HUD PRIVACY INCIDENT REPORT

January 2017

U.S. Department of Housing and Urban Development

Prepared by HUD's Senior Agency Official for Privacy and the HUD Breach Incident Response Team

Table of Contents

1. EXECUTIVE SUMMARY 3

2. BACKGROUND ON INCIDENTS 4

A. Incident A: Empowerment Zone/Renewal Community Locator Tool 4

1. Incident Summary 4

2. Detection, Response, and Remediation Actions Taken 4

3. Threats and Threat Actors, Vulnerabilities, and Impacts 5

B. Incident B: Disclosure of Information to Public Housing Authorities 5

1. Incident Summary 5

2. Detection, Response, and Remediation Actions Taken 5

3. Threats and Threat Actors, Vulnerabilities, and Impacts 6

3. NOTICES AND CREDIT MONITORING SERVICES 6

1. Total Number of Indivduals Impacted by Incidents 6

2. Why is There a Difference in Incident A Numbers? 7

3. How Many Notices Have Gone Out? 7

4. How Many People Have Signed Up for Credit Monitoring? 7

5. Has HUD Received Questions or Complaints? 7

4. LESSONS LEARNED 7

A. Misunderstanding of What Is PII and How to Protect It 7

B. Need to Update HUD's Breach Response Plan 7

C. Strengthen Coordination between CISSO and Privacy Branch 7

5. ACTION PLAN 8

A. Expand Privacy Training 8

B. Recruit Experienced Privacy Professionals 8

C. Conduct Privacy Compliance Review 8

D. Review and Update Breach Response Policy and Procedures 8

ATTACHMENT 1: LAWS, DIRECTIVES, POLICIES, AND GUIDANCE IMPLICATED BY THE PRIVACY INCIDENT 9

A. Federal Regulations and Federal Contract Clauses 9

1. Privacy Act of 1974 9

2. E-Government Act of 2002 9

3. Federal Acquisition Regulation (FAR), Part 42 – Contract Administration and Audit Services, Subpart 42.11, Production and Surveillance Reporting 10

4. FAR, Part 52.224-2 – Privacy Act 10

5. General Services Administration (GSA) Federal Acquisition Regulation (FAR) Clause 1052.201.70 Contracting Officer's Technical Representative (COTR) Appointment and Authority (APR 2004) (Deviation) (DTAR) 10

B. Office of Management and Budget (OMB) Memoranda 11

1. OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments 11
2. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information 11

ATTACHMENT 2: NOTICE LETTER AND SUPPORT MATERIALS 12
A. English Language Notice 12
B. Spanish Language Notice 13
C. Frequently Asked Questions 14

ATTACHMENT 3: TIMELINES 17
A. Timeline for Incident A 17
B. Timeline for Incident B 17

ATTACHMENT 4: LETTER TO EXECUTIVE DIRECTORS 19

HUD Privacy Incident Report

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

1. EXECUTIVE SUMMARY

Since August 29, 2016, the U.S. Department of Housing and Urban Development (HUD) has learned of two privacy incidents that compromised personal information of members of the public.

The first incident, discovered August 29, 2016, involved businesses uploading excess employee data in HUD's Empowerment Zone and Renewal Community (EZ/RC) Locator. This online tool uses employee zip codes to help businesses determine eligibility for tax credits. The excess data included employee Social Security numbers and was stored on an unsecured webserver. Although this excess data was uploaded to the Department's webserver by private businesses, the data was not requested by the Department and was not necessary for determining eligibility for the tax credit. HUD immediately shut down the Locator once the disclosures of sensitive personally identifiable information were confirmed. Approximately 35,533[1] impacted individuals were notified and offered free credit monitoring for one year as a result of this incident.

Another incident, discovered on September 14, 2016, involved some personal information pertaining to public housing residents. While sharing community service requirement information with local public housing authorities, HUD discovered that personal information was made available through its website, **www.hud.gov**. The information included the individual's last name, the public housing building code, and last four of their Social Security Number for 428,828 public housing residents[2]. These residents were notified by HUD and offered free credit monitoring services for one year.

In both instances, HUD removed access to the associated known web pages and links as soon as the disclosures were confirmed. HUD also conducted further review to determine the scope of the incidents, the extent of data exposed, and likelihood of unauthorized use of the information. To date, HUD has found no evidence of malicious intent or that any of the data has been used inappropriately.

This report summarizes these privacy incidents, discusses notifications and provision of credit monitoring services to impacted individuals, identifies lessons learned, and lays out HUD's Action Plan. Additional information regarding these incidents is available in our **FAQs** and Sample Notices (**English** | **Spanish**).

[1] HUD initially identified 50,727 unique individuals that were potentially impacted in this incident. However, after additional analysis of the partial data that was exposed in this incident, only 35, 533 unique individuals were impacted.
[2] HUD provides public housing to approximately 2.5 million individuals nationwide.

2. BACKGROUND ON INCIDENTS

During FY16, HUD had two Major Incidents involving a breach of Personally Identifiable Information (PII), which are described below as Incident A and Incident B. Since these incidents overlapped and were briefed concurrently to stakeholders, HUD is providing a consolidated report.

A. Incident A: Empowerment Zone/Renewal Community Locator Tool

1. Incident Summary

HUD was notified by a member of the public on August 29, 2016, that PII, including Social Security Numbers (SSNs) was accessible on HUD's website via an internet Google search. HUD's Chief Information Security Officer (CISO) reviewed the information and determined that the PII found was contained in Excel files collected through the Empowerment Zone/Renewal Community Locator tool, and stored on a HUD web-server. HUD did not request SSN information, but this information was uploaded by private employers seeking to use the tool to determine whether their employees lived in an Empowerment Zone.

2. Detection, Response, and Remediation Actions Taken

HUD took immediate action to eliminate public access to the PII. The CISO removed the links and began manual review of the more than 37,000 spreadsheets containing various pieces of PII to determine the extent and scope of the incident. The EZ/RC locator tool was subsequently disabled. While the initial review indicated minimal amounts of PII were exposed, review of additional spreadsheets over the following two weeks indicated that approximately 20% of the spreadsheets contained significant PII.

As soon as the analysis revealed that the scope of the incident was broader, HUD's Senior Agency Official for Privacy (SAOP) activated the Breach Notification Response Plan in accordance with HUD policy and federal guidance. This included convening the HUD Breach Incident Response Team (HBIRT). The HBIRT includes the principals or representatives from the Office of the Deputy Secretary, the Office of the General Counsel, the Office of the Chief Information Officer, the Office of the Chief Administrative Officer, the Office of the Chief Human Capitol Officer, Office of the Chief Procurement Officer, the Office of the Chief Financial Officer, and the impacted program offices. The scope of the incident was analyzed through manual review of over 37,000 spreadsheets, which dated back as far as 2014. Approximately 19% of the spreadsheets contained unnecessary PII, which included: names, addresses, SSNs, and last four of SSNs. With further analysis (including de-duplication), HUD found that 35,533[3] unique individuals were impacted by this incident.

The HBIRT determined this incident a high-risk of harm to individuals, and notifications were made to HUD's Office of Inspector General, United States Computer Emergency Readiness Team (US-CERT), OMB, and the appropriate Congressional committees. HUD has provided notice to impacted individuals, along with access to credit monitoring solutions. The HBIRT has also developed a targeted Action Plan, which includes an immediate review of similar systems and updating the system's Privacy

[3] HUD initially identified 50,727 unique individuals that were potentially impacted in this incident. However, after additional analysis of the partial data that was exposed in this incident, only 35, 533 unique individuals were impacted.

Impact Assessment. Longer-term remediation actions include: (1) hiring a dedicated Chief Privacy and Compliance Officer and (2) reviewing all automated systems to identify potential undocumented systems and any previously unidentified collection of PII. HUD is also conducting a compliance review of all required Privacy Impact Assessments and System of Record Notices. The HBIRT served as the cornerstone for this incident, including ensuring coordination across the Department, identifying lessons learned, and developing and implementing the final Action Plan.

3. Threats and Threat Actors, Vulnerabilities, and Impacts

No threat actors were identified. The primary cause of the incident is due to a lack of validation checks in place for the data uploaded, allowing for a wide range of data formats to be uploaded and subsequently downloaded, resulting in a privacy data spillage. The HBIRT declared this incident a high-risk of harm to individuals[4].

B. Incident B: Disclosure of Information to Public Housing Authorities

1. Incident Summary

On September 14, 2016, HUD received notice from a member of the public of an incident involving unsecured Excel files containing PII, including last four digits of residents' social security numbers, available at a public-facing HUD URL. That same day, links to the identified file were disabled, and HUD's Chief Information Security Officer (CISO) began investigating the incident. On September 22, HUD received a separate notice that another related file containing PII was publicly accessible. After identifying that information as PII, the URL was immediately disabled. All PII related to this incident was contained by September 22, 2016.

2. Detection, Response, and Remediation Actions Taken

HUD's SAOP activated the Breach Notification Response Plan in accordance with HUD policy and federal guidance. This included convening the HBIRT. The scope of the incident was analyzed and it was discovered that the Excel files contained information regarding residents in HUD-assisted public housing.

The HIBIRT's review of this incident determined that HUD's Office of Public and Indian Housing (PIH) had begun providing quarterly reports to Public Housing Agencies regarding individual public housing residents' compliance with community service requirements. In order to provide these reports, PIH sent an email to approximately 1,600 Public Housing Authorities (PHAs), which included a link to spreadsheets posted on the web so PHAs could download their data and correct reporting. Emails containing similar links were sent each quarter, beginning in August 2015. The last reports were sent in September of 2016. The combined spreadsheets contained: last name, last four of SSN, and the PHA's unique building identifiers of 428,828 individuals.

The HBIRT declared this incident a medium-risk of harm to individuals, and notifications were made to HUD's Office of Inspector General, US-CERT, OMB, and the appropriate Congressional

[4] The HBIRT voted that the incident be declared a Major Incident that is likely to pose a High Risk of Harm to individuals based on the five factor test outlined in OMB M-07-16.

committees. HUD has provided notice to impacted individuals, along with access to credit monitoring solutions. PHA Executive Directors were also notified of the incident. The HBIRT developed an Action Plan, which includes an immediate review of similar systems and tools. Additional longer-term remediation actions include: (1) hiring a Chief Privacy and Compliance Officer and (2) reviewing all automated systems to identify potential undocumented systems and any previously unidentified collection of PII. HUD is also conducting a compliance review of all required Privacy Impact Assessments and System of Record Notices. The HBIRT served as the cornerstone for this incident, including ensuring coordination across the Department, identifying lessons learned, and developing and implementing the final Action Plan for this incident.

3. Threats and Threat Actors, Vulnerabilities, and Impacts

No threat actors were identified. The primary cause of the incident is a lack of understanding of the definition of PII and a lack of understanding of HUD's Data Encyption Policy. The HBIRT declared this incident a medium-risk of harm to individuals.

3. NOTICES AND CREDIT MONITORING SERVICES

HUD provided notices to all impacted individuals who could be identified. PHA Executive Directors were also notified of the incident and communications to their residents. In addition, key information was posted to the HUD website, including an overview of the incident, sample notice letters in English and Spanish, a Fact Sheet on Frequently Asked Questions, and links on HUD's webpage to additional information on HUD's Privacy Program.

1. Total Number of Individuals Impacted by Incidents

IMPACTED INDIVIDUALS BY INCIDENT

Initial Review identified:

INCIDENT A: 50,727 unique individuals

INCIDENT B: 428,828 unique individuals

Final analysis identified:

INCIDENT A: 35, 533 unique individuals

INCIDENT B: 390,126 unique individuals with good current postal addresses

38,702 individuals who moved/required look-up services to identify individual/ address

(Subtotal for Incident B: 428,828)

2. Why is There a Difference in Incident A Numbers?

As reported previously, the spreadsheets containing the data in incident A were in various formats, and contained amounts of data organized in different ways. HUD had no means to verify the completeness of any particular record. When TransUnion did their analysis and used their locator tools, they discovered that there was insufficient or incorrect information for 15,194 records. The data in those records could not be linked to an individual—so no notice was required.

3. How Many Notices Have Gone Out?

As of January 5, 2017, 425,659 total notices have been mailed.

INCIDENT A: 35, 533 (began 11/10/2016 and finished 11/23/2016)

INCIDENT B: 390,126 (began 11/14/2016 through 11/30/2016)

38,702 (began and finished on 12/1/2016)

4. How Many People Have Signed Up for Credit Monitoring?

As of January 9, 2017: 11,262 individuals have signed up for credit monitoring services.

5. Has HUD Received Questions or Complaints?

The Department has received inquiries on HUD hotlines regarding the authenticity of the letter and questions about the incidents. Approximately two dozen people have requested more information or have had difficulty registering with Trans Union. Our privacy branch and SAOP have been personally responding to and assisting those individuals who require additional assistance.

4. LESSONS LEARNED

HUD's SAOP, in collaboration with the HBIRT, conducted a review of the privacy incidents and actions based on relevant laws, Federal directive, polices and guidance. Key Lessons Learned are summarized below.

A. Misunderstanding of What Is PII and How to Protect It

We discovered that individuals at various levels of the affected program offices had misunderstandings about the definition of PII and the applicability of HUD's Encryption Policy.

B. Need to Update HUD's Breach Response Plan

The plan was executed successfully and was effective, but contains internal references that no longer represent HUD's current organizational structure and the relative roles and responsibilities of the SAOP, CIO, CISO, and Privacy Branch.

C. Strengthen Coordination between HUD's CISO and Privacy Branch

While HUD's Breach Response Plan outlines coordination roles, the plan was developed when the privacy branch was part of the Chief Information Officer's organizational structure. With the move of

the privacy function to the Office of Administration, the plan should be updated to strengthen coordination across offices to better address privacy incidents.

5. ACTION PLAN

HUD's Senior Agency Official for Privacy, in collaboration with (HBIRT), developed the following Action Plan to address gaps in HUD's privacy program.

A. Expand Privacy Training

In addition to required annual privacy awareness training, HUD is conducting specialized training focused on PII and HUD operations. The training plan focuses on providing this training from the top of the organization across every level, beginning with training conducted by the SAOP to the following key groups:

- The Secretary, Deputy Secretary, Chief of Staff, and all HUD Senior staff in October 2016.
- Leadership of all HUD program offices involved in privacy incidents within 60 days of the event.
- All HUD General Deputy Assistant Secretaries in November 2016.
- All mangers in the Office of General Counsel in December 2016.

The SAOP and Privacy Branch will continue to provide specialized training to all program offices and field staff.

B. Recruit Experienced Privacy Professionals

HUD's privacy program has been depleted over the years due to retirement, attrition, and lack of new hires. For example, HUD has been without a Chief Privacy Officer and Privacy Branch Chief for more than two years. These position are critical to maintaining privacy compliance. The SAOP is prioritizing and backfilling those positions with experienced, credentialed privacy professionals.

C. Conduct Privacy Compliance Review

HUD will undertake a compliance review, including:

- Update Data Inventory and Crosswalk System of Records Notices (SORNs) and Privacy Impact Assessments (PIAs).
- Interview all Information System Security Officers (ISSOs) to Identify PII Systems.
- Identify and Address Compliance for Any Undocumented Systems.

D. Review and Update Breach Response Policy and Procedures

Based on the Lessons Learned, HUD will review and update the breach policy and procedures.

ATTACHMENT 1: LAWS, DIRECTIVES, POLICIES, AND GUIDANCE IMPLICATED BY THE PRIVACY INCIDENT

This section identifies relevant laws, federal directives, policies and guidance (whether federal, OMB, or HUD) that resulted in, and/or were related to, the FY16 data breaches and subsequent Privacy Incidents.

A. Federal Regulations and Federal Contract Clauses

1. Privacy Act of 1974[5]

The Privacy Act of 1974 provides, in part, that, —[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to who the record pertains subject to certain exceptions.

The Privacy Act further provides that, —[e]ach agency that maintains a system of records shall…maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President.[6]

2. E-Government Act of 2002[7]

The E-Government Act of 2002 enhances the management and promotion of electronic Government services and processes by establishing a federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to government information and services.

Title III of the E-government Act, also known as the Federal Information Security Management Act (FISMA), further tasked the National Institute of Standards and Technology (NIST) with the responsibility of developing security standards and guidelines for the federal government. Based upon this requirement, NIST developed the following:

- **FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.** Requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.[8]
- **FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.** Specifies minimum security requirements for information and information systems

[5] 5 U.S.C. § 552a.
[6] 5 U.S.C. § 552a(e)(1).
[7] Pub. L. No. 107-347, 116 Stat. 2899
[8] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.[9]

- **Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations***. Provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200. The guidelines apply to all Components of an information system that process, store, or transmit federal information.[10]

3. Federal Acquisition Regulation (FAR),[11] Part 42 – Contract Administration and Audit Services, Subpart 42.11, Production and Surveillance Reporting

The Federal Acquisition Regulation (FAR) details the duties required for maintaining oversight and surveillance of contractors' performance. All surveillance assignments of contract oversight personnel must be made in writing.

The FAR states, —[p]roduction surveillance is a function of contract administration used to determine contractor progress and to identify any factors that may delay performance. Production surveillance involves Government review and analysis of—

(a) Contractor performance plans, schedules, controls, and industrial processes; and (b) The contractor's actual performance under them.

4. FAR, Part 52.224-2 – Privacy Act[12]

As prescribed in 24.104, insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:

(a) The Contractor agrees to—

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function.

5. General Services Administration (GSA) Federal Acquisition Regulation (FAR) Clause 1052.201.70 Contracting Officer's Technical Representative (COTR) Appointment and Authority (APR 2004) (Deviation) (DTAR)[13]

The General Services Administration (GSA) FAR Clause states, —[t]he Contracting Officer (CO) designates the COTR and any alternate COTR(s) in writing. This designation can only be accomplished in writing and cannot be delegated without written approval and a list of COTR duties being issued by the CO.

[9] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.
[10] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
[11] https://www.acquisition.gov/far/current/html/FARTOCP42.html
[12] https://www.acquisition.gov/far/current/html/52_223_226.html#wp1168981.pdf.
[13] FAR Clause 1052.201.70 *Contracting Officer's Technical Representative Appointment and Authority* is not available via an external link.

B. Office of Management and Budget (OMB) Memoranda

1. OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments[14]

This memorandum provides updated guidance on the reporting of security incidents involving personally identifiable information and reminds agencies of existing requirements, and explain new requirements agencies will need to provide addressing security and privacy in budget submissions for information technology.

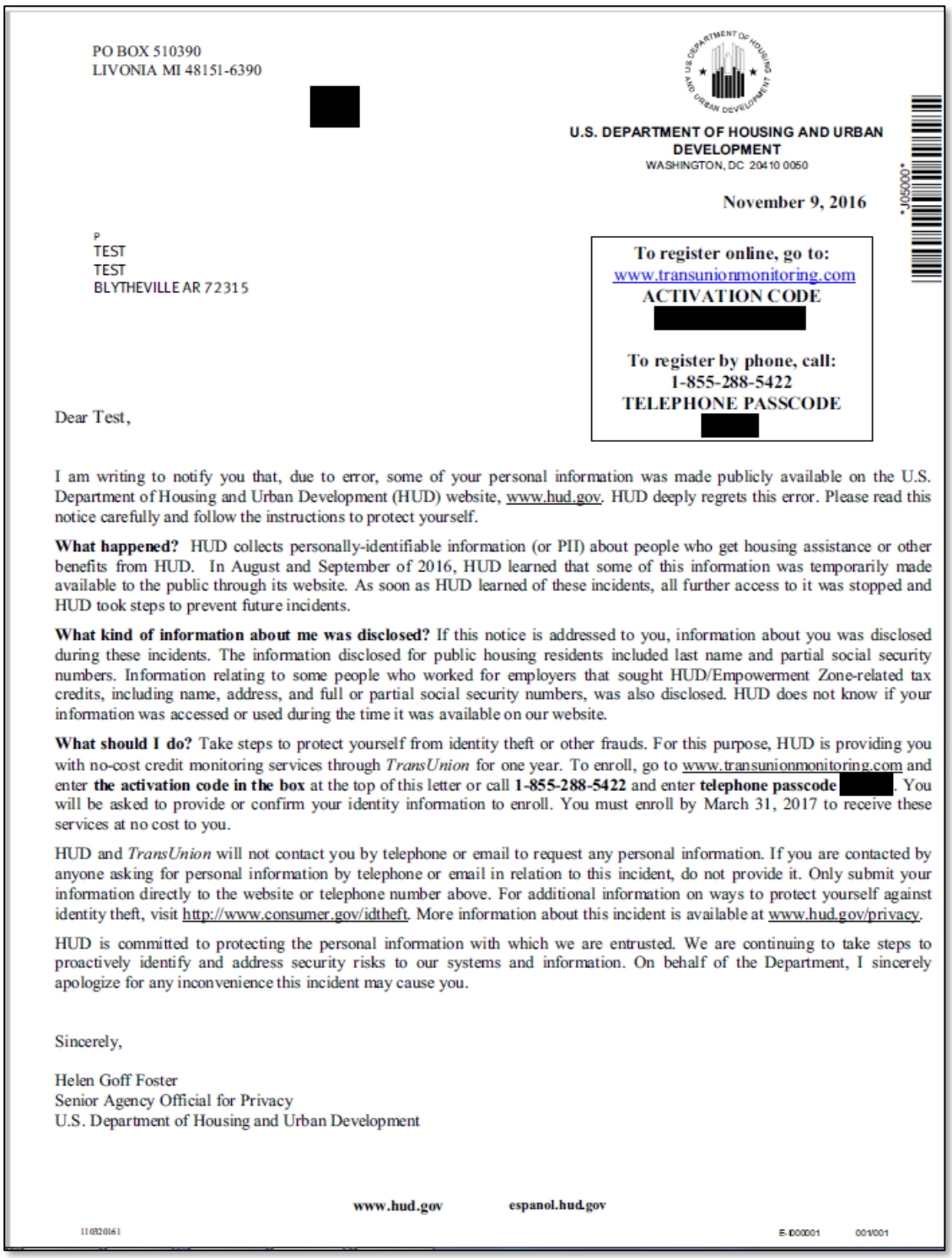
2. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information[15]

This memorandum requires agencies to develop a breach notification policy while ensuring proper safeguards are in place to protect the information in both paper and electronic form. Specifically, OMB M-07-16 requires agencies to develop policies and procedures for reporting and mitigating PII incidents and notification of incidents to the United States Computer Emergency Readiness Team (US-CERT)[16] within one hour of discovery.

[14] http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-19.pdf.
[15] http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf.
[16] US-CERT serves as the designated central reporting organization within the federal government and the central repository for federal incident data.

ATTACHMENT 2: NOTICE LETTER AND SUPPORT MATERIALS

A. English Language Notice



PO BOX 510390
LIVONIA MI 48151-6390

[redacted]

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410 0050

November 9, 2016

P
TEST
TEST
BLYTHEVILLE AR 72315

To register online, go to:
www.transunionmonitoring.com
ACTIVATION CODE
[redacted]

To register by phone, call:
1-855-288-5422
TELEPHONE PASSCODE
[redacted]

Dear Test,

I am writing to notify you that, due to error, some of your personal information was made publicly available on the U.S. Department of Housing and Urban Development (HUD) website, www.hud.gov. HUD deeply regrets this error. Please read this notice carefully and follow the instructions to protect yourself.

What happened? HUD collects personally-identifiable information (or PII) about people who get housing assistance or other benefits from HUD. In August and September of 2016, HUD learned that some of this information was temporarily made available to the public through its website. As soon as HUD learned of these incidents, all further access to it was stopped and HUD took steps to prevent future incidents.

What kind of information about me was disclosed? If this notice is addressed to you, information about you was disclosed during these incidents. The information disclosed for public housing residents included last name and partial social security numbers. Information relating to some people who worked for employers that sought HUD/Empowerment Zone-related tax credits, including name, address, and full or partial social security numbers, was also disclosed. HUD does not know if your information was accessed or used during the time it was available on our website.

What should I do? Take steps to protect yourself from identity theft or other frauds. For this purpose, HUD is providing you with no-cost credit monitoring services through *TransUnion* for one year. To enroll, go to www.transunionmonitoring.com and enter **the activation code in the box** at the top of this letter or call **1-855-288-5422** and enter **telephone passcode** [redacted]. You will be asked to provide or confirm your identity information to enroll. You must enroll by March 31, 2017 to receive these services at no cost to you.

HUD and *TransUnion* will not contact you by telephone or email to request any personal information. If you are contacted by anyone asking for personal information by telephone or email in relation to this incident, do not provide it. Only submit your information directly to the website or telephone number above. For additional information on ways to protect yourself against identity theft, visit http://www.consumer.gov/idtheft. More information about this incident is available at www.hud.gov/privacy.

HUD is committed to protecting the personal information with which we are entrusted. We are continuing to take steps to proactively identify and address security risks to our systems and information. On behalf of the Department, I sincerely apologize for any inconvenience this incident may cause you.

Sincerely,

Helen Goff Foster
Senior Agency Official for Privacy
U.S. Department of Housing and Urban Development

www.hud.gov **espanol.hud.gov**

110820161 E-000001 001/001

B. Spanish Language Notice

EL DEPARTAMENTO DE VIVIENDA Y DESARROLLO URBANO DE LOS ESTADOS UNIDOS
OFICINA DE LA SUBSECRETARIA
WASHINGTON, DC 20410 0050

09 de Noviembre, 2016

Para registrarse en línea, vaya a:
www.transunionmonitoring.com
CÓDIGO DE ACTIVACIÓN
[redacted]

Para registrarse por teléfono llame:
1-855-288-5422
CODIGO DE ACCESO TELEFÓNICO
[redacted]

Estimado(a) Test,

Le escribo para notificarle que, debido a un error, algunos de sus datos personales estuvieron expuestos o disponibles al público en el sitio web del Departamento de Vivienda y Desarrollo Urbano de los Estados Unidos (HUD), en **www.hud.gov**. HUD lamenta profundamente este error. Por favor, lea este aviso cuidadosamente y siga las instrucciones para protegerse.

¿Qué pasó? HUD recopila información de identificación personal (conocida como PII, por sus siglas en inglés) de las personas que reciben asistencia de vivienda u otros beneficios de HUD. En agosto y septiembre de 2016, HUD se dio cuenta que alguna de esta información estaba disponible temporalmente al público a través de su página web. Tan pronto como HUD tuvo conocimiento de estos incidentes, todo acceso a la información fue detenido y HUD tomó medidas para prevenir futuros incidentes.

¿Qué tipo de información sobre mí se reveló? Si este anuncio está dirigido a usted, su información se dio a conocer durante estos incidentes. La información revelada de los residentes de vivienda pública incluyó apellidos y una porción de sus números de seguro social. También se dio a conocer información relacionada con algunas personas que trabajaron para los empresarios que buscaban créditos fiscales relacionados con HUD y zonas conocidas como *Empowerment Zones*, incluyendo nombre, dirección y números de seguro social completos o parciales. HUD no sabe si su información fue accedida o usada durante el tiempo que estuvo disponible en nuestro sitio web.

¿Qué debo hacer? Tome medidas para protegerse del robo de identidad u otros fraudes. Con este propósito, HUD le está proporcionando, sin costo, servicios de monitoreo de crédito a través de TransUnion, por un año. Para inscribirse, vaya a www.transunionmonitoring.com e introduzca el **código de activación en el cuadro** que se encuentra en la parte superior de esta carta o llame al **1-855-288-5422** e introduzca el **código de acceso telefónico** [redacted]. Se le pedirá que proporcione o confirme su información de identidad para inscribirse. Debe inscribirse antes del 31 de marzo de 2017 para recibir estos servicios sin costo para usted.

HUD y *TransUnion* no se pondrán en contacto con usted por teléfono o correo electrónico para solicitar cualquier información personal. Si usted es contactado por alguien pidiendo información personal por teléfono o correo electrónico en relación con este incidente, no la proporcione. Sólo envíe su información directamente a la página web o número de teléfono mencionados arriba. Para obtener información adicional sobre las formas de protegerse contra el robo de identidad, visite http://www.consumer.gov/idtheft. Más información sobre este incidente está disponible en www.hud.gov/privacy.

HUD está comprometido a proteger la información personal con la que se nos ha confiado. Estamos continuando a tomar medidas para identificar de forma proactiva y hacer frente a los riesgos de seguridad de nuestros sistemas y a la información. En nombre del Departamento, me disculpo sinceramente por cualquier inconveniente que este incidente pueda causarle.

Sinceramente,

Helen Goff Foster
Alta Funcionaria para la Privacidad en la Agencia
Departamento de Vivienda y Desarrollo Urbano de los EE.UU.

www.hud.gov **espanol.hud.gov**

C. Frequently Asked Questions

Privacy Incidents at HUD

Frequently Asked Questions

HUD routinely collects personally-identifiable information (or PII) about people who receive housing assistance or other benefits from HUD. PII is information which can be used to distinguish or trace an individual's identity, such as their name or social security number. In August and September of 2016, HUD learned that some of this information was temporarily available to the public through its website. As soon as HUD learned of these incidents, all further access to it was stopped, and HUD took steps to prevent future incidents.

What happened?

- In late August and early September, HUD was alerted to two separate privacy incidents involving PII stored in Excel spreadsheets without adequate security measures.
- The first incident was reported to HUD on August 29, 2016. It involved PII collected by HUD's Empowerment Zone/Renewal Community Locator online tool (EZ/RC locator)
- The second incident was reported to HUD on September 14, 2016. It involved PII pertaining to residents in public housing and the fulfillment of Community Service Self Sufficiency (CSSR) requirements.

August 29, 2016 Incident Involving EZ/RC Locator

What is the EZ/RC Locator?

- Introduced in 1993, the Empowerment Zone (EZ), Enterprise Community (EC), and Renewal Community (RC) Initiatives sought to reduce unemployment and generate economic growth through the designation of Federal tax incentives and award of grants to distressed communities. Local, Tribal, and State governments interested in participating in this program were required to present comprehensive plans that included the following principles:
  - Strategic Visions for Change
  - Community-Based Partnerships
  - Economic Opportunities
  - Sustainable Community Development

- Communities selected to participate in this program embraced these principles and led projects that promoted economic development in their distressed communities. Tax incentives for employers to hire EZ, EC and RC residents were among the federal benefits available to designated communities. HUD developed the EZ/RC Locator to assist employers in determining whether employees' addresses were in the designated geographic areas for purposes of claiming tax incentives.

1 | Page

HUD Response

- On August 29, 2016, HUD was notified that PII including social security numbers (SSN) was accessible on a www.hud.gov website. The PII had been identified via an internet "Google" search.
- HUD subsequently determined that the information was contained in Excel files inadvertently collected through the EZ/RC locator system, and improperly stored on a web-server.
- Upon confirmation of the incident, public access to the directory of files was removed and the upload feature disabled.
- HUD did not request, and did not need this extraneous information. Until reported, HUD was not aware that this information had been erroneously uploaded to the server.
- Further review revealed that, despite the EZ/RC locator instructions that requested uploading of address only, approximately 20% of third-party employers and tax preparers using the Locator had uploaded spreadsheets containing unnecessary PII, including names, social security numbers, and date of birth.
- HUD has undertaken a review of external websites to identify any additional instances of unsecured PII stored or available. To date, these efforts have not identified any additional incidents. This work is ongoing.

PII Disclosed

- The spreadsheets uploaded into the EZ/RC Locator varied in the number of individuals and the type of PII included. Most commonly, the files contained name, full or truncated social security numbers, and address. In some cases, addition PII was included, for example: date of birth, income, and demographic information.

How many people were impacted?

- 35,533

How long was the PII available?

- The files uploaded to the server through the EZ/RC system dated back to 2014. Access to view or upload files through the EZ/RC locator was disabled on August 31, 2016.

September 14, 2016 Incident Involving CSSR information

What is CSSR?

- CSSR is the Community Service and Self Sufficiency requirement for public housing residents. Basically, public housing residents between the ages of 18 and 62 are required to perform a certain amount of public service each month and Public Housing Authorities (PHAS) are required to report compliance or non-applicability of their residents in the above age group. An OIG audit found that HUD was not monitoring the requirement

sufficiently and HUD responded by developing reports to share with PHAs to assist them in fulfilling this requirement.

HUD Response

- On September 14, 2016, HUD received notice of an incident involving unsecured Excel files containing PII available at a public-facing website on www.hud.gov.
- The Excel files were posted as part of HUD's CSSR reporting initiative.
- Links to the identified file were disabled, and HUD began a review of the incident.
- The website information was supplied to points of contact at all PHAs so that each PHA could cull information related to its residents. This also allowed any PHA point of contact to review information related to residents outside of the PHA's area.
- HUD has undertaken a review of external websites to identify any additional instances of unsecured PII stored or available. To date, these efforts have not identified any additional incidents. This work is ongoing.

PII Disclosed

- HUD's CSSR reporting included resident last name, last four digits of the resident's social security number, and building code identifiers.

How long was the PII available?

- HUD made these postings five separate times beginning in August 2015.
- After this incident was reported, HUD confirmed that the information could no longer be accessed online on September 22, 2016.

How many people were impacted?

- 428,828

How do I know if these incidents impacted me?

- HUD is providing direct notice by mail to all individuals impacted by this incident. Those individuals will be offered no-cost credit monitoring services for 1 year.
- If you are impacted by this incident, you will receive a <notice letter>link in the mail. Please note: HUD will NOT contact you by telephone or email to request information.

ATTACHMENT 3: TIMELINES

A. Timeline for Incident A

- On August 29, an email was sent the OCIO Web Manager (ociowebmanager@hud.gov) from a Member of the Public stating, "*I'm hoping I'm contacting the right person here, if not maybe you can direct me to who I need to talk to. I believe I may have stumbled across a security issue with HUD.gov, I was hoping to be able to speak with someone about it to get it escalated. Would you be able to assist with this? I'd prefer to speak by phone if possible. Thanks.*"
- On August 30, the HUD webmaster reported the incident to the HUD Helpdesk, and CISO staff investigated the incident immediately.
- On August 31, the eGIS System was taken off line. Later that day the system was brought back on line, but the Locator tool feature to upload spreadsheets was disabled.
- On August 31, CISO began analysis of the Excel files to determine the scope of the incident.
- On September 15, CISO briefed the HUD Privacy Branch and SAOP and made a determination to report the incident to DHS US-CERT as a category 1 (unauthorized access) incident, as required.
- On September 16, CISO and SAOP reported the incident to OMB as required.
- On September 16, SAOP initiated the HUD Breach Notification Incident Response Plan, and called a meeting of the HBIRT in accordance with the plan. The HBIRT includes the Principals or representatives from each HUD CXO office, the Office of the General Counsel, the impacted program office(s), and the Office of the Deputy Secretary.
- On September 19, the HBIRT was convened for the first time, was briefed on the incident, reviewed actions taken, and planned next steps. HBIRT continued to meet regularly to receive updates and identify additional actions to be taken.
- On September 20 after being briefed on the findings from the investigation, the HBIRT declared (via a unanimous vote) that the incident was a Major Incident that posed a High Risk of Harm to individuals. The team reviewed the draft Action Plan, and commenced executing required actions.
- From November 10, 2016 through November 23, 2016, 35,533 notices were mailed to individuals impacted by this privacy incident.
- As of November 30, approximately 2% of those individuals have registered for credit monitoring services (this includes a total of 8,195 across both incidents). All impacted individuals will have the opportunity to register for credit monitoring service through March 31, 2017.
- On December 21, HIBIRT discussed the incident report and the SAOP recessed the HIBIRT for this incident.

B. Timeline for Incident B

- On September 14 (5:26pm), HUD was alerted by an Attorney at the Housing Justice Center that a HUD website listed names of public housing tenants, partial social security numbers, and in some cases, reported disability status.

- On September 15, the Program Office was notified and that afternoon (2:17pm), public access to the main URL was removed, assuming this removed all access. (However, underlying links to the spreadsheets remained active.)
- On September 22 (2:26pm), HUD CIR was notified by the Housing Financial Services Committee that an email from a vendor who works with PHAs had forwarded the same information via email and that PII was still posted.
- On September 22, HUD discovered that underlying links to the spreadsheets had remained active and immediately disabled them.
- On September 22 (6:01pm), CISO briefed SAOP and a determination was made to report the incident to DHS US-CERT as a Category 4 incident, as required. [insert CERT Ticket #]
- On September 23, CISO and HUD Cyber Incident Response Team (CIRT) staff began investigating the incident immediately. CISO began analysis of the Excel files to determine scope of the incident.
- On September 23, CISO and SAOP reported the incident to OMB as required.
- On September 26, SAOP convened the HBIRT. The HBIRT includes the Principals or representatives from each HUD CXO office, the Office of the General Counsel, the impacted program office(s), and the Office of the Deputy Secretary.
- On September 26, HBIRT declared this was a **Major Incident** under FISMA (OMB M-16-03).
- On September 28, HBIRT declared incident a **MEDIUM risk to INDIVIDUALS** impacted by event under M-07-16. In addition, due to an abundance of caution and due the nature of information released and specific context of the circumstances, **HUD made the decision to notify individuals and provide credit monitoring services**. Key factors affecting the likelihood of harm include social and financial vulnerability of public housing residents.
- On September 28, HUD began Congressional notifications which continued to September 29.
- On November 10, a letter was emailed to 2,690 PHA Executive Directors advising them of the incident and HUD's action plan. The letter asked for Housing Authority personnel to assist with helping residents understand the notification letter and encouraging them to request credit monitoring services.
- From November 11, 2016 through November 30, 390,126 notices were mailed, and an additional 38,702 notices (which required additional address look-up services) were mailed from December 1 through December 2. This resulted in a total of 428,828 notices across both mailings.
- As of November 30, approximately 2% of those individuals have registered for credit monitoring services (this includes a total of 8,195 across both incidents). All impacted individuals will have the opportunity to register for credit monitoring service through March 31, 2017.
- On December 21, HIBIRT discussed the incident report and the SAOP recessed the HIBIRT for this incident.

ATTACHMENT 4: LETTER TO EXECUTIVE DIRECTORS

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

WASHINGTON, DC 20410-5000

DEPUTY ASSISTANT SECRETARY
REAL ESTATE ASSESSMENT CENTER
OFFICE OF PUBLIC AND INDIAN HOUSING

Thursday, November 10, 2016

Dear Executive Director,

The U.S. Department of Housing and Urban Development (HUD) is committed to protecting the personal information with which we are entrusted. The purpose of this correspondence is to notify you that some of your residents will receive a letter offering no-cost credit monitoring services for one (1) year. This service is being offered because HUD learned that while sharing community service requirement information with local housing authorities, some personal information of public housing residents was made available through its website. The website information is no longer available.

While the disclosed information presents a minimal risk to the residents, we ask for your assistance in helping residents understand the notification letter and encouraging them to request credit monitoring services.

Residents will begin receiving the official notification by US mail on or around Monday, November 14, 2016, and there is a possibility that they may contact PHA officials and ask you to explain the letter and seek your advice. The no-cost credit monitoring service is being provided by TransUnion. The notification to affected residents includes TransUnion's website address (www.transunionmonitoring.com) and contact telephone number (1-855-288-5422) for enrollment. It is important to inform residents that they must enroll by March 31, 2017, in order to receive the free service. You can view HUD's notice to residents here.

We apologize for any inconvenience this may have caused and thank you for responding to any questions asked by affected residents, as well as encouraging them to accept the no-cost credit monitoring services. For any additional information on this matter please refer to the HUD privacy website.

Sincerely,

Donald J. LaVoy

www.hud.gov espanol.hud.gov

Stay Connected with HUD's Office of Public and Indian Housing:

SUBSCRIBER SERVICES:
Manage Subscriptions | Unsubscribe All | Help