Supporting Statement for Requests for OMB Approval
For Revised Confidentiality Pledge

Summary

Emergency clearance procedures are being used to obtain Paperwork Reduction Act (PRA) clearance from OMB for the referenced Information Collection Requests (ICRs), in order to implement revised pledge language that is resulting from the mandatory implementation of Einstein monitoring by the Department of Homeland Security (DHS). More specifically, the Cybersecurity Enhancement Act of 2015 (codified in relevant part at 6 U.S.C. § 151), mandates that federal information systems be protected from malicious activities through cybersecurity screening of transmitted data. Approval of this ICR using emergency clearance procedures is necessary to implement a change to the confidentiality pledge to notify respondents of the Einstein monitoring. The Bureau of Justice Statistics (BJS), a component of the Office of Justice Programs (OJP) in the U.S. Department of Justice (DOJ), is required to implement Einstein 3A by December 18, 2016, in accordance with the law. *See* 44 U.S.C. § 3507(j) and 5 C.F.R. § 1320.13.

As per OMB instruction, this single ICR is being submitted to update BJS's pledge of confidentiality for the below listed packages and will not otherwise affect the content, scope, burden, or the current expiration dates of any of these packages. BJS is requesting to add the bolded lines to its pledge of confidentiality to address the new cybersecurity monitoring screening requirements and activities:

"The Bureau of Justice Statistics (BJS) is dedicated to maintaining the confidentiality of your personally identifiable information, and will protect it to the fullest extent under federal law. BJS, BJS employees, and BJS data collection agents will use the information you provide for statistical purposes only, and will not disclose your information in identifiable form without your consent to anyone outside of the BJS project team. All data collected under BJS's authority are maintained under the security provisions outlined in the U.S. Department of Justice statutes at 42 U.S.C. §§ 3735 and 3789g. Any person violating these confidentiality provisions may be punished by a fine up to $10,000, in addition to any other penalty imposed by law. ***Further, per the Cybersecurity Enhancement Act of 2015 (codified in relevant part at 6 U.S.C. § 151), federal information systems are protected from malicious activities through cybersecurity screening of transmitted data. For more information on the federal statutes, regulations, and other authorities that govern how BJS, BJS employees, and data collection agents use, handle, and protect your information, see the BJS Data Protection Guidelines."***

OMB NUMBER	TITLE OF SURVEY AND ABSTRACT
1121-0065	**National Corrections Reporting Program (NCRP)** The National Corrections Reporting Program (NCRP) is the only national data collection furnishing annual individual-level information for State prisoners admitted or released during the year, those in custody at year-end, and persons discharged from parole supervision. The NCRP collects data on sentencing, time served in prison and on parole, offense, admission/release type and demographic information. BJS, the Congress, researchers and criminal justice practitioners use these data to describe annual movements of adult offenders through State correctional system. Providers of the data are personnel in State Departments of Corrections. To review the current OMB-approved Information Collection materials, see -https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201508-1121-001

OMB NUMBER	TITLE OF SURVEY AND ABSTRACT
1121-0094	**Deaths in Custody Reporting Program (DCRP)** The Deaths in Custody Reporting Program (DCRP) collects data on deaths that occur in the process of arrest, or while inmates are in the custody of local jails or state prisons. Local jail and state prison data are collected directly from jails and state departments of corrections. Arrest-related mortality data are collected separately from data on deaths that occur in prisons or jails. The DCRP provides individual-level data on the number of deaths by year, cause of death, and decedent age, race or Hispanic origin, and sex. These data are also used to produce facility and population mortality rates. The collection of individual-level data allows BJS to perform detailed analyses of comparative death rates across demographic categories and offense types, as well as facility and agency characteristics. BJS began the DCRP in 2000 under the Death in Custody Reporting Act of 2000 (P.L. 106-297), which required the collection of individual data on deaths in the process of arrest, local jails, and state prisons. BJS continued the program after this legislation expired in 2006 and continues it with the reauthorization of the Death in Custody Reporting Act of 2013 (P.L. 113-242). To review the current OMB-approved Information Collection materials, see -https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201511-1121-002

National Crime Victimization Survey collections

The Census Bureau collects data on behalf of BJS for the National Crime Victimization Survey (NCVS) and several supplemental surveys. These collections are protected under Title 13 U.S.C. Section 9.

The Census Bureau issued a separate FRN and submitted an emergency clearance request to OMB to revise its confidentiality pledge for its affected information collections, including the below listing of NCVS information collections, with the bolded line added to address the new cybersecurity screening requirements:

"The U.S. Census Bureau is required by law to protect your information. The Census Bureau is not permitted to publicly release your responses in a way that could identify you. ***Per the Federal Cybersecurity Enhancement Act of 2015, your data are protected from cybersecurity risks through screening of the systems that transmit your data."***

OMB Control No.	**Information Collection Title**
1121-0111	National Crime Victimization Survey (NCVS)
1121-0184	School Crime Supplement to the NCVS
1121-0317	Identity Theft Supplement to the NCVS
1121-0260	Police Public Contact Supplement to the NCVS
1121-0302	Supplemental Victimization Survey to the NCVS

The FRN submitted by the Census Bureau can be accessed at https://www.federalregister.gov/documents/2016/12/14/2016-30014/confidentiality-pledge-revision-notice, and the Census Bureau's PRA clearance request can be accessed at https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201612-0607-001.

A. Justification

1. Necessity of Collection:

No change from currently approved underlying packages.

2. Description of the Information Collected:

No change from currently approved underlying packages.

3. Use of Technology to Reduce Burden:

No change from currently approved underlying packages.

4. Identification of Duplication and Availability or Similar Information:

No change from currently approved underlying packages.

5. Small Businesses:

No change from currently approved underlying packages.

6. Less Frequent Conduct of Study:

No change from currently approved underlying packages.

7. Special Circumstances:

No change from currently approved underlying packages.

8. Consultation with Persons Outside of BJS:

This ICR is being submitted under PRA emergency clearance procedures. BJS has submitted a 60-day FRN for publication and will consider public comments received in response to that document.

9. Gifts or Payments to Respondents:

No change from currently approved underlying packages.

10. Confidential Responses:

Pursuant BJS's statutory responsibilities, BJS must maintain the confidentiality of all data they collect and provide a pledge of confidentiality to respondents for collections involving personally

identifiable information. As required by the passage of the Federal Cybersecurity Enhancement Act of 2015, the federal statistical community has implemented DHS' Einstein 3A Cybersecurity Protection Program. Federal statistical agencies are thus modifying their confidentiality pledges to notify respondents of the cybersecurity screening requirements and activities.

BJS information collections involving personally identifiable information

In accordance with BJS's authorizing statute, the Director of BJS "shall be responsible for the integrity of data and statistics and shall protect against improper or illegal use or disclosure." 42 U.S.C. § 3732(b). Further, pursuant to 42 U.S.C. § 3789g, no officer or employee of the federal Government, including BJS employees or BJS data collection agents and contractors, may use or reveal any research or statistical information furnished in connection with a BJS data collection, including data identifiable to any specific private person, by any person for any purpose other than the purpose for which it was obtained. Additionally, under that statute, statistical information provided to BJS that is identifiable to a private person is immune from legal process, and may not, without the consent of the person furnishing such information, be admitted as evidence or be used for any purpose in any action, suit, or other judicial, legislative, or administrative proceedings. Any person violating these confidentiality provisions may be punished by a fine not to exceed $10,000 in addition to any other penalty imposed by law.

For collections conducted by BJS or BJS data collection agents involving personally identifiable information, the following confidentiality pledge will be provided, with the lines in bold added to address the implementation of Einstein 3A (for review purposes only):

"The Bureau of Justice Statistics (BJS) is dedicated to maintaining the confidentiality of your personally identifiable information, and will protect it to the fullest extent under federal law. BJS, BJS employees, and BJS data collection agents will use the information you provide for statistical purposes only, and will not disclose your information in identifiable form without your consent to anyone outside of the BJS project team. All data collected under BJS's authority are maintained under the security provisions outlined in the U.S. Department of Justice statutes at 42 U.S.C. §§ 3735 and 3789g. Any person violating these confidentiality provisions may be punished by a fine up to $10,000, in addition to any other penalty imposed by law. ***Further, per the Cybersecurity Enhancement Act of 2015 (codified in relevant part at 6 U.S.C. § 151), federal information systems are protected from malicious activities through cybersecurity screening of transmitted data. For more information on the federal statutes, regulations, and other authorities that govern how BJS, BJS employees, and data collection agents use, handle, and protect your information, see the BJS Data Protection Guidelines."***

BJS Data Protection Guidelines

BJS has added additional details about the Cybersecurity Enhancement Act and EINSTEIN 3Ato the BJS Data Protection Guidelines, which are referenced in the pledge and provide a way for interested respondents to obtain additional information about the new cybersecurity monitoring requirements. The following text has been added to *Section V. Information System Security and Privacy Requirements*:

"The Cybersecurity Enhancement Act of 2015 (codified in relevant part at 6 U.S.C. § 151) required the Department of Homeland Security (DHS) to provide cybersecurity protection for federal civilian agency information technology systems and to conduct cybersecurity screening of the Internet traffic going in and out of these systems to look for viruses, malware, and other cybersecurity threats. DHS has implemented this requirement by instituting procedures such that, if a potentially malicious malware signature were found, the Internet packets that contain the malware signature would be further inspected, pursuant to any required legal process, to identify and mitigate the cybersecurity threat. In accordance with the Act's provisions, DHS

conducts these cybersecurity screening activities solely to protect federal information and information systems from cybersecurity risks. OJP has installed DHS's cybersecurity protection software, Einstein 3A, on its information technology systems to comply with the Act's requirements and to further safeguard the information transmitted to and from its systems, including BJS data, from cybersecurity threats and vulnerabilities."

11. Sensitive Questions:

No change from currently approved underlying packages.

12. Burden of Collection:

No change from currently approved underlying packages.

13. Capital/Start-up Cost

There are no capital/start-up costs in any of the currently approved underlying packages.

14. Cost to the Federal Government:

No change from currently approved underlying packages.

15. Changes in Burden:

There is no change in respondent burden for the currently approved underlying packages by the addition of the new sentence notifying of Einstein monitoring.

16. Publication Plans/Schedule:

No change to plans from the currently approved underlying packages.

17. OMB Approval Expiration Date:

No change to current requests not to display the expiration dates for the currently approved underlying packages.

18. Exception to Certification Statement:

There are no exceptions to the certification statement.

Part B—Statistical Methods

BJS has determined no Part B is needed for this ICR, as there is no change to the statistical methods from those in the currently approved underlying packages.