Supporting Statement – Part A

Supporting Statement for Paperwork Reduction Act Submission

State Health Insurance Exchange Incident Report

A. Background

As part of the privacy and security oversight of State Health Insurance Exchanges the States will be required to report security incidents including breaches of personally identifiable information (PII). This reporting will be made by completing and electronically submitting the State Health Insurance Exchange Security Incident Report (Incident Report), or providing identical information telephonically.

B. Justification

1 . Need and Legal Basis

45 CFR part 155 (attached) implements the Affordable Insurance Exchanges ("Exchanges") consistent with Title I of the Patient Protection and Affordable Care Act of 2010, referred to collectively as the Affordable Care Act. Section 155.260 describes Exchange requirements regarding the privacy and security of personally identifiable information (PII) including the establishment and implementation of standards consistent with the principle of accountability (Section 155.260(a)(3)(viii). The accountability principle "should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches."

For the purposes of oversight and monitoring PII safeguards the Centers for Medicare & Medicaid Services (CMS) will execute a Computer Matching Agreement (CMA) with the State-Based Administering Entities[1] (AEs). The CMA includes a requirement for AEs to report suspected or confirmed security incidents[2] affecting loss or suspected loss of PII within one hour of discovery to their designated CCIIO State Officer who will then notify the affected Federal agency data sources, i.e., Internal Revenue Service, Department of Defense, Department of Homeland Security, Social Security Administration, Peace Corps, Office of Personnel Management and Veterans Health Administration. The Incident Report will be used by the States to communicate breaches to CMS.

1 Administering Entities (AEs) are state entities administering Insurance Affordability Programs and who will use the data, accessed through the CMS Data Services Hub (Hub), to make Eligibility Determinations for Insurance Affordability Programs and certificates of exemption.

2 A security incident means the act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware or software without the owner's knowledge, instruction or consent. An incident becomes a breach when PII is involved.

2. Information Users

The information collected will be used by CMS conduct oversight of incidents occurring at the State Exchanges.

3. Use of Information Technology

States may submit Incident Reports by either completing the form either handwritten or electronically, and submitting it via email, or by calling the designated CMS Center for Consumer Information and Insurance Oversight (CCIIO) State Officer and providing the information verbally. These reporting options allow 24 hour submission of reports. It is anticipated that approximately 90% of all reports will be submitted electronically. Respondents are not required to sign the report.

4. Duplication of Efforts

This information collection does not duplicate any other effort and the information cannot be obtained from any other source.

5. Small Businesses

This collection of information will not impact small businesses or other small entities.

6. Less Frequent Collection

This data collection is essential to ensuring that incidents, which include breaches of PII, are captured expeditiously. In the absence of this reporting, incidents may not be detected and mitigated, thereby placing the public at a high risk of identity fraud and other misuses of the information.

7. Special Circumstances

Incident Reports must be submitted upon detection of the actual or suspected incident. Reporting less frequently increases the risk to the public for identity fraud and other misuses of the information.

8. Federal Register/Outside Consultation

The emergency Federal Register notice published on August 21, 2013.

9. Payments/Gifts to Respondents

Not Applicable

10. Confidentiality

CMS will comply with all Privacy Act (5 U.S.C. §552a), Freedom of Information laws (5 U.S.C. 552) and regulations (45 C.F.R. Part 5b; 45 C.F.R. Part 5

11. Sensitive Questions

There are not sensitive questions associated with this collection.

12. Burden Estimates (Hours & Wages)

The cost per respondent per form was determined using the follow wage:

- $ 42.93 per hour (Information Security Analyst wage Per BLS)

18 respondents x 0.25 hour reporting burden/report x 52 reports/year
= 234 hours annual burden

234 hours x $42.93/hr wage = $10,045.62

States have never provided this type of reporting to CMS in the past. Estimates are based on similar processes used within the Agency.

13. Capital Costs

There is no capital cost associated with this collection.

14. Cost to Federal Government

Incident Reports will be processed in the normal course of Federal duties. 6 FTE's GS13, 41.00 hr x2=82x6=$502.00

15. Changes to Burden

Not Applicable

16. Publication/Tabulation Dates

This collection of information will not be published.

17. Expiration Date

CMS would like an exemption from displaying the expiration date as these forms are used on a continuing basis.

18. Certification Statement

There are no exceptions to item 19 of OMB Form 83-I.