A).
[60] 44 U.S.C. § 3554(c).
[61] Following the initial submission, in accordance with FISMA and Section XI of this Memorandum, agencies shall submit their breach response plans as part of their annual report to OMB (see 44 U.S.C. § 3554).

The Federal Acquisition Regulatory (FAR) Council, in coordination with OMB, shall work promptly to create appropriate contract clauses and regulatory coverage to address contractor requirements for breach response in the FAR, consistent with the requirements outlined in this Memorandum. In developing regulatory amendments, the FAR Council shall consult with the Federal Privacy Council and the Federal CIO Council, as appropriate.

DHS, in coordination with OMB and the National Security Council, will update the US-CERT Incident Notification Guidelines and associated reporting forms following publication of this Memorandum to provide agencies detailed and standardized procedures for reporting a breach.

If agencies have specific questions about this Memorandum, they may contact OMB at privacy-oira@omb.eop.gov. This Memorandum does not create any right or benefit, substantive or procedural, enforceable at law or in equity against the United States, or any of its departments, agencies, entities, officers, employees, or agents, or any other person.

Appendix I: Model Breach Reporting Template

As a part of the agency's formal process for tracking and documenting a response to a breach (see Section VIII of this Memorandum), each agency is required to create a standard reporting template that reflects its missions and functions. This appendix provides a model internal breach reporting template that identifies examples of types of information that an agency should consider collecting when a suspected or confirmed breach is reported to the agency. In creating a reporting template, the agency should identify the types of information created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of by the agency. This appendix includes examples of data elements and information types that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. In creating a standard internal reporting template, the agency should include as many of these data elements and information types as are relevant to its missions and functions. When responding to a breach, the SAOP shall perform an assessment of the specific risk that an individual can be identified using the potentially compromised information.

Breach Reported by:					
Name:	<<First>>	<<Last>>	**Supervisor:**	<<First>>	<<Last>>
Email:	<< Official Email >>		**Email:**	<< Official Email >>	
Phone:	<< Official Phone >>		**Phone:**	<< Official Phone >>	
Agency/Sub-agency/Component:			<< Agency/Sub-agency/Component >>		

Summary of the Breach:	
Do not include PII or classified information. Summarize the facts or circumstances of the theft, loss, or compromise of PII as currently known, including: a. A description of the parties involved in the breach; b. The physical or electronic storage location of the information at risk; c. If steps were immediately taken to contain the breach; d. Whether the breach is an isolated occurrence or a systematic problem; e. Who conducted the investigations of the breach, if applicable; and f. Any other pertinent information.	
Date and Time of the Breach:	< XX/XX/XXXX, Approximate Time >>
Location of Breach:	<< Street Address >>

Type of Breach:			
Lost Information or Equipment	**Y/N**	**Unauthorized Disclosure** (e.g., email sent to incorrect address, oral or written disclosure to unauthorized person, disclosing documents publicly with sensitive information not redacted)	**Y/N**
Stolen Information or Equipment	**Y/N**	**Unauthorized Access** (e.g., an unauthorized employee or contractor accesses information or an information system)	**Y/N**
Unauthorized Equipment (e.g., using an unauthorized personal device, server, or email account to store PII)	**Y/N**	**Unauthorized Use** (e.g., employee with agency-authorized access to database or file accesses and uses information for personal purposes rather than for official purposes)	**Y/N**

Storage Medium:			
Laptop or Tablet	Y/N	**Smartphone**	Y/N
Desktop	Y/N	**Paper files**	Y/N
External Storage Device	Y/N	**External Storage Device** (e.g., CD, DVD, USB Drive, etc.)	Y/N
IT System (Intranet/Shared Drive)	Y/N	**Oral Disclosure**	Y/N
Email:	<< Provide email address and note the agency, cloud server, personal, private >>		
Other:	<< Provide a detailed description of the medium >>		

Reported to US-CERT, Law Enforcement, or Congress			
Reported to US-CERT	Y/N	**If yes, complete the following:**	
Reported to Law Enforcement	Y/N		
Reported to Congress	Y/N		
Name:	<< Reporting Official >>		
Title:	<< Reporting Official's Title>>		
Email:	<< Official Email >>		
Phone:	<< Official Phone >>		
Agency/Component	<Agency/Component>	**Agency:**	<< Law Enforcement Agency >>
Date and Time of the Report:	<< XX/XX/XXXX, Approximate Time >>		

Number of Individuals and Safeguards	
Number of individuals potentially affected by the breach?	<< ##### >>
Was the information unstructured? (e.g., open fields on a form or survey)	Y/N
Was the information encrypted (see Section VII.E.2. of this Memorandum)	<< ##### >>
Does a duplicate set of the potentially compromised information exist?	Y/N

Additional Information	
Internal breach (e.g., within the agency's network), external, both, or unknown?	<< >>
What counter measures, if any, were enabled when the breach occurred?	
<< List all that apply; include whether NIST certified (e.g., hard drive encryption on laptop, encryption of electronic files, password on smartphone) >>	
What steps, if any, have already been taken to mitigate potential harm?	
<< e.g., calling or sending separate email(s) to recipient(s) of an unauthorized email to request deletion of original email, contacting web publishing to remove unredacted documents from public website, etc.>>	
Do you have knowledge that any information involved in the breach was intentionally stolen or misused?	Y/N
<< If yes, describe the basis for your knowledge and how the information may have been misused (e.g., evidence of identity theft, hacking, adverse publicity, etc.) >>	

Data Elements and Information Types

Identifying Numbers	
Social Security number	Truncated or Partial Social Security number
Driver's License Number	License Plate Number
DEA Registration Number	File/Case ID Number
Patient ID Number	Health Plan Beneficiary Number
Student ID Number	Federal Student Aid Number
Passport number	Alien Registration Number
DOD ID Number	DOD Benefits Number
Employee Identification Number	Professional License Number
Taxpayer Identification Number	Business Taxpayer Identification Number (sole proprietor)
Credit/Debit Card Number	Business Credit Card Number (sole proprietor)
Vehicle Identification Number	Business Vehicle Identification Number (sole proprietor)
Personal Bank Account Number	Business Bank Account Number (sole proprietor)
Personal Device Identifiers or Serial Numbers	Business device identifiers or serial numbers (sole proprietor)
Personal Mobile Number	Business Mobile Number (sole proprietor)

Biographical Information		
Name (including nicknames)	Gender	Race
Date of Birth (Day, Month, Year)	Ethnicity	Nationality
Country of Birth	City or County of Birth	Marital Status
Citizenship	Immigration Status	Religion/Religious Preference
Home Address	Zip Code	Home Phone or Fax Number
Spouse Information	Sexual Orientation	Children Information
Group/Organization Membership	Military Service Information	Mother's Maiden Name
Business Mailing Address (sole proprietor)	Business Phone or Fax Number (sole proprietor)	Global Positioning System (GPS)/Location Data
Personal e-mail address	Business e-mail address	Employment Information
Personal Financial Information (including loan information)	Business Financial Information (including loan information)	Alias (e.g., username or screenname)
Education Information	Resume or curriculum vitae	Professional/personal references

Biometrics/Distinguishing Features/Characteristics		
Fingerprints	Palm prints	Vascular scans
Retina/Iris Scans	Dental Profile	Scars, marks, tattoos
Hair Color	Eye Color	Height
Video recording	Photos	Voice/Audio Recording
DNA Sample or Profile	Signatures	Weight

Medical/Emergency Information (select all that apply)		
Medical/Health Information	Mental Health Information	Disability Information
Workers' Compensation Information	Patient ID Number	Emergency Contact Information

Device Information		
Device settings or preferences (e.g., security level, sharing options, ringtones)	Cell tower records (e.g., logs, user location, time, etc.)	Network communications data

Specific Information/File Types		
Taxpayer Information/Tax Return Information	Law Enforcement Information	Security Clearance/Background Check Information

Specific Information/File Types (Cont.)		
Civil/Criminal History Information/Police Record	Academic and Professional Background Information	Health Information
Case files	Personnel Files	Credit History Information

Appendix II: Examples of Guidance an Agency May Offer

Active Duty Alert: Service members who deploy can place an active duty alert on their credit reports to help minimize the risk of identity theft. These types of alerts on a credit report mean businesses have to take extra steps before granting credit to an individual. Active duty alerts last for one year, and can be renewed by the service member to match the period of their deployment.

Credit Freeze: A credit freeze restricts access to an individual's credit report. When offering this type of guidance, an agency should be aware that because access to a credit report is usually required by creditors, a credit freeze can prevent creditors from approving a new account.

Credit Freezes for Children: Guardians are sometimes able to place a freeze on a child's credit, even if the child does not yet have a credit history. Several states mandate that all credit bureaus provide this option. Outside those states, the option may still be available depending on the credit bureau. In these instances, guardians may have to provide additional information about themselves as well as the child in order to show the relationship.

Closing or Changing Accounts: Individuals should immediately dispute any unauthorized charges to existing accounts, including closing or changing account numbers so that unauthorized activity does not continue. This will not prevent new unauthorized accounts of which individuals may be unaware.

Obtaining a Free Credit Report: Individuals can obtain a free credit report yearly from each of the three national credit bureaus (Equifax, Experian, and TransUnion) from annualcreditreport.com or by calling the credit reporting agencies' toll-free numbers. Individuals should review their credit reports for any accounts they do not recognize.

Cyber Hygiene: Agencies should also consider providing individuals with resources on good cyber hygiene (e.g., setting up multi-factor authentication, using complex passwords). Resources include: DHS's Stop.Think.Connect. Campaign at: https://www.dhs.gov/stopthinkconnect or https://www.ftc.gov/onguardonline; US-CERT's tips on protecting privacy at: https://www.us-cert.gov/ncas/tips/ST04-013; and US-CERT's tips on preventing online identity theft at: https://www.us-cert.gov/ncas/tips/ST05-019.

Deceased Alerts: Deceased individuals can be at heightened risk for identity fraud that may impact the deceased individual's estate.[62] This creates liability for a surviving spouse if, for example, his or her name is on joint accounts. To prevent this, death certificates can be sent to the IRS as well as the major credit bureaus, with a request to place a "deceased alert" on the account to prevent new activity.

Fraud Alert: A fraud alert tells creditors that they must take reasonable steps to verify the identity of the individual who is applying for credit. A fraud alert also allows individuals to

---

[62] *See, e.g.*, *Examples of Identity Theft Investigations - Fiscal Year 2016*, INTERNAL REVENUE SERV., *available at* https://www.irs.gov/uac/examples-of-identity-theft-investigations-fiscal-year-2016 (accessed Oct. 25, 2016) (citing that two Florida residents were convicted of wire fraud conspiracy and aggravated identity theft for filing 32 fraudulent federal income tax returns, 21 of which were joint returns that included PII of deceased individuals).

order one free copy of the individual's credit report from each of the three national credit bureaus. To place this alert, individuals can contact one of the three national credit bureaus, who must then notify the others. The initial fraud alert stays on the credit report for 90 days and can be renewed.

FTC.gov/idtheft: The FTC's website provides free identity theft resources for individuals as well as community leaders, businesses, advocates, and law enforcement to share in their communities. The website includes resources on proactive steps individuals can take to monitor and protect their information and educate themselves on the different types of identity theft and the resources available to protect against and recover from identity theft.

IdentityTheft.gov: This is the Federal Government's one-stop resource for identity theft victims. Individuals can use the website to report identity theft and get a personalized recovery plan that walks them through each step, updates the plan as needed, and pre-fills letters and forms. It also advises individuals on steps they can take to prevent identity theft when they receive notice that their PII has been compromised. The website is managed by the FTC and is integrated with the FTC's complaint system, which makes the complaint information available to law enforcement across the country through Consumer Sentinel, a secure online database available to law enforcement.

Tax Fraud: Agencies may consider recommending that individuals file an IRS Identity Theft Affidavit (Form 14039) to prevent an identity thief from using compromised PII to falsely claim the individual's tax refund.

Appendix III: Examples of Services an Agency May Provide

Credit Monitoring: Many companies, including credit reporting agencies, offer this service as a subscription for a defined period of time. The service includes monitoring an individual's credit report, and notifying the potentially affected individual, usually via email, when new activity is reported to their credit report. Credit monitoring notifies individuals that compromised information may have been used to open a new credit account using their information. It does not monitor other non-credit-based risks for misuse of compromised information.

Identity Monitoring: These services monitor the use of an individual's overall identity beyond information contained in a credit report. This monitoring generally tracks whether the individual's information has been exposed online, in addition to monitoring other databases, which may include information related to change of address, court records, payday loans, health, criminal, and other identifying information beyond just financial credit information. These more comprehensive services mitigate risks of the non-credit identity thefts outlined above. Each company provides different monitoring services, so agencies should ensure that monitoring options are appropriate given the compromised information. The effectiveness of the monitoring will depend on factors such as the databases monitored, the amount and accuracy of the information in the databases, and how often the company checks the databases.

Full-Service Identity Counseling and Remediation Services: These are additional services that provide trained counselors or case managers to help individuals recover from identity theft. The services may include assisting individuals with preventing pre-screened offers of credit, helping consumers dispute charges and removing fraudulent information, and providing legal assistance. Generally, individuals authorize companies offering these services to act on their behalf.

Identity Theft Insurance: Insurance reimburses individuals for certain losses resulting from identity theft. Generally, this insurance covers only out-of-pocket expenses directly associated with recovery from the identity theft. Typically, these are limited to things like postage, copying and notary costs. Some policies cover lost wages or legal fees. Generally, these policies do not provide reimbursement for any funds that are stolen as a result of the identity theft. Agencies should understand what they are purchasing and communicate clearly within any guidance provided the details of what the insurance covers as well as any limitations and exclusions to the potentially affected individuals.

Appendix IV: Government-wide Incident and Breach Response Resources

Federal Laws

Federal Information Security Modernization Act (FISMA) of 2014
Pub. L. 113-283, 128 Stat. 3073 (Dec. 18, 2014) (primarily codified at 44 U.S.C. chapter 35, subchapter II).

Executive Orders, Memoranda, and Directives

Resources Related To Breach

OMB Memorandum M-17-09, Management of Federal High Value Assets (Dec. 9, 2016).
Tip: This Memorandum requires agencies to routinely test incident response procedures for all HVAs as part of agencies implementation and validation of security controls.

OMB Memorandum M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements (Nov. 4 2016).
Tip: See Section II for the definition of "Major Incident," guidance on when a breach constitutes a Major Incident, reporting a Major Incident to US-CERT and OMB, and associated Congressional reporting requirements.
Note: OMB updates this guidance annually and the most current guidance can be located at https://www.whitehouse.gov/omb/memoranda_default.

PPD-41, Annex for Presidential Policy Directive – United States Cyber Incident Coordination (July 2016)
Tip: See Section III, Federal Government Response to Incidents Affecting Federal Networks for guidance on when a Breach meets the definition of a "significant cyber incident" and shall be managed in accordance with this directive.

OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)
Tip: See Appendix II, Section 5(h) for a summary of incident handling responsibilities for managing PII.

OMB Memorandum M-16-14, Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response (July 1, 2016)
Tip: This Memorandum requires, with limited exceptions, that agencies use the government-wide blanket purchase agreement for Identity Monitoring Data Breach Response and Protection Services awarded by the General Services Administration.

OMB Memorandum M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices (Oct. 3, 2014)
Tip: See Section III: FY 2014 FISMA Reporting and Privacy Management Guidance for the requirement that agencies report to US-CERT cyber-related (electronic) incidents with confirmed loss of confidentiality, integrity, or availability within one hour.

Agencies or Sub-Components with Specific Government-wide Guidance

Department of Commerce/ National Institute of Standards and Technology (NIST)

NIST Special Publication 800-61 (Revision 2), Computer Security Incident Handling Guide (Aug. 2012)

NIST Special Publication 800-34 (Revision 1), Contingency Planning Guide for Federal Information Systems and Organizations (Apr. 2013)
Tip: See control MP-6(8) for information on remote purging/wiping of lost or stolen mobile devices. See several controls throughout the document for information on properly encrypting information on various media and contexts.

NIST Special Publication 800-122, Guide to Protecting the Confidentiality of PII (Apr. 2010)

Department of Homeland Security (DHS)/ United States Computer Emergency Readiness Team (US-CERT)

US-CERT Federal Incident Notification Guidelines

National Cybersecurity and Communications Integration Center (NCCIC) Cyber Incident Scoring System

General Services Administration (GSA)

Identity Protection Services (IPS) Multiple Award Blanket Purchase Agreement (BPA)

Glossary

'**Breach**' the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses personally identifiable information for an other than authorized purpose.

'**Breach Response Plan**' is the agency's formal document that includes the policies and procedures that shall be followed with respect to reporting, investigating, and managing a Breach.

'**Breach Response Team**' is the group of agency officials designated by the head of the agency that the agency may convene to respond to a breach. Once convened, the SAOP is responsible for leading the breach response team's response to a breach.

'**Federal Information**' means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.[63]

'**Federal Information System**' means an information system used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency.[64]

'**Incident**' means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.[65]

'**Personally Identifiable Information**' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.[66]

'**Senior Agency Official for Privacy**' means the senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections, compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.[67]

---

[63] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.
[64] *Id.*
[65] 44 U.S.C. § 3552.
[66] OMB Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016), *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.
[67] *Id.*