

Bureau of Justice Statistics (BJS)

BJS Confidentiality Pledge Revision Notice

AGENCY: Department of Justice, Office of Justice Programs, Bureau of Justice Statistics

ACTION: Notice of Revision of Confidentiality Pledges under 42 U.S.C. §§ 3735 and 3789(g)

SUMMARY:

Under [44 U.S.C. § 3506\(e\)](#), and [44 U.S.C. § 3501](#), the Bureau of Justice Statistics (BJS), a component of the Office of Justice Program (OJP) in the U.S. Department of Justice (DOJ), is announcing revisions to the confidentiality pledge(s) it provides to its respondents under 42 U.S.C. §§ [3735](#) and [3789\(g\)](#). These revisions are required by the passage and implementation of provisions of the federal Cybersecurity Enhancement Act of 2015 (codified in relevant part at [6 U.S.C. § 151](#)), which permit and require the Secretary of Homeland Security to provide Federal civilian agencies' information technology systems with cybersecurity protection for their Internet traffic. More details on this announcement are presented in the SUPPLEMENTARY INFORMATION section below.

DATES: These revisions become effective upon publication of this notice in the **Federal Register**.

ADDRESSES: Questions about this notice should be addressed to the Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, ATTN: Allina Lee, 810 7th Street, NW, Washington, D.C. 20151.

FOR FURTHER INFORMATION CONTACT: Allina Lee by telephone at 202-305-0765 (this is not a toll-free number); by email at Allina.Lee@usdoj.gov; or by mail or courier to the Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, ATTN: Allina Lee, 810 7th Street, NW, Washington, D.C. 20151. Because of delays in the receipt of regular mail related to security screening, respondents are encouraged to use electronic communications.

SUPPLEMENTARY INFORMATION: Federal statistics provide key information that the Nation uses to measure its performance and make informed choices about budgets, employment, health, investments, taxes, and a host of other significant topics. The overwhelming majority of Federal surveys are conducted on a voluntary basis. Respondents, ranging from businesses to households to institutions, may choose whether or not to provide the requested information. Many of the most valuable Federal statistics come from surveys that ask for highly sensitive information such as proprietary business data from companies or particularly personal information or practices from individuals. Strong and trusted confidentiality and exclusively statistical use pledges under 42 U.S.C. §§ 3735 and 3789(g), Title 13 U.S.C. Section 9, and similar statistical confidentiality pledges, are effective and necessary in honoring the trust that businesses, individuals, and institutions, by their responses, place in statistical agencies.

Under 42 U.S.C. §§ 3735 and 3789(g) and similar statistical confidentiality protection statutes, many Federal statistical agencies make statutory pledges that the information respondents provide will be seen only by statistical agency personnel or their agents and will be used only for statistical purposes. These acts protect such statistical information from administrative, law enforcement, taxation, regulatory, or any other non-statistical use and immunize the information submitted to statistical agencies from legal process. Moreover, many of these statutes carry monetary fines and/or criminal penalties for conviction of a knowing and willful unauthorized disclosure of covered information. Any person violating the confidentiality provisions of 42 U.S.C. §§ 3735 and 3789(g) may be punished by a fine up to \$10,000, in addition to any other penalties imposed by law.

As part of the Consolidated Appropriations Act for Fiscal Year 2016 signed on December 17, 2015, the Congress included the Federal Cybersecurity Enhancement Act of 2015 (codified in relevant part at 6 U.S.C. § 151). This Act, among other provisions, permits and requires the Secretary of Homeland Security to provide Federal civilian agencies' information technology systems with cybersecurity protection for their Internet traffic. The technology currently used to provide this protection against cyber malware is known as Einstein 3A. Einstein 3A electronically searches Internet traffic in and out of Federal civilian agencies in real time for malware signatures.

When such a signature is found, the Internet packets that contain the malware signature are shunted aside for further inspection by Department of Homeland Security (DHS) personnel. Because it is possible that such packets entering or leaving a statistical agency's information technology system may contain a small portion of confidential statistical data, statistical agencies can no longer promise their respondents that their responses will be seen only by statistical agency personnel or their agents. However, they can promise, in accordance with provisions of the Federal Cybersecurity Enhancement Act of 2015, that such monitoring can be used only to protect information and information systems from cybersecurity risks, thereby, in effect, providing stronger protection to the integrity of the respondents' submissions.

Consequently, with the passage of the Federal Cybersecurity Enhancement Act of 2015, the Federal statistical community has an opportunity to welcome the further protection of its confidential data offered by DHS' Einstein 3A cybersecurity protection program. The DHS cybersecurity program's objective is to protect Federal civilian information systems from malicious malware attacks. The Federal statistical system's objective is to ensure that the DHS Secretary performs those essential duties in a manner that honors the Government's statutory promises to the public to protect their confidential data. Given that DHS is not a Federal statistical agency, both DHS and the Federal statistical system have been

successfully engaged in finding a way to balance both objectives and achieve these mutually reinforcing objectives.

Accordingly, DHS and Federal statistical agencies, in cooperation with their parent departments, have developed a Memorandum of Agreement for the installation of Einstein 3A cybersecurity protection technology to monitor their Internet traffic and have incorporated an associated Addendum on Highly Sensitive Agency Information that provides additional protection and enhanced security handling of confidential statistical data.

However, pledges of confidentiality made pursuant to 42 U.S.C. §§ 3789g and 3735 and similar statistical confidentiality pledges promise that respondents' data will be seen only by statistical agency personnel or their agents. Since it is possible that DHS personnel could see some portion of those confidential data in the course of examining the suspicious Internet packets identified by Einstein 3A sensors, statistical agencies need to revise their confidentiality pledges to reflect this process change.

Therefore, BJS is providing this notice to alert the public to these confidentiality pledge revisions in an efficient and coordinated fashion. Below is a listing of BJS's current Paperwork Reduction Act (PRA) OMB numbers and information collection titles and their associated revised confidentiality pledge(s) for the Information Collections whose confidentiality pledges will change to reflect the statutory implementation of DHS' Einstein 3A monitoring for cybersecurity protection purposes.

The following BJS statistical confidentiality pledge will now apply to the Information Collections conducted by BJS and protected under 42 U.S.C. §§ 3735 and 3789(g), whose PRA OMB numbers and titles are listed below. The new lines added to address the new cybersecurity monitoring activities are bolded for reference only, and will not be bolded in the pledge provided to respondents:

*“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 Control No.	Information Collection Title
1121-0094	Deaths in Custody Reporting Program
1121-0065	National Corrections Reporting Program

BJS has also added information about the Cybersecurity Enhancement Act and Einstein 3A to the [BJS Data Protection Guidelines](#) to provide more details to interested respondents 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.”

The Census Bureau collects data on behalf of BJS for the below listing of PRA OMB numbers and information collection titles. These collections are protected under Title 13 U.S.C. Section 9. The Census Bureau issued an FRN and submitted an emergency clearance request to OMB for revised confidentiality pledge language, with the new line to address the new cybersecurity screening requirements bolded for reference:

*“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.**”*

<u>OMB Control No.</u>	<u>Information Collection Title</u>
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.

If additional information is required contact: Jerri Murray, Department Clearance Officer,
United States Department of Justice, Justice Management Division, Policy and Planning Staff,
Two Constitution Square, 145 N street NE, 3E.405B, Washington, DC 20530.

Dated:

Jerri Murray,

Department Clearance Officer for PRA, U.S. Department of Justice