World Privacy Forum Report

Data Brokers and the Federal Government: A New Front in the Battle for Privacy Opens

Third report in a series on data brokers

By Robert Gellman and Pam Dixon

October 30, 2013

Background of Report

This report focuses on government use of commercial data brokers, the implications for that usage, and what needs to be done to address privacy problems. The government must bring itself fully to heel in the area of privacy. If it is going to outsource its data needs to commercial data brokers, it needs to attach the privacy standards it would have been held to if it had collected the data itself. Outsourcing is not an excuse for evading privacy obligations.

This report discusses new Office of Management and Budget (OMB) guidance for an initiative (Do Not Pay Initiative) that on one hand provides for expanded use of commercial data brokers by federal agencies and on the other it establishes new privacy standards for the databases used in the Initiative. Although incomplete, its extension of privacy standards to commercial databases purchased by the federal government is groundbreaking. As such, this report recommends that OMB should expand its new guidance to cover *all* government data purchases, bartering, and exchanges from commercial data brokers and databases containing personal information. The problems created by unregulated government use of commercial data sources need to be seen clearly and addressed directly.

If all federal government uses of commercial data brokers are not required to satisfy the new OMB guidelines at a minimum, then the very databases that are supposed to be used for society's benefit will be less accurate, timely, relevant, and complete, and can therefore cause unnecessary and avoidable harms such as garbled identities, blocking individuals from government benefits, and potential misclassification or even law enforcement actions against people due to errors in data. On a broader level, a lack of trust in the government's ability to properly protect fair information rights in a new digital era can be the expensive societal result.

This report is Part III in a three-part series of reports concerning data brokers. Parts I and II are forthcoming. This report is available at www.worldprivacyforum.org, which is also where updates and further parts of the series will be published.

About the Authors

Robert Gellman is a privacy and information policy consultant in Washington DC. (www.bobgellman.com.) Pam Dixon is the Founder and Executive Director of the World Privacy Forum. Gellman and Dixon are the authors of *Online Privacy A Reference Handbook* (ABC CLIO, 2011) as well as co-authors and authors of numerous and well-regarded privacy-focused research, articles, and policy analysis.

About the World Privacy Forum

The World Privacy Forum is a non-profit public interest research and consumer education group focused on the research and analysis of privacy-related issues. The Forum was founded in 2003 and has published significant privacy research and policy studies in the area of health, online and technical, privacy, self-regulation, financial, and identity among other areas. www.worldprivacyforum.org

Executive Summary

The US federal government is one of the largest and most frequent customers of commercial data brokers. Instead of creating its own databases subject to privacy laws applicable to federal agencies, the federal government often outsources the collection of significant amounts of information to external companies where privacy laws do not apply. It is well-established that commercial data brokers have been and are widely used in this manner for government law enforcement activities. However, that is not their only use by government.

In April 2012, the US Treasury launched a Do Not Pay portal designed to verify and check on the eligibility of individuals to receive government benefits and payments, such as those receiving food stamps, housing assistance, and survivor benefits. The scope of the people and vendors affected by the information in the portal is quite broad. The portal includes government-operated databases with information about individuals, databases that are usually subject to the Privacy Act of 1974. However, the Do Not Pay portal also includes information from a commercial database called The Work Number. The Work Number, owned by Equifax, is not a government-held database and is not subject to the Privacy Act.

This is important because The Work Number collects salary and other information on more than 190 million Americans. However, unlike most of the government-maintained databases in the portal, The Work Number is not subject to the privacy rules that apply standards of accuracy, relevance, timeliness, and completeness to federally-operated databases. This matters because eligible people whose Work Number files contain errors may fail to pass verification to receive government benefits or payments for services provided to the government.

Few people know that their salary information is available commercially in this way, and few know that their salary information may be used to verify government benefits. If an individual is the victim of an identity thief who created fictitious or erroneous pay records, or if the Work Number data contains inadvertent or even intentional errors from participating employers, individuals will be harmed when the federal government relies on that information. In the case of the Do Not Pay portal, people may not receive government benefits for which they qualify. If the digital era has taught one lesson it has taught that errors in files and databases do not discriminate – errors, including identity errors -- can happen to any file in any data base, and they can impact the most vulnerable people who need government assistance the most. Those with data errors may need to work through a long correction process before they can receive their benefits. However, finding and correcting errors is difficult, especially when no law grants access and correction rights for most private sector databases.

By using The Work Number, the Do Not Pay portal employs the increasingly popular model of government outsourcing its data needs to commercial data brokers that do not have to abide by the same privacy standards applicable to the government, a model which has been criticized for its privacy shortcomings. This is because commercial databases do not have to satisfy the same privacy standards as databases held by the government. If the federal government obtains personal information from commercial data brokers but keeps the information outsourced and does not maintain that information in a government system of records, then a key law – the

Privacy Act of 1974 – imposes few or no privacy constraints on federal agencies, and no constraints at all on the commercial data brokers supplying the information.

Being denied important government benefits is no small matter, and meaningful privacy protections must be in place to prevent harms from data errors and other problems. Recognizing the potential for harm and the shortcomings of using private databases, the Office of Management and Budget took the novel and long-requested step of issuing new guidance that establishes privacy standards for commercial data brokers used in the Do Not Pay Portal, such as The Work Number. The new standards extend some of the privacy requirements applicable to the federal government to commercial databases that the government uses.

Albeit only within the Do Not Pay Initiative, this is the first time the government's commercial data outsourcing model has been meaningfully altered to apply important privacy safeguards.

The positive news is that because of the new OMB requirements, information in commercial databases used in the Do Not Pay Initiative– including The Work Number -- must be sufficiently accurate, up-to-date, relevant, and complete to ensure fairness to the individuals who are the subject of those records. The other good news is that the OMB standard rejects using a commercial database that includes records about the exercise of rights protected by the First Amendment. Commercial data brokers that cannot meet these standards will not be able to sell their information for the Do Not Pay Initiative.

The guidance is new, and it is welcome, but it is just one step. There are still significant loopholes remaining in the OMB guidance. As discussed, the "data outsourcing" model that allows the government to evade Privacy Act protections can still exist almost everywhere else in government other than the Do Not Pay Initiative. OMB should act to provide guidance to establish privacy standards that are at least a good as those in the Do Not Pay Initiative **covering all government purchases of commercial databases containing personal information**, not just those in the Do Not Pay Initiative. This action would serve the rest of the government well – and citizens for that matter -- by rejecting personal data from commercial sources that does not meet the same standards that the law imposes on that collected by federal agencies. Everyone benefits when better quality databases are used for decision-making about individuals. Programs will be more efficiently and more individuals will receive fair and appropriate treatment.

If this does not happen, and these standards are not created and applied to cover all government purchases of information from commercial databases, the model of government outsourcing its data needs while circumventing privacy protections will become a deeply entrenched norm across all levels of government. If the practice continues unabated, sloppy databases without the protection of federal standards can and will cause further harm to the millions of people who have been victims of identity theft and other forms of fraud, and the millions of people who unknowingly have erroneous, incomplete, or out of date information in their records.

When OMB wrote its new guidance, it only chose to use four of the much more complete set of Privacy Act standards to apply to the commercial databases in the Do Not Pay Initiative. (The four standards OMB used were that records must be accurate, up-to-date, relevant, and complete). OMB should not have cherry-picked some privacy standards while leaving others

behind. At the earliest opportunity, OMB needs to expand the privacy standards for the Do Not Pay Initiative to require that participating commercial databases comply fully with all Fair Information Practices, including collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, access and correction rights, and accountability. It is especially important that data subjects have meaningful, timely, and effective access and correction rights to any commercial databases used by federal agencies. OMB should take steps to expand the privacy standards at the earliest possible opportunity following a reasonable test of the new Do Not Pay procedures.

If the additional standards are not applied, then it could lead to a significant long-term weakening of privacy standards in government databases. A substantial reduction in privacy protections could be substituted as a new norm, which would be a negative consequence of truncating these protections in the long term.

Another issue in the OMB guidance is the allowance of a 6-month pilot period where the new rules do not apply. Currently, The Work Number is being used within this pilot program. Therefore, the information of the millions of people in this database is being tested and is available for viewing, although it is not supposed to be used for adverse actions during this period. The first substantive test of the new OMB guidance will be how the US Treasury and other participants in the Do Not Pay Initiative apply the guidance to The Work Number as it moves out of the pilot phase.

Before permanent use of The Work Number database can happen, the OMB requirements call for public notice and comment. This is another novel feature of the OMB privacy standards for the Do Not Pay Initiative. OMB should provide ample and prominent public notice and comment opportunity. The public notice should include full documentation about the accuracy, timeliness, relevance, and completeness of The Work Number. An independent audit of The Work Number's compliance with these data standards would be especially useful. In addition, all of the data fields maintained by The Work Number must be published to allow the public to evaluate whether any of the data reflects on the exercise of First Amendment rights.

If the privacy protections OMB established are effective, it will be an important step forward. At least in the Do Not Pay Initiative, people would have more ability to challenge the information coming from databases such as The Work Number and get redress from problems when they occur. If the OMB guidance was then taken up widely across the federal government and by state governments, the result could be better quality commercial databases for use by governments and by others. There would be fewer errors, less fraud, less government waste, more redress for individuals, and a higher overall standard of modern fair information practices would be set. Data could be used in a fair way that helps, not hurts, people.

Table of Contents:

I. Introduction and Background

The US federal government uses commercial data brokers[1] extensively for a wide variety of governmental activities. It is unquestioned that the government provides considerable revenue to commercial data brokers. How much? A reasonable and conservative estimate is that the number ranges in the billions of dollars. Over the course of the last 20 years, the extent of the relationship has become clear through a series of detailed investigations and scholarly research. For background purposes, we reference a leading study and discuss a newer use. This report does not seek to reinvestigate and re-document known uses.

Generally, government use of commercial data providers accelerated after 9/11 and has been quite extensive in the area of law enforcement.[2] The extent of the use was documented through repeated Freedom of Information Act requests and subsequent analysis by Chris Jay Hoofnagle, who then worked at the Electronic Privacy Information Center and is currently the Director of Information Privacy Programs, Berkeley Center for Law & Technology, UC Berkeley School of Law. His paper, *Big Brother's Little Helpers: How ChoicePoint and Other Data Brokers Collect and Package Your Data For Law Enforcement*,[3] collects and summarizes older activity.

In 2008, the data broker ChoicePoint that was a primary subject of Hoofnagle's work was acquired by Reed Elsevier for more than $3 billion.[4] ChoicePoint is now part of LexisNexis, a very large commercial data broker that is part of the Reed Elsevier conglomerate. The federal government is a significant customer of LexisNexis. On its website, LexisNexis says that "70 percent of local agencies and almost 80 percent of the Federal government use LexisNexis."[5]

---

[1] This report relies on Federal Trade Commission definition of data broker found in its report, *Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission Report, p. 68, March 2012. "Data brokers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud." http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[2] See generally, Robert O'Harrow, Jr., No Place to Hide (2005).

[3] Hoofnagle, Chris Jay, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement*, 29 N.C.J. Int'l L. & Com. Reg 595 (2003), available at SSRN, http://ssrn.com/abstract=582302.

[4] The deal was announced in February 2008, and closed 2008. See New York Times, *Reed Elsevier to acquire ChoicePoint for $3.6 billion*, (Feb. 21, 2008), http://www.nytimes.com/2008/02/21/technology/21iht-reed.4.10279549.html?_r=0. See also LexisNexis 2008 Annual Report ("On 19 September 2008, Reed Elsevier acquired ChoicePoint, Inc. ChoicePoint has merged with the LexisNexis Risk Information and Analytics Group, creating a risk management business with approximately US$1.4bn revenues. ChoicePoint's principal operating groups are Insurance Services, Screening, Business Services and Government Services."). http://www.reedelsevier.com/annualreport08/business/Pages/lexis-nexis.aspx.

[5] http://www.lexisnexis.com/risk/about/.

One LexisNexis product, the Accurint for Law Enforcement database, is used by over 4,000 federal, state, and local law enforcement agencies across the country.[6]

Recently the company announced a new service to help law enforcement officers monitor social media. The service debuted Oct. 19, 2013. "Social Media Monitor, a new capability in the LexisNexis Accurint® for Law Enforcement platform that is powered by the technology of DigitalStakeout®, allows agencies to discover risks and threats by leveraging social media to provide actionable intelligence."[7] LexisNexis describes in one of its federal agency case studies for its public records service[8] that its service was used to "[l]ocate missing or hard-to-find people and track ownership of assets." [9] The study noted the agency subscribed to LexisNexis Public Records because it "provided ability to look across all 50 states with one search. The company noted in a release that: "Our government solutions allow law enforcement and government agencies to derive insight from complex data sets, improve operational efficiencies, make timely and informed decisions to enhance investigations, increase program integrity, and discover and recover revenue."[10]

This report does not address the value or quality of these commercial databases or does this report assess necessary outsourcing of some database activities by the federal government. It is the privacy consequences of outsourcing that are the subject of this report. The OMB Do Not Pay Initiative properly asks whether information in commercial databases is sufficiently respectful of privacy so that government use of the information is appropriate.

The first real test of this question is likely to come because the US Treasury is currently testing The Work Number as part of a pilot program for the government's Do Not Pay Initiative.[11] The Work Number has been controversial for the scope of its payroll information and its lack of transparency, with one critic saying it was like a secret CIA.[12] The Work Number collects employment and salary information on Americans, and a lot of them. According to a company news release, "[t]he database includes more than 50 million current payroll records, updated each pay period to provide the most up-to-date information to lenders."[13]

---

[6] "Accurint for Law Enforcement is a proven and effective tool already used by over 4,000 federal, state and local law enforcement agencies across the country," http://www.lexisnexis.com/risk/downloads/casestudy/realcrimesrealresults.pdf.

[7] http://www.lexisnexis.com/risk/newsevents/press-release.aspx?Id=1381851197735305.

[8] http://www.lexisnexis.com/en-us/products/public-records.page.

[9] http://www.techvalidate.com/product-research/lexisnexis-research-and-litigation-solutions/case-studies/982-D1F-754.

[10] http://www.lexisnexis.com/risk/newsevents/press-release.aspx?Id=1314881279715051 .

[11] See https://smartpay.gsa.gov/cardholders/smartpay-charge-cards/purchase-card/do-not-pay and https://www.theworknumber.com/SocialServices/News/newsletters/vol2_2012/federal-do-not-pay-program.asp.

[12] Bob Sullivan, NBC News, The Red Tape Chronicles, *Your employer may share your salary, and Equifax might sell that data* (Jan. 30, 2013), http://www.nbcnews.com/technology/exclusive-your-employer-may-share-your-salary-equifax-might-sell-1B8173066. See also Jeff Gelles, *Credit-reporting companies know more than they tell you*, Philadelphia Inquirer (Feb. 4, 2013), http://articles.philly.com/2013-02-04/business/36723466_1_credit-reports-free-reports-credit-reporting-system.

[13] PR Newswire, *The Work Number and DealerTrack Partner to Provide Automated Employment and Income Verification to the Auto Finance Industry* (March 9, 2011). http://www.reuters.com/article/2011/03/09/idUS134583+09-Mar-2011+PRN20110309.

In some cases, the reporting of payroll and information is mandatory for employees, but some employers obtain consent before sending employee information sent to The Work Number.[14]

The Work Number is part of Equifax, one of the leading credit bureaus. The Work Number database is said to contain information on more than 190 million Americans,[15] with as many as 12 million added each year. Information from The Work Number is sold to debt collectors, financial service companies, and other entities. Equifax says that employment verification information (that is, *where* you work, but not specific pay information) is only sold to debt collectors with consent, as required by the Fair Credit Reporting Act.[16]

The Privacy Rights Clearinghouse has raised issues relating to the accuracy of the information in The Work Number.[17] There does not appear to be any public information on the accuracy of the database, and that will be an important issue if the database is to be accepted for permanent use in the Do Not Pay Initiative. There is ample reason to be concerned about the accuracy of commercial databases. In 2013 at the conclusion of its national, Congressionally-mandated national study of credit report accuracy,[18] the Federal Trade Commission found that 21% of consumers had verified errors in their credit reports, 13% had errors that affected their credit scores, and 5% had errors that were serious enough to be denied or to pay more for credit. It remains to be seen whether The Work Number has error rates that high and whether those rates would meet OMB's standard of *sufficient accuracy to assure fairness to data subjects*.

One reason the OMB memo is so welcome is that it provides an opportunity for an inquiry about the accuracy of commercial data brokers and databases that the government uses. This a subject rarely debated because the data broker companies generally are not compelled to supply accuracy information in this way.

Government Reliance on Commercial Databases has Few Legal Limits

There are few legal or regulatory constraints on the government's use of commercial data sources about individuals. Commercial database owners are largely unregulated for privacy, and they are generally free to sell information as they please with little regard for accuracy, currency, completeness, or fairness. Individual consumers may or may not have a practical remedy when

---

[14] See, e.g., http://www.hr.emory.edu/eu/docs/talx-guide.pdf and http://www.gcu.edu/Documents/upload/Faculty%20and%20Staff/Employment%20Verification%20FAQs.pdf.

[15] The Work Number, Commercial Verifiers Page, "The Work Number is a service that organizations can use to verify employment and income information. The more than 190 million records on The Work Number database are provided to us by over 2,000 employers and are updated on a regular basis." http://acceptance.theworknumber.com/Verifiers/Help/faq.asp?category=general.

[16] See Kashmir Hill. *Sadly, It's Not Actually This Easy To Find Out How Much Money Someone Makes,* Forbes (Feb. 4, 2013), http://www.forbes.com/sites/kashmirhill/2013/02/04/equifax-the-work-number/.

[17] See https://www.privacyrights.org/ar/WorkNumber.htm.

[18] Federal Trade Commission, *Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003* (2012), http://ftc.gov/os/2013/02/130211factareport.pdf.

commercial databases include personal information that is wrong, untimely, incomplete, or unfair. Consumer legal remedies are difficult at best and impossible at worst unless a statute like the Fair Credit Reporting Act[19] provides a specific remedy, such as the ability to access and correct a file. When a person has a data problem and it does not come with a legal remedy, these are the anecdotes where people describe spending years trying to clean up their files. In some extreme cases, people are forced to prove their identity in novel ways such as x-rays, or they must travel with documents proving their identity due to these kinds of entrenched errors.[20]

The key privacy law that defines how the US government may process most records about individuals is the Privacy Act of 1974. The Act has its own shortcomings, but that is a topic for another day. It imposes some useful privacy limits on federal government activities involving personal information, and more importantly, it gives privacy rights to individuals. Federal agencies have long evaded the privacy standards in the Privacy Act of 1974 by using information from commercial databases that do not meet the standards of the Act.[21] The new OMB Do Not Pay policy takes useful steps in the direction of limiting that type of abuse.

How The Do Not Pay Initiative Affects Data Brokers

The Do Not Pay Initiative and the resulting OMB memo about how to handle the privacy of databases used in the initiative is an important part of debate about data brokers and the privacy policies that they do -- or should -- follow.

The OMB memo requires agencies involved in the Do Not Pay Initiative to apply privacy standards for evaluating the use of commercial databases with personal information.[22] The standards themselves are not new. They are the same standards that federal agencies have compiled with for the nearly forty years that the Privacy Act of 1974 has been in place. What is new is that the standards will **apply externally to commercial services and databases provided to the government and not just internally to government activities or information that the government maintains**.

---

[19] 15 U.S.C. § 1681 et seq. The FCRA regulates consumer reporting agencies ("credit bureaus"), but credit reporting is a narrow part of the commercial database world. Those companies regulated under the FCRA typically offer numerous unregulated databases to government and commercial companies.

[20] Many of these case studies have been documented over the years. See generally the Identity Theft Resource Center, http://www.idtheftcenter.org/, and the Privacy Rights Clearinghouse, https://www.privacyrights.org/. See also the medical identity theft reporting of the World Privacy Forum for the documentation of identity and medical information, http://worldprivacyforum.org/category/med-id-theft.

[21] Agencies do this by consulting commercial database and by avoiding including information in a Privacy Act system of records subject to privacy standards.

[22] DNP relies on five existing federal databases, which are described below. These databases are subject to existing privacy rules applicable to the federal government when those laws apply.

The Do Not Pay Initiative seeks to curb waste and fraud in the federal government by limiting, reviewing, and verifying information to identify inappropriate federal agency payments.[23] Excluded from this Initiative are regularly occurring salary payments for members of the military. Also excluded are benefits to employees such as those enrolled in FEDVIP or long-term care.[24] Even with these exclusions, though, the mandate of the Initiative is broad.

To facilitate the review and verification process, the Initiative uses two newly-built online portals to centralize and disseminate information. This report focuses on one of them, the Do Not Pay Portal.[25]

The **Do Not Pay Portal** is a centralized website where government agencies can seek to verify or determine eligibility of individuals for receiving government payments. Determining which individuals are ineligible for payments requires a great deal of personal and sensitive information. The portal seeks to use external sources because the US government does not always have the necessary information in its own files. The US Treasury describes the "Do Not Pay Business Center [as a location that] provides many data sources – in one place - that your agency can review to verify eligibility."[26]

This is OMB's description of the Do Not Pay Initiative:

> In response to the President's June 2010 directive, the federal government has worked aggressively to develop tools that will enable the centralized, detailed review of relevant databases envisioned as part of the "Do Not Pay List." As a first step, agencies reviewed internal controls and processes surrounding its existing pre-payment and pre-award procedures and databases monitored pursuant to those procedures. Building on these reviews, OMB and the Department of the Treasury (Treasury) have established the Do Not Pay solution, available for use by all agencies. The Do Not Pay solution is comprised of two components geared toward reducing improper payments:
>
> > A web-based, single-entry access portal that enables agencies to access the data sources identified in the June 2010 Memorandum (including the Death Master File, the Excluded Parties List System, Treasury's Debt Check Database, and the List of Excluded Individuals and Entities). In addition, Treasury will continue to add other high-value data sources to the portal.

---

[23] The Do Not Pay Initiative will also affect businesses and other legal persons. However, because this report focuses on privacy and because only individuals have privacy rights, the consequences for legal persons of the Do Not Pay Initiative are not under review. We note, however, that better quality records benefit all data subjects, whether they are individuals with privacy rights or not.

[24] Do Not Pay Webinar Questions, April 2012, p. 5. http://donotpay.treas.gov/DoNotPayWebinarQuestionsApril2012.pdf.

[25] The Do Not Pay Program also includes a website called PaymentAccuracy.gov, which we do not cover in this report. This website publishes general information about improper payments made regarding certain high-risk government programs. The PaymentAccuracy.gov website also allows the public to report suspected fraud, waste, and abuse.

[26] Do Not Pay Portal, http://donotpay.treas.gov.

> Data Analytics Services that utilize additional data sources which are not available through the Portal. These include Treasury's Office of Foreign Assets Control List, zip code data, prison information, and several privately available sources. The sources are augmented by advanced data analytic activities for identifying trends, risks, and patterns of behavior that may warrant further review by the agency. [27]

Of particular note are Treasury plans to add other data sources to the portal. It in fact, has already done so.

Current Databases Used in the Do Not Pay Initiative

The Treasury Do Not Pay Portal launched in April 2012. As of 2013, it uses an array of databases, some for vetting vendors, some for checking on individuals. The focus of this report is on how the Initiative affects individuals.

According to the Department of the Treasury, the Do Not Pay portal uses information compiled from the following databases to determine payment eligibility, including of individuals:

> **Excluded Party List System (EPLS)**
>
> Identifies parties excluded from receiving Federal contracts, certain subcontracts, and certain types of Federal financial and nonfinancial assistance and benefits (Examples include:
>
> Verifies whether an individual that is receiving unemployment payments is still living, owes federal non-tax debt, and/or is recently employed;
>
> Identifies providers, individuals, or vendors that are excluded from doing further business with the government or should be subject to more oversight based on past performance; and
>
> Identifies keying errors that could cause the wrong entity to receive a payment
>
> Keeps the Federal purchasing community aware of administrative and statutory exclusions across the entire government, suspected terrorists, and individuals barred from entering the United States.
>
> **Death Master File (DMF)**
>
> Verifies whether an individual that is receiving unemployment payments is still living,

[27]Office of Management and Budget, *Reducing Improper Payments through the "Do Not Pay List*" (April 122, 2012) (OMB M-12-11). https://smartpay.gsa.gov/sites/default/files/wysiwyg/OMB%20Memo%20on%20Do%20Not%20Pay%20List.pdf.

owes federal non-tax debt, and/or is recently employed.

List of Excluded Individuals/Entities (LEIE)

Verifies whether an individual that is receiving unemployment payments is still living, owes federal non-tax debt, and/or is recently employed

Identifies providers, individuals, or vendors that are excluded from doing further business with the government or should be subject to more oversight based on past performance

Debt Check

Verifies whether an individual that is receiving unemployment payments is still living, owes federal non-tax debt, and/or is recently employed

Identifies vendors that owe federal non-tax debt and ensure vendors that owe debts are paid via the Treasury offset process instead of through a credit card.

Central Contractor Registration (CCR)

Identifies providers, individuals, or vendors that are excluded from doing further business with the government or should be subject to more oversight based on past performance

During the payment process, ensures that the name associated with the DUNS is the name associated with that DUNS in CCR, thus preventing payment to the wrong entity

Identifies keying errors that could cause the wrong entity to receive a payment

The Work Number

Verifies whether an individual that is receiving unemployment payments is still living, owes federal non-tax debt, and/or is recently employed for agency programs that are means tested

Verifies the accuracy of income levels at the time of enrollment

Office of Foreign Assets Control (OFAC) feed

The Work Number is a commercial database that has received a great deal of critical attention. According to the User Guide for the Do Not Pay portal, "The Work Number is the leading provider of employment and income verifications; the data provided could help you determine eligibility for certain government programs."[28]

[28] Do Not Pay Portal User Guide DNP User Guide R 1.3.0.1 v4 at p. 19, http://donotpay.treas.gov/Do%20Not%20Pay%20User%20Guide.pdf.

The OMB rules that will determine whether The Work Number meets privacy standards are discussed in detail below. The Treasury Department and other participants in the Initiative must follow the new OMB rules for The Work Number database, including providing public notice and the opportunity for public comment. How Treasury handles its use of The Work Number will be the first test of the sincerity and viability of the new OMB privacy guidance. One of the key recommendations in this report is how notice and comment for The Work Number should be accomplished.

II. Discussion and Analysis of the OMB Do Not Pay Guidance

The best starting point for understanding the OMB Do Not Pay memo is with the legal framework behind the Do Not Pay Initiative. The Initiative derives from a combination of little-noticed executive orders and updates to existing laws.

In 2009, Executive Order 13520, *Reducing Improper Payments,*[29] directed agencies to identify "ways in which information sharing may improve eligibility verification and pre-payment scrutiny." This was the start of the current Do Not Pay Initiative.

In 2012, Congress followed the 2009 Executive Order up with additional legislation, The Improper Payments Elimination and Recovery Improvement Act of 2012,[30] or IPERIA. IPERIA amends an earlier law, the Improper Payments Information Act of 2002.[31] The important thing about IPERIA is that it gave OMB additional authority to allow the use of new databases for the Do Not Pay Initiative. IPERIA also authorized OMB, acting to implement the law, to issue guidance in the application of the law. On August 16, 2013, OMB issued the memo – the main subject of this report – to agencies with instructions on how to implement Do Not Pay Initiative. The OMB memo has the interesting title *Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative*.[32]

The OMB Do Not Pay memo provides for expanded use of commercial data brokers by federal agencies and, most importantly for present purposes, it establishes new privacy standards for the databases used in the Do Not Pay Initiative. Its extension of privacy standards to commercial databases purchases by the federal government is groundbreaking.

As discussed, the Do Not Pay List that will be a single point of entry for agencies to access data to determine eligibility for a federal award or payment went live in April, 2012.

---

[29] http://www.whitehouse.gov/sites/default/files/omb/assets/financial_improper/11202009_improper_payments.pdf (Nov. 20, 2009).
[30] Pub. L. No. 112-248, 126 Stat. 2390 (2012), http://www.gpo.gov/fdsys/pkg/PLAW-112publ248/html/PLAW-112publ248.htm.
[31] 31 U.S.C. 3321 note.
[32] OMB Memorandum M-13-20, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-20.pdf (2013).

Analysis of The Do Not Pay Memorandum

The new OMB Do Not Pay memorandum is long and complex. In essence, the memo seeks to use the federal government's marketplace power to set privacy standards for private sector information services that affect individual rights, at least for services that the federal government purchases.
Among other things, it includes detailed instructions telling agencies how to comply with the computer matching provisions in the Privacy Act of 1974.

OMB's instructions about how to carry out Do Not Pay activities while complying with computer matching requirements include requirements for due process that ensure verification, notice, and opportunity to contest adverse information. Those details, while extremely important otherwise, are not of immediate interest here. Our focus in this analysis is on the privacy requirements OMB set for commercial databases. However, we observe that due process procedures are essential whenever the government considers any action that affects the rights, benefits, or privileges of individuals. We are pleased to see appropriate due process procedures included in the Do Not Pay Initiative as required by law.

DNP Databases and Requirements for Databases

The Do Not Pay Initiative directs agencies to have prepayment and pre-award procedures and to ensure that a thorough review of available databases with relevant information on eligibility occurs. The goal is to determine program or award eligibility and to prevent improper payments before the release of any Federal funds.

Under the 2012 legislation, agencies are generally required to review five existing federal databases prior to payment.

These **2012** databases are:

- Death Master File of the Social Security Administration.
- General Services Administration's Excluded Parties List System.
- Debt Check Database of the Department of the Treasury.
- Credit Alert System or Credit Alert Interactive Voice Response System of HUD
- List of Excluded Individuals/Entities of the Office of Inspector General of HHS.[33]

The Do Not Pay Initiative also provides for the use of other databases "designated by the Director of the Office of Management and Budget in consultation with agencies and in accordance with paragraph (2)."[34] This is an important distinction.

[33] Pub. L. No. 112-248 § 3(a), amending § 5(a)(2) of the Improper Payments Information Act of 2002, 31 U.S.C. 3321 note.
[34] OMB Memorandum M-13-20 at § 5(b)(1)(B).

The current **2013** list, as found on the Treasury Do Not Pay portal as of October 27, 2013, includes all of the 2012 databases and adds the OFAC database and importantly, The Work Number.

Unlike the other databases mentioned on the site, this is not a database that originates with the federal government, therefore, it will be the first database subject to the new OMB guidance for commercial databases.

Paragraph (2) of the OMB memo requires the Director of OMB to consider any database that substantially assists in preventing improper payments and to provide public notice and an opportunity for comments before designating another database for use in the Do Not Pay Initiative.[35] This has not yet been done yet for The Work Number because it is still a pilot program.

OMB's New Standards and Procedures for Evaluating New Databases

OMB established standards and procedures for evaluating new commercial databases for the Do Not Pay Initiative.

> Before designating additional databases, OMB will publish a 30-day notice of the designation proposal in the Federal Register asking for public comment. At the conclusion of the 30-day comment period, if OMB decides to finalize the designation, OMB will publish a notice in the Federal Register to officially designate the database for inclusion in the Do Not Pay Initiative. When considering additional databases for designation, OMB will consider:
>
> 1. Statutory or other limitations on the use and sharing of specific data;
> 2. Privacy restrictions and risks associated with specific data;
> 3. Likelihood that the data will strengthen program integrity across programs and agencies;
> 4. Benefits of streamlining access to the data through the central Do Not Pay Initiative;
> 5. Costs associated with expanding or centralizing access, including modifications needed to system interfaces or other capabilities in order to make data accessible; and
> 6. Other policy and stakeholder considerations, as appropriate.[36]

Asking for public comments before using a new database for a governmental purpose is a positive step and both welcome and appropriate, but it is not entirely new. The Privacy Act of 1974 requires federal agencies to publish in the Federal Register a notice when it establishes or changes a system of records.[37] Agencies generally accept and consider public comments, and

[35] Id. at § 5(b)(2).
[36] OMB Memorandum M-13-20 at § 5(b).
[37] 5 U.S.C. § 552a(e)(4).

they must do so when proposing or changing a routine use that allows disclosure of personal information.[38] For some privacy affecting activities, agencies must sometimes prepare and publish privacy impact assessments (PIA).[39] Some agencies accept public comments on PIAs.

OMB's establishment of express standards for making decisions about using new databases appears to be completely new, and it is the first truly groundbreaking aspect of database evaluation in the Do Not Pay Initiative. Neither the Privacy Act of 1974 nor the PIA process requires anything comparable. In addition, OMB itself must officially designate any new databases for Do Not Pay purposes, a step that should prevent poorly-considered undertakings that might occur in the absence of adequate supervision and oversight.[40]

The first of the OMB standards recognizes that existing law may make a database unavailable for Do Not Pay. The third, fourth, and fifth standards cover the value, benefits, and costs associated with using a database. These standards are familiar ground for OMB, and the standards are welcome but are mostly unremarkable.

The second and sixth standards are more creative. The second standard requires consideration of privacy restrictions and risks. This suggests not only that that privacy concerns are relevant to evaluation of a database but also that privacy concern could possibly overcome other factors. The sixth standard calls for other policy and stakeholder considerations. While this standard may not be quite as important for privacy as the second standard, its open-ended invitation for evaluating other policy and stakeholder considerations suggests that other factors and other voices deserve the chance to affect decisions about databases. These are good steps toward a fair evaluation of new personal information resources in federal programs.

The standards and procedures described so far apply to any new databases proposed for use in Do Not Pay. This includes any federally operated databases. OMB's setting of standards for internal government activities is not unusual. Indeed the five designated databases already approved for Do Not Pay are all federally operated.

Elsewhere in the memo, OMB expressly addresses the possibility of using *commercial* databases in the Do Not Pay Initiative, something that the 2012 law allows (but does not require).[41] It is here where OMB's requirements for the use of commercial databases are where the innovations are truly groundbreaking.[42] OMB recognizes the privacy consequences of commercial databases

---

[38] Id. at § (e)(11).

[39] E-Government Act of 2002, Pub. L. No. 107-347, 44 U.S.C. § 3501 note ("if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." §208(b)(1)(B)(iii).
OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, http://www.whitehouse.gov/omb/memoranda_m03-22 (2003).

[40] OMB Memorandum M-13-20 at § 5(b).

[41] Public Law 112-248, § 5(d)(2)(C). OMB Memorandum M-13-20 at § 11.

[42] There is a vague precedent in the PIA requirements. One of the reasons for conducting a PIA is "when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement)". OMB Memorandum M-03-22, Attachment A at § II.B(2)(f). The DNP Initiative's requirements go much further.

that contain inaccurate or out-of-date information.[43] OMB requires public notice and comment before use of any proposed commercial database. OMB establishes standards that commercial databases must meet.[44] OMB must approve before the Treasury Department can use of a commercial database. This is how OMB explains the new standards:

> Because commercial databases used or accessed for purposes of the Do Not Pay Initiative will be used to help agencies make determinations about individuals, it is important that agencies apply safeguards that are similarly rigorous to those that apply to systems of records under the Privacy Act. Thus, commercial data may only be used or accessed for the Do Not Pay Initiative when the commercial data in question would meet the following general standards:
>
> 1. Information in commercial databases must be relevant and necessary to meet the objectives described in section 5 of IPERIA.
>
> 2. Information in commercial databases must be sufficiently accurate, up-to-date, relevant, and complete to ensure fairness to the individual record subjects.
>
> 3. Information in commercial databases must not contain information that describes how any individual exercises rights guaranteed by the First Amendment, unless use of the data is expressly authorized by statute.[45]

It is commendable that OMB establishes standards that commercial databases must meet in order to be used by federal agencies in the Do Not Pay Initiative. It is useful if not so extraordinary that the databases must be relevant and necessary to the goals of the Initiative.[46] Other OMB standards are more interesting and more privacy-protective.

Commercial database standards: accurate, up-to-date, relevant, complete

A database used for the Do Not Pay Initiative must be sufficiently accurate, up-to-date, relevant, and complete to ensure fairness to data subjects.[47] These standards for federal use of a commercial database appear to break new ground in several ways. First, the OMB standards are better than those required under the Fair Credit Reporting Act, a law that regulates credit bureaus. The FCRA only requires "reasonable procedures to assume maximum possible

[43] OMB Memorandum M-13-20 at § 11(a).
[44] Id. at § 11(b).
[45] Id. at § 11(b).
[46] The Privacy Act of 1974, a law applicable only to federal agencies, has similar but slightly stronger language. Each agency must "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." 5 U.S.C. § 552a(e)(1).
[47] The Privacy Act of 1974 has slightly stronger language. Each agency must "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C. § 552a(e)(5).

accuracy."[48] The Do Not Pay requirements address accuracy (albeit only sufficient accuracy) and then adds currency, relevance, and completeness, all with an express goal of ensuring fairness to data subjects.

First Amendment limitation

Second, the OMB standards require that a commercial database provided to a federal agency must not contain information that describes how any individual exercises First Amendment rights (except if expressly authorized by statute). Heretofore, that First Amendment limitation only applied to federal agency records.[49]

Written assessment to document suitability and public notice

Third, OMB requires that the Treasury Department prepare and submit to OMB a written assessment to document the suitability of the commercial database for use in Treasury's Working System. The assessment must explain the need to use or access the data, explain how the data will be used or accessed, provide a description of the data (including each data element that will be used or accessed), and explain how the database meets all applicable requirements in this Memorandum.

Just as important, OMB will provide the written assessment to the public as part of the public comment period. This will oblige any commercial database to demonstrate how it meets the standards and will allow the public a better opportunity to review and comment on the information.[50]

Any commercial database that wants to provide information for federal agencies to use in the Do Not Pay Initiative must meet new and meaningful privacy standards. The agency responsible for central Do Not Pay activities, the Treasury Department, will be unable to incorporate the contents of a commercial database that fails to meet the standards, and there will be an opportunity for public comment and for federal review of the degree to which a commercial database qualifies. In this area, the federal government will not be able to purchase and use a commercial database without regard to the quality and content of the database.

The OMB standards are innovative, creative, and welcome. What the OMB Do Not Pay Memorandum shows is that the federal government may have considerable marketplace power to influence privacy standards for commercial databases. If federal dollars are only used to purchase commercial databases that meet reasonable privacy standards, commercial databases

[48] 15 U.S.C. §1681e(b). Presumably, if agencies use credit reports for the DNP Initiative, there must be a determination that the reports meet the higher standards in the OMB Memorandum.

[49] This language also echoes a requirement in the Privacy Act of 1974 that prohibits the maintenance of a record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the data subject or unless within the scope of an authorized law enforcement activity. 5 U.S.C. § 552a(e)(7).

[50] OMB Memorandum M-13-20 at § 11(d) & 5(b).

will have a powerful incentive to clean up their acts. The federal government can, if it chooses, use its market power to improve the quality and fairness of privately-owned databases, and it can do so without the need for legislation. Nothing in IPERIA expressly requires OMB to set privacy standards for commercial databases. OMB chose to do so on its own, and for this, OMB deserves much praise.[51]

Limitations

However, the OMB standards do not affect commercial databases made available to customers other than federal agencies. For example, if a database contains prohibited information about First Amendment rights, the database owner can strip out the prohibited information, create a subset of the database for federal consumption, and continue to maintain and sell that information otherwise. Commercial databases can continue to be sold to other customers without meeting any standards for accuracy, currency, relevance, or completeness. However, if database vendors improve the accuracy or currency of data to meet the federal standards, that may result in better quality data for other users as well, and that that would benefit data subjects and data users alike. In effect, any rising tide of accuracy or currency will affect all boats.

Pilot program

Somewhat less welcome is another provision that allows for the use of commercial databases as part of a pilot program that need not satisfy the privacy or other standards set out by OMB. Pilot programs are limited to six months, and they cannot be used to take any adverse action against an individual.[52] The prohibition against adverse actions balances the loosening of standards allowed for pilot programs. Any commercial database actually used for the Do Not Pay Initiative will have to meet the required privacy standards. How the Treasury will evaluate its use of The Work Number in the Do Not Pay Portal will be a major test of the effectiveness of the OMB guidance.

Congress could always pass laws setting privacy standards for commercial databases with information about individual, but there is no evidence that Congress will act any time soon.

---

[51] Several additional requirements pertaining to the use of commercial databases by federal agencies are also welcome although familiar. The Treasury Department is obliged to establish rules of conduct for persons involved in the use of or access to commercial databases. Training and penalties for noncompliance are also required, as appropriate. OMB Memorandum M-13-20 at § 11(c)(1). These requirements are similar to existing provisions in the Privacy Act of 1974 that require "appropriate administrative, technical, and physical safeguards." 5 U.S.C. § 552a(e)(10). Treasury must also establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of information in commercial databases when Treasury controls the information. OMB Memorandum M-13-20 at § 11(c)(2). These requirements are similar to existing provisions in the Privacy Act of 1974 that require "appropriate administrative, technical, and physical safeguards." 5 U.S.C. § 552a(e)(10). Additionally, in the memorandum, OMB reminds agencies that information in commercial databases used in the DNP Initiative may constitute a system of records or become part of a system of records and would therefore be subject to all Privacy Act requirements. It is important that any information used use in making a decision become part of a system of record so that individuals have an opportunity to see and challenge the information. OMB Memorandum M-13-20 at § 11(f). These provisions are not novel, but the repetition is welcome nevertheless.

[52] Id. at § 11(e).

Overall, the privacy standards for commercial databases that OMB establishes in its Do Not Pay Memorandum are a wonderful precedent. The standards should be considered a first step.

Application of the OMB Standards to the Do Not Pay Portal

The Do Not Pay Portal uses The Work Number in a pilot program. Under the OMB Guidelines, before The Work Number can be fully incorporated into the Do Not Pay Initiative, there must be an opportunity for public notice and comment. How the evaluation is done will say much about whether the process will be meaningful and how the new standards will be applied in practice.

Under the OMB guidance, it appears that the Treasury has a six-month window to use The Work Number without notice, if the database is being used as part of a pilot program. The OMB Guidance took effect as of August 2013, suggesting that of the date of the initial release of this report, Treasury has approximately three months before providing public notice and comment.[53]

If the OMB Guidance is followed, the following things will happen before The Work Number can become a permanent part of the Do Not Pay Initiative:

- The Treasury Department must prepare and submit to OMB a written assessment to document the suitability of the commercial database for use in Treasury's Working System. The assessment must explain the need to use or access the data, explain how the data will be used or accessed, provide a description of the data (including each data element that will be used or accessed), and explain how the database meets all applicable requirements.

- OMB will make the Treasury Department's assessment available to the public.

- OMB will provide formal public notice about the proposed use of The Work Number.

- The public will have an opportunity to comment on the proposed use of The Work Number.

- OMB will take the comments of the public into account in its decision regarding the use of the database.

[53] The Treasury posted a notice in the Federal Register in February 2012, just prior to launching the portal. The notice changed a government System of Records. This change in an existing system of records is obviously not the public notice and comment required by the OMB DNP Memo.
https://www.federalregister.gov/articles/2012/02/15/2012-3459/privacy-act-of-1974-as-amended-systems-of-records.

III. Recommendations

Recommendations for the Office of Management and Budget:

- OMB should establish privacy standards that are at least a good as those in and recommended for the Do Not Pay Initiative to cover ***all government purchases of commercial databases with personal information.*** OMB should consider accomplishing an expansion by establishing a task force that includes representatives of consumer and privacy groups.

- In the near future, OMB should expand the privacy standards for the Do Not Pay Initiative to require that commercial databases comply fully with all Fair Information Practices, including collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, access and correction rights, and accountability.[54] It is especially important that data subjects have meaningful, timely, and effective access and correction rights to any commercial databases used by federal agencies. OMB should take steps to expand the privacy standards at the earliest possible opportunity following a reasonable test of the new Do Not Pay procedures.

- Because The Work Number will be the first test of a pilot project under the Do Not Pay Initiative, OMB should ensure that it provides for ample and prominent notice and public comment opportunity if it proposes permanent adoption of The Work Number. This is essential so that there will be a fair test of the effectiveness of public oversight of the new private sector database standards. Public notice should include extensive documentation about the accuracy, timeliness, relevance, and completeness of The Work Number. An independent audit of The Work Number's compliance with data standards would be especially useful. In addition, all of the data fields maintained by The Work Number must be published to allow an evaluation whether any of the data reflects on the exercise of First Amendment rights.

- According to the OMB FAQ on the Initiative, Treasury is considering inclusion of state-level data.[55] Before expanding the Initiative to state data, OMB should apply to state databases the same privacy standards and procedures that the Do Not Pay memo applies to commercial databases.

---

[54] For a history of Fair Information Practices, see Robert Gellman, Fair Information Practices: A Basic History, at http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

[55] Treasury Department, April 2012 Webinar Questions at 2 (Is there a possibility for Do Not Pay to obtain state data?), http://donotpay.treas.gov/DoNotPayWebinarQuestionsApril2012.pdf.

Recommendations for the States:

- The states also use commercial data sources and have market power. Each state should follow the example policies established by OMB and require that any commercial databases containing personal information used for state activities meet privacy standards consistent with Fair Information Practices. Standards for state purchases might be established using executive rather than legislative authority. Governors or State Attorneys General might consider establishing uniform standards here so that all states impose the same standards.

Recommendations for Congress:

- Congress should request that the Government Accountability Office review the implementation of the OMB Do Not Pay Initiative to make sure that the privacy standards are fairly implemented.

- If Congress is unwilling to legislate broadly applicable privacy standards consistent with Fair Information Practices for commercial databases containing personal information, Congress should nevertheless encourage, authorize, or direct OMB to establish standards for all government purchases of commercial databases containing personal information.

Recommendation for the Federal Trade Commission:

- The Federal Trade Commission has long had the ability to determine that the failure of a commercial database containing personal information to meet Fair Information Practices is an unfair trade practice. The Commission has not yet taken any meaningful step in that direction. Nevertheless, any partial action by the FTC toward the goal of broader implementation of Fair Information Practices would still be welcome.

Recommendation for the public, including consumer and privacy groups:

- The public as well as and consumer and privacy groups should closely monitor the Do Not Pay Initiative and should actively participate in any opportunity for public comment about the use of commercial databases.

IV. Conclusion

OMB deserves much praise for this novel privacy initiative, but it has more work to do. The evaluation of the first private sector database in the Do Not Pay Initiative needs to be accomplished in the open with full participation by all interested parties. The OMB memo provides for that. We need to see how well that process works.

There is more to be done elsewhere. The OMB privacy standards for the Do Not Pay initiative could usefully be expanded to include all Fair Information Practices, rather than just some. Individuals need a practical and available process to find and fix records that are wrong. That need is the same whether the records are maintained by the government or by the private sector.

The standards for the Do Not Pay Initiative should also be extended to cover *all* government use of commercial data brokers, including in law enforcement. The federal government should broadly use its marketplace power to improve privacy and improve databases. Regulation is not the only way to achieve a better result. Individuals need the same rights and protections whenever the government uses commercial databases.

If the privacy protections OMB established are effective, it will be an important step forward. At least in the Do Not Pay Initiative, people would have more ability to challenge the information coming from databases such as The Work Number and get redress from problems. If the protections were then to be taken up widely across the federal government and by state governments, the result could be better quality commercial databases for use by governments and by others. There would be fewer errors, less fraud, less government waste, more redress for individuals, and a higher overall standard of modern fair information practices would be set.

Data brokers, data users, and data subjects benefit when databases become more accurate, timely, relevant, and complete. Privacy isn't just about individuals. Everyone gains when privacy protections result in better records.

The Do Not Pay Initiative demonstrates that there is no need to wait for legislation to find creative ways to extend privacy standards to the commercial sector. The World Privacy Forum hopes that it is a first step in using executive authority to implement additional privacy protective actions and norms.

Appendix A: Chronology of Do Not Pay

Chronology of the Do Not Pay Initiative

Aug. 16, 2013: Office of Management and Budget issues memorandum M-13-20 instructing agencies how to comply with the Improper Payments Elimination and Recovery Improvement Act.

January 10, 2013: The President signs Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA) into law. IPERIA enhances the Administration's efforts to combat improper payments. Consistent with existing protections for individual data privacy, the new law seeks to improve the determination of improper payments by agencies, improve recovery of improper payments, and reinforce and accelerate the President's "Do Not Pay" efforts."

April 12, 2012: OMB issues memorandum M-13-20 Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative.

April 12, 2012: Do Not Pay solution opens at the US Treasury
http://www.whitehouse.gov/blog/2012/04/12/do-not-pay-solution-open-business

June 18, 2010: Do Not Pay list established:
http://www.whitehouse.gov/sites/default/files/omb/assets/financial_improper/06232010_donotpaylist.pdf

Nov. 20, 2009: Executive Order launches the Do Not Pay Initiative issuing Executive Order 13520 of November 20, 2009 (Reducing Improper Payments), which established new measures to increase agency transparency and accountability.

Appendix B: Text of the OMB Do Not Pay Memo

Text of OMB Do Not Pay Memo:

Available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-20.pdf

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

August 16, 2013

M-13-20

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Sylvia M. Burwell
Director

SUBJECT: Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative

This Memorandum implements section 5 of the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA) [56] and provides guidance to help Federal agencies protect privacy while reducing improper payments with the Do Not Pay (DNP) Initiative.

In Executive Order 13520 of November 20, 2009 *(Reducing Improper Payments),* the President directed agencies to identify "ways in which information sharing may improve eligibility verification and pre-payment scrutiny."[57] To help agencies implement the Executive Order, the President issued memoranda on finding and recapturing improper payments [58] and enhancing payment accuracy through a "Do Not Pay List."[59] The President directed the establishment of a "single point of entry" through which agencies would access relevant data in order to determine eligibility for a Federal award or payment.

In April2012, OMB released a memorandum describing the efforts of OMB and the Department of

[56] Pub. L. No. 112-248, 126 Stat. 2390 (2013).

[57] 74 Fed. Reg. 62201 (Nov. 20, 2009), available at http://www.gpo.gov/fdsys/pkg/FR-2009-11-25/pdf/E9-28493.pdf.

[58] Memorandum of March 10, 2010, Finding and Recapturing Improper Payments, 75 Fed. Reg. 12119 (Mar. 10, 201 0), available at http://www.whitehouse.gov/sites/default/files/omb/assets/financial_improper/03102010_improper_payments.pdf.

[59] Memorandum of June 18, 2010, Enhancing Payment Accuracy Through a "Do Not Pay List," 75 Fed. Reg. 35953 (June 18, 201 0), available at http://www.whitehouse.gov/sites/default/files/omb/assets/financial_improper/06232010_donotpaylist.pdf.

the Treasury (Treasury) to establish the DNP Initiative.[60] The memorandum directed agencies to develop a plan for using the DNP Initiative for pre-payment eligibility reviews. In January 2013, the President signed IPERIA into law, codifying the ongoing efforts to develop and enhance the DNP Initiative. As the Federal Government takes these important steps to prevent waste, fraud, and abuse in Federal spending, it is vital for agencies to ensure that individual privacy is fully protected.

As required by IPERIA, this Memorandum sets forth implementation guidance for the DNP Initiative to help ensure that the Federal Government's efforts to reduce improper payments comply with privacy laws and policies.

1. Background

On January 10, 2013, the President signed IPERIA into law. Among other things, the law codified the Administration's DNP Initiative already underway across the Federal Government. The DNP Initiative includes multiple resources that are designed to help agencies confirm that the right recipient receives the right payment for the right reason at the right time. IPERIA provides the Federal Government with new tools and authorities to help agencies effectively implement the DNP Initiative.

Section 5(e)(3) of IPERIA requires OMB to issue guidance implementing the relevant parts of the law. In particular, the statute requires OMB to provide guidance to agencies on reimbursement of costs between agencies, retention and timely destruction of records, and prohibiting the duplication and redisclosure of records. Furthermore, under IPERIA, OMB must also provide guidance to help improve the effectiveness and responsiveness of agencies' Data Integrity Boards (DIBs). This Memorandum addresses all of these points and provides additional guidance on several other issues that are relevant to the DNP Initiative.

This Memorandum builds on previous OMB guidance. In 1988, Congress amended the Privacy Act of 1974 [61] to establish procedural safeguards for agencies' use of computer matching programs.[62] The following year, OMB issued guidance to help agencies interpret the law and meet the new requirements.[63] Since releasing the original computer matching guidance, OMB has issued additional guidance regarding computer matching.[64] This Memorandum supplements the existing OMB documents and provides new guidance to help agencies protect privacy while reducing improper payments with the DNP Initiative.

2. Scope and Applicability

---

[60] See OMB Memorandum M-12-11, Reducing Improper Payments through the "Do Not Pay List" (Apr. 12, 2012), available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-11_1.pdf.

[61] 5 U.S.C. § 552a.

[62] Computer Matching and Privacy Protection Act of 1988, Pub. L. No.l00-503, 102 Stat. 2507 (1988).

[63] Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818 (June 19, 1989), available at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/final_guidance_pl100-503.pdf.

[64] See OMB Memorandum M-0 1-05, Guidance on Inter-Agency Sharing of Personal Data-Protecting Personal Privacy (Dec. 20, 2000), available at http://www.whitehouse.gov/omb/memoranda mOI-05/; see also OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals, available at http://www.whitehouse.gov/omb/circulars_a130_a130trans4.

This Memorandum implements section 5 of IPERIA and applies to agencies' activities related to the DNP Initiative.[65] Some of the requirements in this Memorandum apply to all DNP Initiative activities (indicated by the term "DNP Initiative"), while other requirements are specific to Treasury's Working System (indicated by the term "Treasury's Working System"), as defined in section 3 of this Memorandum. As required by section 5(e)(3)(B) of IPERIA, this guidance also clarifies some issues regarding matching programs in general.[66]

Although this Memorandum creates new policy requirements, nothing in this document extends the legal requirements of the Privacy Act to information or activities that would not otherwise be covered under the statute.[67] Notably, IPERIA does not modify the definitions in the Privacy Act. For example, the matching requirements of the Privacy Act only apply to a "matching program," and only apply to a Federal benefit match if the match involves a "Federal benefit program," as defined in the statute. Agencies should consult with their counsel and senior agency official for privacy to determine whether an activity is covered by the requirements in the Privacy Act and the corresponding requirements in this Memorandum.

While IPERIA does not explicitly amend the definitions in the Privacy Act, it nonetheless changes how the Privacy Act applies for purposes of the DNP Initiative.[68] Specifically, IPERIA establishes new standards and procedures that apply to matching programs conducted exclusively for purposes of the DNP Initiative. The DNP-specific standards and procedures do not apply to other efforts to combat improper payments or matching programs that are not part of the DNP Initiative. For all matching programs, agencies shall continue to follow the existing standards and procedures in law and OMB policies unless directed otherwise in this guidance. In particular, agencies shall follow OMB's *Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of1988,*[69] OMB Circular A130,[70] and OMB Memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data Protecting Personal Privacy.*[71]

3. Definitions

---

[65] IPERIA applies only to executive agencies of the Federal Government, not to State or local governments or non-executive Federal agencies.

[66] For example, section 13 of this Memorandum establishes some general requirements regarding the performance of agencies' Data Integrity Boards.

[67] As provided in OMB guidance, agencies shall consider applying the matching principles in contexts other than those covered by the matching requirements. See OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing ofPersonal Data-Protecting Personal Privacy (Dec. 20, 2000) ("Although this guidance applies directly only to programs covered by the Matching Act, agencies should consider applying these principles in other data sharing contexts.").

[68] For example, section 5(e)(2)(D) of IPERIA provides that, for the purposes of IPERIA, section 552a(o)(1) of the Privacy Act shall be applied by substituting "between the source agency and the recipient agency or non-Federal agency or an agreement governing multiple agencies" for "between the source agency and the recipient agency or non-Federal agency" in the matter preceding subparagraph (A).

[69] Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818 (June 19, 1989), available at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/final_guidance_pl100-503.pdf.

[70] OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals, available at http://www.whitehouse.gov/omb/circulars_a130_a130trans4.

[71] OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data-Protecting Personal Privacy (Dec. 20, 2000), available at http://www.whitehouse.gov/omb/memoranda_m01-05/.

a The terms "agency," "individual," "maintain," "record," "system of records," "routine use," "recipient agency," "non-Federal agency," and "source agency," as used in this Memorandum, are defined in the Privacy Act.[72]

b. ***Computer matching agreement.*** The term "computer matching agreement" (CMA) means a written agreement between a source agency and a recipient agency (or multiple source and/or recipient agencies, as appropriate) or a non-Federal agency that allows the parties to engage in a matching program. In a Do Not Pay matching program, original source agencies need not be a party to a computer matching agreement between Treasury and a payment-issuing agency. Computer matching agreements are described in more detail in the Privacy Act, 5 U.S.C. § 552a(o), and in OMB guidance.[73]

c. ***Data Integrity Board.*** The term "Data Integrity Board" (DIB) means the board of senior personnel designated by the head of an agency that is responsible for reviewing the agency's proposals to conduct or participate in a matching program, and for conducting an annual review of all matching programs in which the agency has participated.

d. ***Do Not Pay Initiative.*** The term "Do Not Pay Initiative" (DNP Initiative) means the initiative codified by section 5 of IPERIA to facilitate Federal agencies' review of payment or award eligibility for purposes of identifying and preventing improper payments. The initiative may include other activities, as designated by OMB.

e ***Do Not Pay matching program.*** The term "Do Not Pay matching program" (DNP matching program) means a matching program (as defined in this Memorandum) that is conducted for purposes of the Do Not Pay Initiative and involves at least one of the five databases enumerated in section 5(a)(2) of IPERIA and/or a database designated by OMB pursuant to section 5(b) of this Memorandum. Do Not Pay matching programs are subject to alternative standards and procedures (as provided in this Memorandum) that are different from the standards and procedures that apply to matching programs outside of the Do Not Pay Initiative.

f. ***Federal benefit program.*** The term "Federal benefit program" is defined in the Privacy Act[74] and refers to any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals.

g. ***Improper payment.*** The term "improper payment" is defined in the Improper Payments Information Act of 2002[75] and refers to a payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. The definition includes any payment made to an ineligible recipient, any payment for an ineligible service, any duplicate payment, payments for services not rendered, and any payment that does not account for credit for applicable discounts.

h. ***Inspector General.*** The term "Inspector General" means a Federal agency official described in

---

[72] See 5 U.S.C. § 552a(a)(1)-(5), (7), (9)-(11).
[73] See Final Guidance Interpreting the Provisions ofPublic Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818, 25826 (June 19, 1989).
[74] See 5 U.S.C. § 552a(a)(12).
[75] Pub. L. No. 107-300 (2002) (codified at 31 U.S.C. § 3321 note).

subparagraph (A), (B), or (I) of section ll(b)(l) of the Inspector General Act of 1978[76] and any successor Inspector General.

i. ***Matching program.*** The term "matching program" is defined in the Privacy Act[77] and generally refers to a computerized comparison of records from two or more automated systems of records, or an automated system of records and automated records maintained by a non-Federal agency (or agent thereof). A matching program either pertains to Federal benefit programs or Federal personnel or payroll records. A Federal benefit match is performed for purposes of determining or verifying eligibility for payments under Federal benefit programs, or recouping payments or delinquent debts under Federal benefit programs. A matching program involves not just the matching activity itself, but also the investigative follow-up and ultimate action, if any.

j. ***Multilateral computer matching agreement.*** The term "multilateral computer matching agreement" (multilateral CMA) means a computer matching agreement that involves more than two agencies.[78] For the purposes of a Do Not Pay matching program involving Treasury's Working System, a multilateral computer matching agreement involves Treasury and more than one payment-issuing agency.

---

[76] 5 U.S.C. App.

[77] The term "matching program" (A) means any computerized comparison of-(i) two or more automated systems of records or a system of records with non-Federal records for the purpose of –

(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or –

(II) recouping payments or delinquent debts under such Federal benefit programs ...

(B) but does not include--

(i) matches performed to produce aggregate statistical data without any personal identifiers; (ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals; (iii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons; (iv) matches of tax information . .. (v) matches

(I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes ... –

(II) conducted by an agency using only records from systems of records maintained by that agency if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel; or (vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel; (vii) matches performed incident to a levy described in section 61 03(k)(8) of the Internal Revenue Code of 1986; or (viii) matches performed pursuant to section 202(x)(3) or 16ll(e)(l.) of the Social Security Act (42 U.S.C. § 402(x)(3), § 1382(e)(l).

5 U.S.C. § 552a(a)(8).

[78] The term "multilateral" simply refers to an agreement with multiple parties; it does not refer to an agreement that involves databases outside the United States that are not under the control of a Federal (or non-Federal) agency.

k. ***Original source agency.*** The term "original source agency" means a Federal agency that discloses records from a system of records to another agency in order to allow that agency to use the records in a matching program with a payment-issuing agency. For the purposes of a Do Not Pay matching program involving Treasury's Working System, an original source agency discloses records to Treasury in order to allow Treasury to engage in a Do Not Pay matching program with payment-issuing agencies. In a Do Not Pay matching program, original source agencies need not be a party to a computer matching agreement between Treasury and a payment-issuing agency.

l. ***Payment-issuing agency.*** The term "payment-issuing agency" means a Federal agency that has the authority to issue a payment or award and engages in a matching program for the purposes of determining or verifying eligibility for the payment or award under a Federal benefit program or of recouping the payment under a Federal benefit program. Generally, the payment-issuing agency will be the agency that benefits from the matching program. The payment-issuing agency is responsible for conducting the cost-benefit analysis and meeting the reporting and publication requirements in the matching provisions of the Privacy Act. If more than one payment-issuing agency is a party to a matching program, the payment-issuing agencies may assign these responsibilities as described in section 12(c) of this Memorandum.[79]

m. ***Treasury's Working System.*** The term "Treasury's Working System" means the Do Not Pay Initiative functions performed by the Department of the Treasury that are authorized by section 5 of IPERIA. Treasury's Working System includes Treasury's system of records for Do Not Pay, as well as other activities such as investigation activities for fraud and systemic improper payments detection through analytic technologies and other techniques.

4. Roles and Responsibilities

a. ***Office of Management and Budget.*** OMB is responsible for:

1. Implementing the DNP Initiative and providing guidance, oversight, and continued assistance to agencies.
2. Establishing a working system for pre-payment and pre-award review as part of the DNP Initiative.
3. Submitting annual reports to Congress regarding the operation of the DNP Initiative.

b. ***Department of the Treasury.*** Treasury is responsible for:

1. Hosting a working system (Treasury's Working System) for the DNP Initiative that includes a system of records for DNP that allows agencies to perform prepayment eligibility reviews, as required in IPERIA.
2. Developing memoranda of understanding (MOUs) with original source agencies, as described in this Memorandum, and periodically reviewing the MOUs to determine whether the terms are sufficient.
3. Entering into CMAs with payment-issuing agencies, as described in this Memorandum.

[79] For guidance on the publication and reporting requirements of the Privacy Act, see OMB Circular A-130, Appendix I.

4. Periodically reassessing whether all of the data in Treasury's Working System are relevant and necessary to meet the objectives in section 5 of IPERIA and deleting or expunging any data that are not.
5. Taking reasonable steps to ensure that records in Treasury's Working System are sufficiently accurate, complete, and up-to-date as is reasonably necessary to ensure fairness to the individual record subjects.
6. Coordinating with original source agencies to develop a process that allows individuals to request the correction of data.
7. Preparing and submitting to OMB a written assessment to document the suitability of any commercial databases that could be designated for use in Treasury's Working System.
8. Maintaining the central DNP Initiative website that includes all relevant information, including all relevant CMAs, system of records notices, and privacy impact assessments.
9. Complying with all applicable requirements in the Privacy Act and other applicable laws, regulations and policies, as well as with the terms of all relevant CMAs and MOUs.
10. Submitting periodic reports to OMB.

c. Original source agencies. Original source agencies are responsible for:

1. Ensuring that they have sufficient legal authority and a specific designation from OMB (except as provided by law) before disclosing records to Treasury for Treasury's Working System.
2. Entering into a written MOU with Treasury that describes how Treasury may use the records in question and provides rules for protecting and correcting the information and for the retention and destruction of records.
3. Confirming that Treasury has the appropriate level of security controls before sharing any records with Treasury.
4. Coordinating with Treasury to develop a process that allows individuals to request the correction of data, and promptly reviewing any request for correction.
5. Complying with all applicable requirements in the Privacy Act and other applicable laws, regulations, and policies, as well as with the terms of all relevant MOUs.

d. Payment-issuing agencies. Payment-issuing agencies are responsible for:

1. Ensuring that they have sufficient legal authority to engage in a matching program for purposes of the DNP Initiative.
2. Entering into CMAs with Treasury, as described in this Memorandum.
3. Conducting the cost-benefit analysis and meeting the reporting and publication requirements in the matching provisions of the Privacy Act.
4. Ensuring that they only match against data sources that are relevant and necessary for the specific matching purpose.
5. Making determinations about the disbursement of payments or awards, consistent with legal authority.
6. Complying with all applicable requirements in the Privacy Act and other applicable laws, regulations, and policies, as well as with the terms of all relevant CMAs.

e. ***Senior agency officials for privacy.*** All agencies' senior agency officials for privacy are responsible for:

1. Developing a training program for the agency's DIB to ensure that all members of the DIB are properly trained and prepared to fulfill their duties with respect to all matching activities at the

agency.

2. Periodically reviewing the effectiveness and responsiveness of the agency's DIB to determine whether the DIB needs additional support or instruction.

5. Including Databases in Do Not Pay

a. ***Enumerated databases.*** Section 5(a)(2) of IPERIA lists five databases that shall be included in the DNP Initiative without the need for OMB designation-the Social Security Administration's Death Master File, the General Services Administration's System for Award Management (formerly known as the Excluded Parties List System), Treasury's Debt Check Database, the Department of Housing and Urban Development's Credit Alert System or Credit Alert Interactive Voice Response System, and the Department of Health and Human Services Office of the Inspector General's List of Excluded Individuals/Entities.

b. ***OMB designation of additional databases***. Section 5(b)(1)(B) of IPERIA provides that OMB may designate additional databases for inclusion in the DNP Initiative, in consultation with the appropriate agencies. Treasury may only use or access additional databases for Treasury's Working System once OMB has officially designated such databases for inclusion, except as provided by law. Before designating additional databases, OMB will publish a 30-day notice of the designation proposal in the Federal Register asking for public comment. At the conclusion of the 30-day comment period, if OMB decides to finalize the designation, OMB will publish a notice in the Federal Register to officially designate the database for inclusion in the DNP Initiative.

When considering additional databases for designation, OMB will consider:

1. Statutory or other limitations on the use and sharing of specific data;
2. Privacy restrictions and risks associated with specific data;
3. Likelihood that the data will strengthen program integrity across programs and agencies;
4. Benefits of streamlining access to the data through the central DNP Initiative;
5. Costs associated with expanding or centralizing access, including modifications needed to system interfaces or other capabilities in order to make data accessible; and
6. Other policy and stakeholder considerations, as appropriate.

c. ***Data minimization***. OMB will only consider the inclusion of data in the DNP Initiative ifthe data are relevant and necessary to meet the objectives of section 5 of IPERIA. In the case ofTreasury's Working System, Treasury shall periodically reassess whether all data in Treasury's Working System meet this standard and delete or expunge any data that do not.

d. ***Disclosure from an original source agency to Treasury***. An OMB designation is not sufficient to allow agencies to provide records to Treasury for Treasury's Working System; agencies must also have legal authority to disclose records. This Memorandum alone does not provide agencies with such authority. Whenever OMB designates additional databases for inclusion in Treasury's Working System, the designation is subject to the original source agency's determination that it has the necessary legal authority to share the data with Treasury. In addition:

1. Prior to sharing any records, original source agencies shall confirm that Treasury affords the

appropriate level of security controls, comparable to those employed by the original source agency.

2. Original source agencies shall develop a MOU with Treasury that describes all restrictions on the use of a particular dataset, and all security controls and other requirements. Treasury shall describe all of these restrictions, security controls, and requirements in the CMAs with payment-issuing agencies, as applicable.

6. Use, Maintenance, Duplication, and Redisclosure of Records

a. ***Limits on Treasury's use, maintenance, duplication, and redisclosure of records.*** Any records provided from an original source agency to Treasury for purposes of Treasury's Working System shall not be used, maintained, duplicated, or redisclosed for any purpose other than those described in section 5 of IPERIA or this Memorandum, except where required by law.[80] All uses of the records shall be clearly described in the MOU between Treasury and the original source agency, as well as in Treasury's system of records notice for DNP. At a minimum, original' source agencies shall specify in the MOU that all limitations on the use, maintenance, duplication, or disclosure of the records at the original source agency also apply to Treasury. In addition, Treasury shall ensure that all routine uses listed in the DNP system of records notice are appropriate and properly tailored for every dataset to which they apply in Treasury's Working System.

b. ***Matching with a payment-issuing agency.*** In a DNP matching program, Treasury shall allow payment-issuing agencies to match against only those datasets in Treasury's Working System that are relevant and necessary for the specific matching purpose *(e.g.,* payment-issuing agencies shall not be allowed to match against income data if income is not relevant to the payment or award in question). The specific terms of the DNP matching program shall be described in the CMA and reviewed by each payment-issuing agency's DIB. All parties to the CMA shall be responsible for fully adhering to these terms.

c. ***Disclosure from Treasury to payment-issuing agency.*** In accordance with IPERIA, Treasury may disclose information *(i.e.,* the results of the match) to the payment-issuing agencies.

7. Retention and Destructions of Records

a. ***General guidelines on retention and destruction of records.*** Agencies shall follow all applicable record retention requirements, including those from the National Archives and Records Administration (NARA).

---

[80] Pursuant to the Privacy Act at 5 U.S.C. § 552a(o)(l)(H), a recipient agency may also duplicate or redisclose records provided by a source agency where "essential to the conduct of the matching program." As explained in OMB guidance, "The essential standard is a strict test that is more restrictive than the 'compatibility' standard the Privacy Act establishes for disclosures made pursuant to section (b)(3): 'for a routine use.' Thus, under the essential standard, the results of the match may be disclosed for follow-up and verification or for civil or criminal law enforcement investigation or prosecution if the match uncovers activity that warrants such a result." See Final Guidance Interpreting the Provisions ofPublic Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818,25826 (June 19, 1989).

b. ***Specific requirements on retention and destruction of records.*** The MOU between Treasury and an original source agency shall specify that Treasury will abide by the same rules for the retention and destruction of records that apply to the original source agency. The rules shall not change simply because records are provided to Treasury. As required in the Privacy Act, the relevant agencies' DIBs shall annually review agency recordkeeping and disposal policies and practices for compliance with the Privacy Act.

8. Correction of Data

a. ***Accuracy of records in Treasury's Working System.*** Because the records in Treasury's Working System will be used to help agencies make determinations about individuals, Treasury shall take reasonable steps to ensure that records in Treasury's Working System are sufficiently accurate, complete, and up-to-date as is reasonably necessary to ensure fairness to the individual record subjects. Treasury's MOUs with original source agencies shall describe the means by which the original source agencies will ensure that the records provided to Treasury meet these standards. Treasury's senior agency official for privacy shall periodically review the MOUs to determine whether the terms are sufficient.

b. ***Correction of data.*** Section 5(e)(4) of IPERIA of IPERIA requires OMB to establish procedures providing for the correction of data in order to ensure compliance with the Privacy Act. Treasury shall coordinate with original source agencies to develop a process that allows individuals to request the correction of data. The process shall meet the following general requirements:

1. If a request for correction is made directly to Treasury, Treasury shall promptly inform the original source agency (or agencies) of the request. The original source agency shall promptly review the request and determine whether corrections should be made to the data in question. Original source agencies shall follow their existing process for handling such requests. Some original source agencies have laws, regulations, or policies that govern how individuals may request corrections to records in a system of records. Thus, original source agencies may not be able to make corrections to records solely based on information provided by Treasury. However, original source agencies shall review all information provided by Treasury and, if appropriate, contact the individual making the request.

2. If a request for correction is made to an original source agency, the original source agency shall determine whether corrections should be made to the data and promptly inform Treasury of the determination if the data are included in Treasury's Working System. Whenever an original source agency determines that corrections are needed to data, the data shall be corrected at both the original source agency and in Treasury's Working System. Treasury and the original source agency shall take reasonable steps to avoid discrepancies between two versions of the same dataset. The data correction processes shall be described on Treasury's DNP website, in Treasury's DNP system of records notice, and in all relevant MOUs and CMAs.

c. ***Reporting to OMB***. Treasury shall annually report to OMB the total number of requests made to Treasury for the correction of data in Treasury's Working System. In addition, Treasury shall report to OMB the number of such requests that actually led to corrections of records. OMB will include this information in its annual report to Congress.

9. Procedural Safeguards

a. General procedural safeguards. The Privacy Act, at 5 U.S.C. § 552a(p), establishes certain procedural safeguards that individuals whose records are used in a matching program shall be afforded when matches uncover adverse information about them. As provided in section 5(e)(6) of IPERlA, nothing in IPERIA shall be construed to affect the rights of an individual under the Privacy Act at 5 U.S.C. § 552a(p).

b. Verification of adverse information. Before adverse action is taken against an individual, any adverse information that agencies discover shall be subjected to investigation and verification, unless an agency's DIB waives this requirement pursuant to the Privacy Act at 5 U.S.C. § 552a(p)(l)(A)(ii). Verification requires a confirmation of the specific information that would be used as the basis for an adverse action against an individual. As explained in OMB guidance, "Absolute confirmation is not required; a reasonable verification process that yields confirmatory data will provide the agency with a reasonable basis for taking action."[81] In each case, agencies shall document the specific information on which any determination about an individual is based. For additional guidance on verification of adverse information, agencies shall consult OMB's existing guidance.[82]

c. Notice and opportunity to contest. Once agencies have verified the adverse information, they shall provide the individual with notice and an opportunity to contest before taking adverse action. The notice shall inform the individual of the relevant information and give him or her an opportunity to provide an explanation. Individuals shall have 30 days to respond to a notice of adverse action, unless a statute or regulation provides a different period of time. For additional guidance on notice and opportunity to contest, agencies shall consult OMB's existing guidance.[83]

d. Stopping a payment or award. Except as provided by law, only the agency with authority to issue a payment or award may decide to stop the payment or award. Treasury disburses payments only as directed by payment-issuing agencies; IPERIA does not provide Treasury with authority to issue a payment or award. However, the Treasury disbursing official, consistent with his or her responsibility to ensure that payments are issued accurately and correctly, may act on behalf of the certifying agency to stop a payment *(i.e.,* not disburse the payment) only as directed by the certifying agency, in accordance with criteria and instructions specified by the certifying agency. As provided in section 5(b)(4) of IPERIA, there may be circumstances in which the law requires a payment or award to be made to a recipient, regardless of whether that recipient is identified as potentially ineligible under the DNP Initiative.

10. Cost Reimbursement

a. ***Need for cost reimbursement.*** When Federal agencies share data, cost reimbursement may be necessary in order to appropriately support additional work that one agency requests from another.

b. **General requirements for cost reimbursement**. In general, cost reimbursement for the DNP

[81] See Final Guidance Interpreting the Provisions of Public Law I 00-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25818, 25827 (June 19, 1989).
[82] Id.
[83] Id.

Initiative shall reflect the true costs incurred by an agency in order to provide data, recognizing that agencies may sometimes offset costs through reciprocal exchanges of data. Rather than paying for the same data multiple times, cost reimbursement is a mechanism to capture the actual total cost of providing access to the data.

c. **Specific considerations for cost reimbursement**. Appropriate cost reimbursement may vary for different data sources based on factors including, but not limited to, statutory obligations and restrictions associated with accessing a specific data source. In accessing and paying for data, agencies shall ensure proper coordination across programs and components.

11. Commercial Databases

a. ***Use of or access to commercial databases***. Section 5(d)(2)(C) of IPERIA provides that the DNP Initiative may include the use of or access to commercial databases to investigate activities for fraud and systematic improper payments detection. Some commercial databases may help the Federal Government meet the objectives of the DNP Initiative. At the same time, commercial databases may also present new or increased privacy risks, such as databases with inaccurate or out-of-date information. The requirements in this section of the Memorandum shall apply to all information in commercial databases that are not part of a system of records under the Privacy Act.

b. ***General standards for the use of or access to commercial databases***. Treasury may use or access a commercial database for Treasury's Working System only if OMB has officially, previously designated such database for inclusion following a period of public notice and comment, as described in section 5(b) of this Memorandum. Because commercial databases used or accessed for purposes of the DNP Initiative will be used to help agencies make determinations about individuals, it is important that agencies apply safeguards that are similarly rigorous to those that apply to systems of records under the Privacy Act. Thus, commercial data may only be used or accessed for the DNP Initiative when the commercial data in question would meet the following general standards:

1. Information in commercial databases must be relevant and necessary to meet the objectives described in section 5 of IPERIA.
2. Information in commercial databases must be sufficiently accurate, up-to-date, relevant, and complete to ensure fairness to the individual record subjects.
3. Information in commercial databases must not contain information that describes how any individual exercises rights guaranteed by the First Amendment, unless use of the data is expressly authorized by statute.

c. ***Specific requirements for Treasury's use o for access to commercial databases***. In addition to the general standards provided above, Treasury shall meet the following specific requirements whenever agencies use or access a commercial database as part of Treasury's Working System:

1. Treasury shall establish rules of conduct for persons involved in the use of or access to commercial databases and instruct each person with respect to such rules, including penalties for noncompliance, as appropriate.
2. Treasury shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of information in commercial databases when such information is under Treasury's control.

d. ***Written assessment of the suitability of a commercial database***. Before OMB considers designating a

commercial database for use or access in Treasury's Working System, Treasury shall prepare and submit to OMB a written assessment to document the suitability of the commercial database for use in Treasury's Working System. The assessment shall explain the need to use or access the data, explain how the data will be used or accessed, provide a description of the data (including each data element that will be used or accessed), and explain how the database meets all applicable requirements in this Memorandum. OMB will provide the written assessment to the public as part of the notice of the designation proposal described in section 5(b) of this Memorandum.

e. ***Pilot programs***. Treasury may use or access commercial databases as part of a pilot program without satisfying the requirements in this section of the Memorandum. A pilot program involves the small scale use of or access to commercial data in order to gather information on which to base a decision about seeking broader use or access. A pilot program shall terminate after a maximum of 6 months. No agency may stop any payments or awards or take any other adverse action against an individual as a result of a pilot program.

f. ***Compliance with law***. Agencies are reminded that information in commercial databases used in the DNP Initiative may constitute a system of records or become part of a system of records; such information would be subject to all applicable requirements in the Privacy Act. As with all aspects of this guidance in addition to the Privacy Act, agencies shall comply with all applicable requirements in the Paperwork Reduction Act,[84] the Federal Records Act,[85] the Information Quality Act[86] and other applicable laws, regulations, and policies.

12. Computer Matching Agreements for Do Not Pay

a. Multilateral CMAs. Section 5(e)(2)(D) of IPERIA authorizes CMAs "governing multiple agencies" for purposes of the DNP Initiative.[87] Agencies' default for a matching program shall always be traditional CMAs between one source agency and one recipient agency. However, in certain circumstances there may be advantages to using a multilateral CMA.

b. Considerations for the use of multilateral CMAs. Agencies may consider using multilateral CMAs if both the matching purpose and the specific data elements that will be matched are sufficiently similar across each of the agencies to allow all parties to satisfy the requirements in a single CMA that is clear to all relevant agencies and to the public. In making this determination, agencies shall consider whether using a multilateral CMA would lead to unnecessary complexities or inefficiencies that may offset the benefits. For example, it is possible that a multilateral CMA would make it more cumbersome for the agencies to alter or amend the CMA.

c. Reporting and publication requirements. Whenever agencies enter into a multilateral CMA, each of the payment-issuing agencies is responsible for meeting the reporting and publication requirements

[84] 44 U.S.C. § 3501 et seq.
[85] 44 U.S.C. Chapters 21, 22, 29, 31, and 33.
[86] Consolidated Appropriations Act of2001, Pub. L. No. 106-554, § 515, 114 Stat. 2763, 2763A154 (2000) (codified at 44 U.S.C. § 3516 note).
[87] As a matter of policy, agencies may use multilateral CMAs for non-DNP matching programs, as appropriate.

associated with the matching program.[88] However, the payment-issuing agencies may designate a single agency to report the CMA to OMB and Congress and publish the notice in the Federal Register on behalf of the other agencies, if such designation is clear in the report and notice. Each agency's DIB shall review the designation and determine that the arrangement is sufficient to meet the requirements in the Privacy Act and provide adequate notice to the public.

d. Termination date of CMAs. Section 5(e)(2)(C) of IPERIA provides that a CMA for a DNP matching program shall have a termination date of "less than 3 years." Furthermore, during the 3-month period leading up to the scheduled termination of a CMA, agencies may renew the CMA for a maximum of 3 years. These new termination periods apply only to DNP matching programs; CMAs outside of the DNP Initiative remain subject to the original termination periods in the Privacy Act.[89] Before a matching program may be renewed, each party shall certify that the matching program has been conducted in compliance with the CMA, and the participating agencies' DIBs shall review the request for renewal and make a determination that the matching program will be conducted without change.[90]

e. Additional guidance on CMAs. If agencies currently have CMAs with Treasury (or any other agency) that involve records that will be provided for Treasury's Working System, the agencies may be required to develop new CMAs in order to accommodate the DNP framework. Like system of records notices, CMAs shall be published and reported to OMB and Congress at the departmental or agency level, even if the records involved are maintained at a component level. For example, the Department of Health and Human Services would publish and report a CMA to OMB and Congress on behalf of the Centers for Medicare and Medicaid Services (CMS), even if the match involves only CMS records.

13. General Guidance on Review by Data Integrity Boards

a. ***General guidance for DIBs***. Agencies' DIBs are responsible for approving or disapproving proposed matching programs based on an assessment of the adequacy of the CMA and other relevant information. When DIBs review a proposed matching program, they shall assess the CMA to ensure that it fully complies with the Privacy Act, as well as any other applicable laws, regulations, and policies. When making a determination, DIBs shall document in writing their reasons for approving or disapproving a matching program. This documentation shall be provided to the appropriate agency officials.

b. ***Training for DIBs***. The senior agency official for privacy shall ensure that all members of the DIB are properly trained and prepared to fulfill their duties with respect to all matching activities at the agency.

---

[88] For guidance on the publication and reporting requirements of the Privacy Act, see OMB Circular A-130, Appendix I.

[89] Pursuant to 5 U.S.C. § 552a(o)(2)(C)-(D), a CMA outside of the DNP Initiative may only remain in effect for a maximum of 18 months, with an optional renewal period of one year. All termination dates and renewals are subject to approval by agencies' DIBs.

[90] Before a matching program may be renewed, each party shall certify that the matching program has been conducted in compliance with the CMA, and the participating agencies' DIBs shall review the request for renewal and make a determination that the matching program will be conducted without change.

The senior agency official for privacy shall develop a training program that members of the DIB shall be required to complete, as appropriate. In particular, all DIB members shall receive training regarding the requirements in the Privacy Act, other relevant laws, and guidance from OMB, NARA, and the Department of Commerce's National Institute of Standards and Technology.

c. ***Effectiveness and responsiveness of DIBs***. Agencies' DIBs shall meet with sufficient frequency to ensure that matching programs are carried out efficiently, expeditiously, and in compliance with the law. At a minimum, DIBs shall meet annually to evaluate ongoing matching programs and consider whether any modifications are warranted. In addition, agencies shall ensure that DIBs review matching proposals expeditiously so as not to cause delays to necessary programs. The senior agency official for privacy shall periodically review the effectiveness and responsiveness of the agency's DIB to determine whether the DIB needs additional support or instruction.

d. ***60-day deadline for review of a CMA***. Section 5(e)(2)(B) of IPERIA requires DIBs to respond to a proposed CMA for the DNP Initiative no later than 60 calendar days after the proposal has been presented to the DIB. This 60-day deadline shall apply to new CMAs, as well as requests for the renewal of an established CMA. The 60-day clock shall begin as soon as the agency provides the DIB with the materials required for the DIB's review. Although the 60-day deadline in the law applies only to DNP matching programs, agencies are encouraged to adopt this timeframe as a general practice for all matching programs, as appropriate.

   In most cases, the DIB's response to the proposal shall be a definitive approval or disapproval of the matching program. If DIBs have questions about the proposal, those questions shall be submitted to agency officials by day 30 of the 60-day period, if possible. Agency officials shall answer any questions from DIBs in a timely manner. If circumstances do not permit the DIB to approve or disapprove the DNP matching program within 60 days, the DIB shall provide a brief memorandum to the head of the agency (or to the Inspector General in cases where the Inspector General proposed the matching program) describing the necessity for the delay.

e. ***Reporting to OMB***. Agencies shall annually report to OMB the specific number of days that it takes the DIB to approve or disapprove each proposed DNP matching program.

14. Cost-Benefit Analysis

a. ***Specific estimate of savings not required***. The Privacy Act at 5 U.S.C. § 552a(u)(4) requires agencies to perform a cost-benefit analysis for a proposed matching program. This cost-benefit analysis normally includes a specific estimate of any savings, which is included as part of the justification for the matching program in the CMA. However, section 5(e)(2)(E) of IPERIA provides that agencies' cost-benefit analyses for a DNP matching program need not contain a specific estimate of any savings.

b. ***Cost-benefit analysis still required***. Although agencies need not provide a specific estimate of savings, they shall perform a qualitative analysis of the potential costs and benefits of any proposed DNP matching program, unless the cost-benefit analysis is not required pursuant to the Privacy Act at 5 U.S.C. § 552a(u)(4)(B)-(C). This qualitative analysis of potential costs and benefits shall allow the agency to explain in the CMA why there is good reason to believe that the DNP matching program would provide cost savings (or why the matching activity would be justified on other grounds).

c. ***DIBs shall review all relevant data***. When an agency proposes to renew a DNP matching program (or proposes a new DNP matching program that is similar to a previously approved matching program),

the agency's DIB shall review all relevant data that was reported to OMB or Congress, including specific data about costs and benefits.

15. Public Availability of Computer Matching Agreements

a. ***Publication of CMAs on a public website.*** Section 5(e)(3)(C) of IPERIA requires OMB to establish rules regarding what constitutes making a DNP Initiative CMA available upon request to the public, pursuant to the Privacy Act at 5 U.S.C. § 552a(o)(2)(A)(ii). The statute provides that these rules shall include requiring publication of the CMA on a public website. As a responsibility of hosting Treasury's Working System, Treasury shall maintain the central DNP Initiative website that includes all of the relevant information about Treasury's Working System. In particular, Treasury shall post (or provide direct links to) all of the CMAs, system of records notices, and privacy impact assessments that pertain to Treasury's Working System. Providing such documents on Treasury's DNP Initiative website will promote transparency and provide examples that other agencies may use to help develop future CMAs and other materials related to Treasury's Working System.

b. ***Removing or redacting sensitive information in CMAs.*** Whenever agencies make CMAs or other materials available to the public, they shall remove or redact any unnecessary personally identifiable information, as appropriate. In addition, agencies shall consider removing or redacting any information that could present security risks, such as specific information about security controls for a system *(e.g.,* password length or complexity).

16. Matching by Inspectors General

a. General guidelines for CMAs and Inspectors General. Section 5(e)(2)(A) of IPERIA provides that each Inspector General and the head of each agency may enter into CMAs with other Inspectors General and agency heads that allow ongoing data matching (which shall include automated data matching) to assist in the detection and prevention of improper payments. Inspectors General may use the authority provided in IPERIA to enter into CMAs only if the purpose of the match is to detect and prevent improper payments. Although Inspectors General may enter into CMAs, all CMAs shall be published and reported to OMB and Congress at the departmental or agency level.[91]

b. Specific requirements for CMAs and Inspectors General. CMAs that involve one or more Inspector General are subject to all applicable requirements that pertain to CMAs for the DNP Initiative, including, but not limited to, DIB review, termination dates, correction of data, procedural safeguards, and reporting and notice requirements. If an Inspector General's proposed CMA is disapproved by the agency's DIB, the Inspector General may appeal the disapproval to OMB, pursuant to the Privacy Act at 5 U.S.C. § 552a(u)(5).

17. Matches Involving a Subset of Records from a System of Records

The matching requirements of the Privacy Act shall apply to all matching activities that involve a subset of records from a system of records when the subset of records itself would meet the definition of "system of records" in the Privacy Act *(i.e.,* it is a group of any records under the control of any agency from

[91] For guidance on the publication and reporting requirements of the Privacy Act, see OMB Circular A-130, Appendix I.

which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual), so long as the other qualifications in the statute are met.

18. For Further Information

If agencies have specific questions regarding this Memorandum, they may contact OMB at privacy-oira@omb.eop.gov. If agencies have general questions regarding Treasury's Working System, they may visit http://donotpay.treas.gov or contact Treasury at donotpay@bpd.treas.gov.

Appendix C: Executive Order 13520

Executive Order 13520-- Reducing Improper Payments and Eliminating Waste in Federal Programs

November 23, 2009

EXECUTIVE ORDER

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in the interest of reducing payment errors and eliminating waste, fraud, and abuse in Federal programs, it is hereby ordered as follows:

Section 1. Purpose. When the Federal Government makes payments to individuals and businesses as program beneficiaries, grantees, or contractors, or on behalf of program beneficiaries, it must make every effort to confirm that the right recipient is receiving the right payment for the right reason at the right time. The purpose of this order is to reduce improper payments by intensifying efforts to eliminate payment error, waste, fraud, and abuse in the major programs administered by the Federal Government, while continuing to ensure that Federal programs serve and provide access to their intended beneficiaries. No single step will fully achieve these goals. Therefore, this order adopts a comprehensive set of policies, including transparency and public scrutiny of significant payment errors throughout the Federal Government; a focus on identifying and eliminating the highest improper payments; accountability for reducing improper payments among executive branch agencies and officials; and coordinated Federal, State, and local government action in identifying and eliminating

improper payments. Because this order targets error, waste, fraud, and abuse -- not legitimate use of Government services -- efforts to reduce improper payments under this order must protect access to Federal programs by their intended beneficiaries.

Sec. 2. Transparency and Public Participation.

(a) Within 90 days of the date of this order, the Director of the Office of Management and Budget (OMB) shall:

(i) identify Federal programs in which the highest dollar value or majority of Government-wide improper payments occur (high-priority programs);

(ii) establish, in coordination with the executive department or agency (agency) responsible for administering the high-priority program annual or semi-annual targets (or where such targets already exist, supplemental targets), as appropriate, for reducing improper payments associated with each high-priority program;

(iii) issue Government-wide guidance on the implementation of this order, including procedures for identifying and publicizing the list of entities described in subsection (b)(v) of this section and for administrative appeal of the decision to publish the identity of those entities, prior to publication; and

(iv) establish a working group consisting of Federal, State, and local officials to make recommendations to the Director of OMB designed to improve the Federal Government's measurement of access to Federal programs by the programs' intended beneficiaries. The working group's recommendations shall be prepared in consultation with the Council of Inspectors General on Integrity and Efficiency (CIGIE) and submitted within 180 days of the date of this order, and the recommended measurements may be incorporated by the Secretary of the Treasury in the information published pursuant to subsection (b) of this section.

(b) Within 180 days of the date of this order, the Secretary of the Treasury in coordination with the Attorney General and the Director of OMB, shall publish on the Internet information about improper payments under high-priority programs. The information shall include, subject to Federal privacy policies and to the extent permitted by law:

(i) the names of the accountable officials designated under section 3 of this order;

(ii) current and historical rates and amounts of improper payments, including, where known and appropriate, causes of the improper payments;

(iii) current and historical rates and amounts of recovery of improper payments,

where appropriate (or, where improper payments are identified solely on the basis of a sample, recovery rates and amounts estimated on the basis of the applicable sample);

(iv) targets for reducing as well as recovering improper payments, where appropriate; and

(v) the entities that have received the greatest amount of outstanding improper payments (or, where improper payments are identified solely on the basis of a sample, the entities that have received the greatest amount of outstanding improper payments in the applicable sample).

Information on entities that have received the greatest amount of outstanding improper payments shall not include any referrals the agency made or anticipates making to the Department of Justice, or any information provided in connection with such referrals.

(c) Within 180 days of the date of this order, the Secretary of the Treasury in coordination with the Attorney General and the Director of OMB and in consultation with the CIGIE, shall establish a central Internet-based method to collect from the public information concerning suspected incidents of waste, fraud, and abuse by an entity receiving Federal funds that have led or may lead to improper payments by the Federal Government.

(d) Agencies shall place a prominently displayed link to Internet-based resources for addressing improper payments, including the resources established under subsections (b) and (c) of this section, on their Internet home pages.

Sec. 3. Agency Accountability and Coordination.

(a) Within 120 days of the date of this order, the head of each agency responsible for operating a high-priority program shall designate an official who holds an existing Senate-confirmed position to be accountable for meeting the targets established under section 2 of this order without unduly burdening program access and participation by eligible beneficiaries. In those agencies where the majority of payments are isolated to a single component, the head of the agency shall name a second accountable official for that component whose sole responsibility would be for program integrity activities and, as appropriate, shall consolidate and coordinate all program integrity activities within the component.

(b) Within 180 days of the date of this order, each agency official designated under subsection (a) of this section, or otherwise designated by the Director of OMB, shall provide the agency's Inspector General a report containing:

i. the agency's methodology for identifying and measuring improper payments

by the agency's high-priority programs;

ii. the agency's plans, together with supporting analysis, for meeting the reduction targets for improper payments in the agency's high-priority programs; and

iii. the agency's plan, together with supporting analysis, for ensuring that initiatives undertaken pursuant to this order do not unduly burden program access and participation by eligible beneficiaries.

Following the receipt and review of this information, the agency Inspector General shall assess the level of risk associated with the applicable programs, determine the extent of oversight warranted, and provide the agency head with recommendations, if any, for modifying the agency's methodology, improper payment reduction plans, or program access and participation plans.

(c) If an agency fails to meet the targets established under section 2 of this order or implement the plan described in subsection (b)(iii) of this section for 2 consecutive years, that agency's accountable official designated under subsection (a) of this section shall submit to the agency head, Inspector General, and Chief Financial Officer a report describing the likely causes of the agency's failure and proposing a remedial plan. The agency head shall review this plan and, in consultation with the Inspector General and Chief Financial Officer, forward the plan with any additional comments and analysis to the Director of OMB.

(d) Within 180 days of the date of this order, the Chief Financial Officers Council (CFOC) in consultation with the CIGIE, the Department of Justice, and program experts, shall make recommendations to the Director of OMB and the Secretary of the Treasury on actions (including actions related to forensic accounting and audits) agencies should take to more effectively tailor their methodologies for identifying and measuring improper payments to those programs, or components of programs, where improper payments are most likely to occur. Recommendations shall address the manner in which the recommended actions would affect program access and participation by eligible beneficiaries.

(e) Within 180 days of the date of this order, the Secretary of the Treasury and the Director of OMB in consultation with the CIGIE, the Department of Justice, and program experts, shall recommend to the President actions designed to reduce improper payments by improving information sharing among agencies and programs, and where applicable, State and local governments and other stakeholders. The recommendations shall address the ways in which information sharing may improve eligibility verification and pre-payment scrutiny, shall identify legal or regulatory impediments to effective information sharing, and shall address the manner in which the recommended actions would affect program access and participation by eligible beneficiaries.

(f) Within 180 days of the date of this order, and at least once every quarter thereafter, the head of each agency shall submit to the agency's Inspector General and the CIGIE, and make available to the public, a report on any high-dollar improper payments identified by the agency, subject to Federal privacy policies and to the extent permitted by law. The report shall describe any actions the agency has taken or plans to take to recover improper payments, as well as any actions the agency intends to take to prevent improper payments from occurring in the future. The report shall not include any referrals the agency made or anticipates making to the Department of Justice, or any information provided in connection with such referrals. Following the review of each report, the agency Inspector General and the CIGIE shall assess the level of risk associated with the applicable program, determine the extent of oversight warranted, and provide the agency head with recommendations, if any, for modifying the agency's plans.

Sec. 4. Enhanced Focus on Contractors and Working with State and Local Stakeholders.

(a) Within 180 days of the date of this order, the Federal Acquisition Regulatory Council, in coordination with the Director of OMB, and in consultation with the National Procurement Fraud Task Force (or its successor group), the CIGIE, and appropriate agency officials, shall recommend to the President actions designed to enhance contractor accountability for improper payments. The recommendations may include, but are not limited to, subjecting contractors to debarment, suspension, financial penalties, and identification through a public Internet website, subject to Federal privacy policies and to the extent permitted by law and where the identification would not interfere with or compromise an ongoing criminal or civil investigation, for knowingly failing timely to disclose credible evidence of significant overpayments received on Government contracts.

(b) Within 30 days of the date of this order, the Director of OMB shall establish a working group consisting of Federal and elected State and local officials to make recommendations to the Director of OMB designed to improve the effectiveness of single audits of State and local governments and non-profit organizations that are expending Federal funds. The Director of OMB may designate an appropriate official to serve as Chair of the working group to convene its meetings and direct its work. The working group's recommendations shall be prepared in consultation with the CIGIE and submitted within 180 days of the date of this order. The recommendations shall address, among other things, the effectiveness of single audits in identifying improper payments and opportunities to streamline or eliminate single audit requirements where their value is minimal.

(c) Within 30 days of the date of this order, the Director of OMB shall establish a working group (which may be separate from the group established under subsection (b) of this section) consisting of Federal and elected State and local officials to make recommendations to the Director of OMB for administrative actions designed to improve the incentives and accountability of State and local governments, as well as other entities receiving Federal funds, for reducing improper payments. The Director of OMB may designate an appropriate official to serve as Chair of the working group to convene its meetings and direct its work. The working group's recommendations shall be prepared in consultation with the CIGIE and submitted within

180 days of the date of this order.

Sec. 5. Policy Proposals. The Director of OMB, in consultation with the appropriate agencies and the CIGIE, shall develop policy recommendations, including potential legislative proposals, designed to reduce improper payments, including those caused by error, waste, fraud, and abuse, across Federal programs without compromising program access, to be included, as appropriate, in the Budget of the United States Government for Fiscal Year 2011 and future years, or other Administration proposals.

Sec. 6. General Provisions.

(a) Nothing in this order shall be construed to impair or otherwise affect:

(i) authority granted by law to a department, agency, the head thereof, or any agency Inspector General; or

(ii) functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(b) Nothing in this order shall be construed to require the disclosure of classified information, law enforcement sensitive information, or other information that must be protected in the interests of national security.

(c) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

THE WHITE HOUSE,
November 20, 2009.