

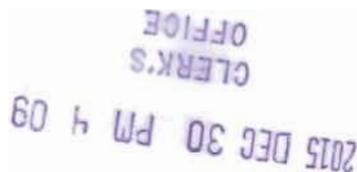
Social Security Number Protection Task Force

Report to Governor Bruce Rauner, Attorney General Lisa Madigan,
Secretary of State Jesse White, and Illinois General Assembly

December 30, 2015

CONTENTS

- I. Task Force Background
 - a. Recent Privacy Developments
 - b. Membership of the Task Force
- II. Part I: Protection of SSNs in the Public Record
 - a. Identity Protection Act: Identity-Protection Policy
 - b. Illinois CIO Council Cybersecurity Working Group
- III. Part II: SSNs as Internal Identifiers
 - a. Medicare Access and CHIP Reauthorization Act of 2015
 - b. Department of the Army - Pamphlet 600-8-14
- IV. Task Force Appointments & Updates
- V. Conclusion
- VI. Appendix A: Template Identity-Protection Policy
- VII. Appendix B: Template Statement of Purpose(s)
- VIII. Appendix C: HB1260 – *Passed Third Reading, December 02, 2015*
- IX. Appendix D: Illinois Consumer Fraud and Deceptive Business Practices Act (815 ILCS 505/1 *et seq.*) Sections 2QQ & 2RR
- X. Appendix E: Medicare Access and CHIP Reauthorization Act of 2015
- XI. Appendix F: Department of the Army – Pamphlet 600-8-14



TASK FORCE BACKGROUND

The Social Security Number (SSN) remains the key piece of sensitive personally identifiable information that identity thieves use to commit fraud. The SSN was intended to be used solely to distribute Social Security benefits, but in the years since its inception in 1935, it has been also used as a unique identification number. The SSN is therefore not only tied to an individual's credit report, financial records, and Social Security earnings with the federal government, but is also present in employment, educational, health, insurance, and criminal records. The wide dissemination of SSNs increases the likelihood that the numbers can be accessed and subsequently used for fraudulent purposes.

Consumers are therefore encouraged to limit their exposure to identity theft by protecting their SSNs. Businesses are also encouraged to do their part by taking necessary steps to limit the collection of SSNs, protect SSNs in their possession, and dispose of documents containing SSNs in a manner that renders them unusable. Local and state government agencies also have a role in protecting SSNs they maintain and reducing their continued widespread dissemination. Government agencies have the larger task of maintaining a system of open records for the public, while taking measures to reduce the amount of sensitive personally identifiable information in those records.

The General Assembly created the Social Security Number Protection Task Force (Task Force) through Public Act 93-0813 in 2004. The Task Force is charged with examining the procedures used by the State to protect an individual against the unauthorized disclosure of his or her SSN when the State requires the individual to provide that number to an officer or agency of the State. The Task Force also is required to explore the technical and procedural changes that are necessary to implement a unique identification system to replace the use of SSNs by State and local governments for identification and record-keeping purposes. In 2007, the General Assembly amended the law governing the Task Force by Public Act 95-0482. The Office of the Attorney General is charged with chairing and administering the activities of the Task Force.

RECENT PRIVACY DEVELOPMENT

On February 27, 2015, President Obama announced the Consumer Privacy Bill of Rights Act of 2015, a draft aimed at providing business stakeholders with a code of conduct as they collect treasure troves of data from consumers' daily interactions using a multitude of sensors, applications, web clicks, online advertisements, and browser cookies. The 2015 announcement serves as a re-introduction of President Obama's 2012 Consumer Privacy Bill of Rights, which represented key principles from the *Consumer Data Privacy In a Networked World: A Framework For Protecting Privacy And Promoting Innovation In the Global Digital Economy* (Privacy Report). According to the White House, the proposed Privacy Bill of Rights is intended to stimulate discussions among Congress, consumers, and industry stakeholders with the intended goal of passing new federal privacy legislation.

Similar to the 2012 Consumer Privacy Bill of Rights, the 2015 Act focuses on seven core principles. These principles include: (1) Transparency – Consumers have a right to easily understandable and accessible information about an entity's privacy and security practices; (2)

Individual Control – Consumers have a right to exercise control over what personal data companies collect from them, how the data is used, and the ability to withdraw consent over data collection in a manner similar to which it was originally given; (3) Respect for Content – Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data in conjunction with any representations made by the consumer facing entity; (4) Focused Collection and Responsible Use – Consumers have a right to reasonable limits on the personal data that companies collect, create, process, retain, use, and disclose; (5) Security – Consumer have the right to expect that entities will implement safeguards to ensure secure and proper handling of personal data; (6) Access and Accuracy – Consumer have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to the consumer if the data is inaccurate; and (7) Accountability – Consumers have the right to have personal data handled by companies with appropriate measures in place to assure that they adhere to the fundamentals and obligations pursuant to this Consumer Privacy Bill of Rights. As discussed in prior Social Security Number Protection Task Force Reports, this Consumer Privacy Bill of Rights applies to all commercial uses of personal data, including data which may be linked directly to a specific individual, thus the core principles aid in protecting SSNs and limiting their widespread dissemination and potential misuse.

While the President’s 2015 announcement appears to be gaining strength with Congressional leaders, critics point out that as a result of weak enforcement provisions, specifically those aimed at assessing appropriate fines for violations, significant changes must occur going forward in order for strong enforcement power to exist. Other critical aspects of the Privacy Bill of Rights include the controversial preemption of state privacy and data security laws, as well as a business’s ability to draft their own code of conduct, both of which may prove serious pitfalls for holding businesses accountable for their conduct towards consumers.

The Task Force will monitor the President’s Consumer Privacy Bill of Rights, as well as other such associated initiatives, taking special care to ensure that as each address and advance forward Illinois residents’ data privacy rights.

MEMBERSHIP OF THE TASK FORCE

- Two members representing the House of Representatives, appointed by the Speaker of the House – **Representative Sara Feigenholtz, Representative Ann Williams**
- Two members representing the House of Representatives, appointed by the Minority Leader of the House – ***Awaiting Member Appointment Confirmation***
- Two members representing the Senate, appointed by the President of the Senate – **Senator Jacqueline Collins, *Awaiting Additional Member Appointment Confirmation***
- Two members representing the Senate, appointed by the Minority Leader of the Senate - **Senator Dan Duffy, *Awaiting Additional Member Appointment Confirmation***
- One member representing the Office of the Attorney General – **Deborah Hagan, Task Force Chair**
- One member representing the Office of the Secretary of State – **Micah Miller**
- One member representing the Office of the Governor – ***Awaiting Member Appointment Confirmation***

- One member representing the Department of Natural Resources – **John “J.J.” Pohlman**
- One member representing the Department of Healthcare and Family Services – **Elizabeth Festa**
- One member representing the Department of Revenue – *Awaiting Member Appointment Confirmation*
- One member representing the Department of State Police – *Awaiting Member Appointment Confirmation*
- One member representing the Department of Employment Security – **Joseph Mueller**
- One member representing the Illinois Courts – **James Morphew**
- One member representing the Department on Aging – *Awaiting Member Appointment Confirmation*
- One member representing Central Management Services – **Markus Veile**
- One member appointed by the Executive Director of the Board of Higher Education – *Awaiting Member Appointment Confirmation*
- One member appointed by the Secretary of Human Services – *Awaiting Member Appointment Confirmation*
- Three members representing local-governmental organizations – **Dorothy Brown, Larry Reinhardt, Virginia Hayden**
- One member representing the Office of the State Comptroller – **Alissa Camp**
- One member representing school administrators, appointed by the State Superintendent of Education – **Sara Boucek**

PART I: PROTECTION OF SSNs IN THE PUBLIC RECORD

The first statutory requirement of the Social Security Number Protection Task Force Act is to examine the procedures used by the State to protect an individual against the unauthorized disclosure of his or her SSN.

IDENTITY PROTECTION ACT

One way to limit the unauthorized disclosure of SSNs is to limit their collection in the first place. If fewer entities collect and use SSNs, fewer entities are capable of disclosing those numbers improperly.

The Identity Protection Act, 5 ILCS 179/1 *et seq.*, prohibits certain collections, uses and disclosures of an individual’s SSN by any person, or State or local government agencies. Specifically, the Act, with several exceptions, prohibits a person, or State or local government agency from collecting, using, or disclosing a SSN unless: (1) required to do so under state or federal law or the collection, use, or disclosure of the Social Security number is otherwise necessary for the performance of the agency’s duties and responsibilities; (2) the need and purpose for the SSN is documented before the request; and (3) the SSN collected is relevant to the documented need and purpose. The need and purpose for the collection and use of SSNs must be documented in a written Identity-Protection Policy.

Each local government agency must file a written copy of its policy with the governing board of the unit of local government within 30 days after approval of the policy. Under Section 37(b),

“each State agency must provide a copy of its identity-protection policy to the Social Security Number Protection Task Force within 30 days after the approval of the policy.” State agencies were reminded of this requirement on August 24, 2011. Policies can be submitted to the Task Force by mailing a copy to:

Illinois Attorney General
Social Security Number Protection Task Force
c/o: AAG Matthew W. Van Hise
500 S. Second Street
Springfield, IL 62706

As part of the implementation of the policies, local and state agencies will require that all employees identified as having access to SSNs in the course of performing their duties be trained to protect the confidentiality of SSNs. Training should include instructions on the proper handling of information that contains SSNs from the time of the collection of the information through its destruction.

Identity-Protection Policies were to have been implemented within 12 months of the date of approval and a copy was to have been sent to the Task Force no later than June 1, 2012. For reference, an Identity-Protection Policy and Statement of Purpose(s) template can be found in Appendixes A and B.

Updated and/or amended Identity-Protection Policies may be sent electronically to S3@atg.state.il.us. Submissions shall occur as soon as practicable or within the calendar year in which the updated amendment was implemented. An acknowledgement of receipt and record will be provided by a duly authorized representative of the Task Force chairperson.

(Template Identity-Protection Policy – Appendix A)
(Template Statement of Purpose(s) – Appendix B)

ILLINOIS CIO COUNCIL – CYBERSECURITY WORKING GROUP

Created in 2015 by the newly appointed Illinois Chief Information Officer (“CIO”), the Illinois CIO Council’s Cybersecurity Working Group was developed to help drive the modernization of information technology within the state. Under the guidance of Illinois state agency CIOs, CISOs, and other relevant state agency information technology representatives, the CIO Council has made the need for ongoing and improved protection of personally identifiable information (PII) in state information systems a top priority. To date, the CIO Council has been executing an aggressive strategy to ensure the ongoing protection of PII within current systems, while ensuring newly developed systems minimize the use of PII and specifically, SSNs.

Within the CIO Council, the Illinois Chief Information Security Officer (“CISO”) was assigned to ensure the ongoing focus on securing the state’s most critical information assets, including PII. Since getting involved, the CISO has been deploying advanced encryption technologies to protect Illinois residents’ sensitive personal information, both at rest, stored in a data system, and in transit, shared across systems.

Moving forward into 2016, the CIO Council will be developing training for all state employees regarding the appropriate handling of personally identifiable information. Through training, technology, and newly developing processes, the CIO Council will continue to push Illinois as a national leader in securing PII.

The Task Force will continue to monitor the efforts of the CIO Council, providing yearly updates in subsequent Reports.

PERSONAL INFORMATION PROTECTION ACT

In an effort to further protect against the unauthorized disclosure of SSNs, as well as protect against the unauthorized use and disclosure of other data elements constituting consumer personal information, two notable bills were introduced during the 99th General Assembly that aimed at expanding the Personal Information Protection Act (“PIPA”).

Currently, PIPA requires entities that suffer security breaches of personal information to notify affected individuals of the breach in the most expedient time possible and without unreasonable delay. Notification in the event of a breach allows affected individuals to take steps to protect themselves against identity theft or other financial fraud. A breach is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. Personal information includes an individual’s name (first name or first initial and last name) combined with either the individual’s SSN, driver’s license number/State identification card number, or financial account number. As discussed in the 2012 Task Force Report, it is important for Task Force members to be aware of the requirements of PIPA, as PIPA also applies to state agencies that collect consumers’ personal information. Furthermore, although breach notification is limited for most entities to computerized data **only**, when a state agency suffers a security breach of either *written* or *computerized* data, notification to affected consumers must be made.

In addition to the requirements above, PIPA also provides guidance as to the responsibilities of data collectors that maintain personal information, but do not own or license such information. PIPA also details how breach notification to consumers shall occur, the contents of such notification, and lastly, covers how proper disposal shall occur when disposing of consumers’ personal information.

Of the two bills introduced during the 99th General Assembly, HB1260, a continuation of the prior SB1833, amends the Personal Information Protection Act (“PIPA”) to provide for the expansion of the following:

- (1) new data elements constituting consumers’ personal information (and therefore triggering the breach notification requirement of PIPA if these data elements are breached), specifically:
 - a. medical information;
 - b. health insurance information;
 - c. unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an

- individual (such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data);
- (2) the method for providing notice those limited to one geographic area, specifically, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required;
 - (3) the trigger and requirements for when a state agency must notify the Attorney General's Office of a breach and what such notice must include, specifically, any state agency that suffers a single breach of the security of the data concerning the personal information of more than 250 Illinois residents shall provide notice to the Attorney General of the breach. Within this addition, several items are highlighted concerning what must be provided within such notice;
 - (4) the requirement that data collectors implement and maintain reasonable security measures to protect records containing personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure; And
 - (5) the acknowledgment that a covered entity or business associate that is subject to and in compliance with the privacy and security standards for the protection of electronic health information under the federal Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act is deemed to be in compliance with the Personal Information Protect Act if certain requirements are met.

With these proposed expansions to the data elements of personal information, along with the requiring of data collectors to implement and maintain reasonable security measures when protecting personal information, Illinois residents will have greater protections from the unauthorized disclosure of their sensitive information.

The Task Force will continue to monitor the progression of HB1260 with the hope it becomes new law.

(HB1260 – *Passed Third Reading, December 02, 2015* – Appendix C)

PART II: SSNS AS INTERNAL IDENTIFIERS

The second requirement of the Task Force is to explore the technical and procedural changes that are necessary to implement a unique identification system to replace the use of SSNs for identification and record-keeping purposes by State and local governments. State and local government agencies continue to internally assess the collection and use of SSNs. Such an assessment was critical in drafting Identity-Protection Policies.

Not since the 2012 amendments to the Illinois Consumer Fraud and Deceptive Business Practices Act (815 ILCS 505/1 *et seq.*) “Consumer Fraud Act” has there been such a significant update aimed at replacing the use of SSNs for identification and record keeping purposes than the recent passage of the Medicare Access and CHIP Reauthorization Act of 2015 and Department of the Army implementation of Pamphlet 600-8-14.

As background, the Consumer Fraud Act, which in part covers the collection, use, and posting of SSNs in its 2012 updates to Section 2QQ and 2RR, already contains state-level updates similar to the federal matters noted below.

In Section 2QQ, the Consumer Fraud Act indicates that a person or entity may not print an individual's SSN on an insurance card. It goes on to state that a person or entity that provides an insurance card must print on the card an identification number unique to the holder of the card in the format prescribed by the Uniform Prescription Drug Information Card Act.

Generally, Section 2RR of the Consumer Fraud Act covers a broader set of restrictions for the use, display, and transmission of an individuals' SSN.

(Illinois Consumer Fraud and Deceptive Business Practices Act (815 ILCS 505/1 *et seq.*)
Sections 2QQ & 2RR – Appendix D)

MEDICARE ACCESS AND CHIP REAUTHORIZATION ACT OF 2015

In taking a nod from the Consumer Fraud Act, the Medicare Access and CHIP Reauthorization Act of 2015 creates the prohibition of including SSNs on Medicare cards as a means of member identification. As enacted, the new Act requires that the Secretary of Health and Human Services, in consultation with the Commissioner of Social Security, establish cost effective procedures to ensure that a Social Security account number not be displayed, coded, or embedded on the Medicare card issued to an individual entitled to receive such Medicare related benefits.

In rolling out the transition to alternative unique numerical identifiers, the Secretary of Health and Human Services will have four years from the enactment of this Act to complete full card issuance to new Medicare recipients and full current card re-issuance to all existing Medicare recipients. The Act further calls for a transition process which involves the least amount of disruption to, as well as necessary assistance for, Medicare beneficiaries and health care providers. The Act also includes a provision requiring the offering of assistance through toll-free telephone numbers and provider outreach.

With a reported 4,500 seniors enrolling in Medicare every day, and an already existing 50 million benefit cards in circulation, Congress has provided for 320 million dollars to be allocated over four years to allow for successful implementation.

(Medicare Access and CHIP Reauthorization Act of 2015 – Appendix E)

DEPARTMENT OF THE ARMY – PAMPHLET 600-8-14

In a further attempt to reduce the use and reliance of SSNs as a primary identifier, the Department of the Army released Pamphlet 600-8-14. Pamphlet 600-8-14 dictates that going forward all SSNs on identification tags shall be replaced with a 10-digit Department of Defense, DOD Service ID Number.

As set out within the Pamphlet, all active duty Army, Army National Guard, Army National Guard of the United States, U.S. Army Reserve, and other designated Department of the Army civilian personnel, will receive updated identification tags as soon as possible after entry on active duty, initial active duty for training, or assignment to a Reserve Component Unit. For all existing personnel, identification tags currently in use will be changed only upon specific request by the individual wearing the ID tags through their unit's adjutant. As discussed further within the Pamphlet, only a limited number of justifications for reissuance will be permitted.

The Task Force will monitor each of these significant undertakings as each have noteworthy benefits to Illinois Medicare recipients and Illinois military and service personnel alike.

(Department of the Army – Pamphlet 600-8-14 – Appendix F)

TASK FORCE APPOINTMENTS & UPDATES

The Task Force awaits year 2015 appointment and confirmations for the following currently vacant membership seats:

- Two members representing the House of Representatives, appointed by the Minority Leader of the House
- One of the two members representing the Senate, appointed by the President of the Senate
- One of the two members representing the Senate, appointed by the Minority Leader of the Senate
- One member representing the Office of the Governor
- One member representing the Department of Revenue
- One member representing the Department of State Police
- One member representing the Department on Aging
- One member representing the Board of Higher Education
- One member appointed by the Secretary of Human Services

CONCLUSION

Identity-Protection Policies at local and state government agencies throughout Illinois continue to be implemented according to the requirements of the Identity Protection Act. Additionally, proposed expansions to the Illinois Personal Information Protection Act, if passed, will significantly expand the security and safeguards to Illinois residents' SSNs as well as other sensitive personal information. Over the course of the last year the Task Force has continued to monitor state-level discussions regarding further contemplated protections for Illinois individuals' Social Security numbers and has also monitored federal bills which seek to both overlap and expand existing state laws involving the protections and restrictions associated with using Social Security numbers as individual identifiers. With the newly formed CIO Council Cybersecurity Working Group focusing on encrypting existing personally identifiable

information, along with the significant expansions to federal law regarding the reduction of using SSNs as primary identifiers, Illinois has shown itself as a front runner in protecting its residents' sensitive information. Overall, the Task Force will continue to monitor state and federal activities, recommending updates as needed and will continue to work together with all stakeholders to identify the best ways to protect SSNs in public records and limit the use of SSNs as internal identifiers.

APPENDIX A – Template Identity-Protection Policy

[AGENCY] IDENTITY-PROTECTION POLICY

The [AGENCY] adopts this Identity-Protection Policy pursuant to the Identity Protection Act. 5 ILCS 179/1 *et seq.* The Identity Protection Act requires each local and State government agency to draft, approve, and implement an Identity-Protection Policy to ensure the confidentiality and integrity of Social Security numbers agencies collect, maintain, and use. It is important to safeguard Social Security numbers (SSNs) against unauthorized access because SSNs can be used to facilitate identity theft. One way to better protect SSNs is to limit the widespread dissemination of those numbers. The Identity Protection Act was passed in part to require local and State government agencies to assess their personal information collection practices, and make necessary changes to those practices to ensure confidentiality.

Social Security Number Protections Pursuant to Law

Whenever an individual is asked to provide this Office with a SSN, [AGENCY] shall provide that individual with a statement of the purpose or purposes for which the [AGENCY] is collecting and using the Social Security number. The [AGENCY] shall also provide the statement of purpose upon request. That Statement of Purpose is attached to this Policy.

The [AGENCY] shall not:

- 1) Publicly post or publicly display in any manner an individual's Social Security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise intentionally make available to the general public.
- 2) Print an individual's Social Security number on any card required for the individual to access products or services provided by the person or entity.
- 3) Require an individual to transmit a Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted.
- 4) Print an individual's Social Security number on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless State or federal law requires the Social Security number to be on the document to be mailed. SSNs may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the Social Security number. A Social Security number that is permissibly mailed will not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.

In addition, the [AGENCY] shall not¹:

¹ These prohibitions do not apply in the following circumstances:

(1) The disclosure of Social Security numbers to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and

- 1) Collect, use, or disclose a Social Security number from an individual, unless:
 - i. required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the Social Security number is otherwise necessary for the performance of the [AGENCY]'s duties and responsibilities;
 - ii. the need and purpose for the Social Security number is documented before collection of the Social Security number; and
 - iii. the Social Security number collected is relevant to the documented need and purpose.
- 2) Require an individual to use his or her Social Security number to access an Internet website.
- 3) Use the Social Security number for any purpose other than the purpose for which it was collected.

Requirement to Redact Social Security Numbers

The [AGENCY] shall comply with the provisions of any other State law with respect to allowing the public inspection and copying of information or documents containing all or any portion of an individual's Social Security number. The [AGENCY] shall redact social security numbers from the information or documents before allowing the public inspection or copying of the information or documents.

When collecting Social Security numbers, the [AGENCY] shall request each SSN in a manner that makes the SSN easily redacted if required to be released as part of a public records request. "Redact" means to alter or truncate data so that no more than five sequential digits of a Social Security number are accessible as part of personal information.

Employee Access to Social Security Numbers

Only employees who are required to use or handle information or documents that contain SSNs will have access. All employees who have access to SSNs are trained to protect the confidentiality of SSNs.

responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how the requirements imposed under this Act on a governmental entity to protect an individual's Social Security number will be achieved.

(2) The disclosure of Social Security numbers pursuant to a court order, warrant, or subpoena.

(3) The collection, use, or disclosure of Social Security numbers in order to ensure the safety of: State and local government employees; persons committed to correctional facilities, local jails, and other law-enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a State or local government agency facility.

(4) The collection, use, or disclosure of Social Security numbers for internal verification or administrative purposes.

(5) The disclosure of Social Security numbers by a State agency to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.

(6) The collection or use of Social Security numbers to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.

APPENDIX B – Template Statement of Purpose(s)

What does the [AGENCY] do with your Social Security Number?

Statement of Purpose for Collection of Social Security Numbers
Identity-Protection Policy

The Identity Protection Act, 5 ILCS 179/1 *et seq.*, requires each local and State government agency to draft, approve, and implement an Identity-Protection Policy that includes a statement of the purpose or purposes for which the agency is collecting and using an individual's Social Security number (SSN). This statement of purpose is being provided to you because you have been asked by the [AGENCY] to provide your SSN or because you requested a copy of this statement.

Why do we collect your Social Security number?

You are being asked for your SSN for one or more of the following reasons:
[THE FOLLOWING PURPOSES MAY NOT APPLY; IDENTIFY PURPOSES
APPROPRIATE FOR YOUR AGENCY]

- Complaint mediation or investigation;
- Crime victim compensation;
- Vendor services, such as executing contracts and/or billing;
- Law enforcement investigation;
- Child support collection;
- Internal verification;
- Administrative services; and/or
- Other: _____

What do we do with your Social Security number?

- We will only use your SSN for the purpose for which it was collected.
- We will not:
 - Sell, lease, loan, trade, or rent your SSN to a third party for any purpose;
 - Publicly post or publicly display your SSN;
 - Print your SSN on any card required for you to access our services;
 - Require you to transmit your SSN over the Internet, unless the connection is secure or your SSN is encrypted; or
 - Print your SSN on any materials that are mailed to you, unless State or Federal law requires that number to be on documents mailed to you, or unless we are confirming the accuracy of your SSN.

Questions or Complaints about this Statement of Purpose

Write to the [AGENCY]:

[CONTACT INFORMATION]

APPENDIX C – HB1260 – PASSED THIRD READING, DECEMBER 02, 2015

HB1260 Engrossed

LRB099 05116 JLS 25145 b

1 AN ACT concerning business.

2 Be it enacted by the People of the State of Illinois,
3 represented in the General Assembly:

4 Section 5. The Personal Information Protection Act is
5 amended by changing Sections 5, 10, and 12 and adding Sections
6 45 and 50 as follows:

7 (815 ILCS 530/5)

8 Sec. 5. Definitions. In this Act:

9 "Data Collector" may include, but is not limited to,
10 government agencies, public and private universities,
11 privately and publicly held corporations, financial
12 institutions, retail operators, and any other entity that, for
13 any purpose, handles, collects, disseminates, or otherwise
14 deals with nonpublic personal information.

15 "Breach of the security of the system data" or "breach"
16 means unauthorized acquisition of computerized data that
17 compromises the security, confidentiality, or integrity of
18 personal information maintained by the data collector. "Breach
19 of the security of the system data" does not include good faith
20 acquisition of personal information by an employee or agent of
21 the data collector for a legitimate purpose of the data
22 collector, provided that the personal information is not used
23 for a purpose unrelated to the data collector's business or

HB1260 Engrossed

- 2 -

LRB099 05116 JLS 25145 b

1 subject to further unauthorized disclosure.

2 "Health insurance information" means an individual's
3 health insurance policy number or subscriber identification
4 number, any unique identifier used by a health insurer to
5 identify the individual, or any medical information in an
6 individual's health insurance application and claims history,
7 including any appeals records.

8 "Medical information" means any information regarding an
9 individual's medical history, mental or physical condition, or

10 medical treatment or diagnosis by a healthcare professional,
11 including such information provided to a website or mobile
12 application.

13 "Personal information" means either of the following:

14 (1) an individual's first name or first initial and
15 last name in combination with any one or more of the
16 following data elements, when either the name or the data
17 elements are not encrypted or redacted or are encrypted or
18 redacted but the keys to unencrypt or unredact or otherwise
19 read the name or data elements have been acquired without
20 authorization through the breach of security:

21 (A) ~~(1)~~ Social Security number.

22 (B) ~~(2)~~ Driver's license number or State
23 identification card number.

24 (C) ~~(3)~~ Account number or credit or debit card
25 number, or an account number or credit card number in
26 combination with any required security code, access

HB1260 Engrossed

- 3 -

LRB099 05116 JLS 25145 b

1 code, or password that would permit access to an
2 individual's financial account.

3 (D) Medical information.

4 (E) Health insurance information.

5 (F) Unique biometric data generated from
6 measurements or technical analysis of human body
7 characteristics used by the owner or licensee to
8 authenticate an individual, such as a fingerprint,
9 retina or iris image, or other unique physical
10 representation or digital representation of biometric
11 data.

12 (2) user name or email address, in combination with a
13 password or security question and answer that would permit
14 access to an online account, when either the user name or
15 email address or password or security question and answer
16 are not encrypted or redacted or are encrypted or redacted
17 but the keys to unencrypt or unredact or otherwise read the
18 data elements have been obtained through the breach of
19 security.

20 "Personal information" does not include publicly available
21 information that is lawfully made available to the general

22 public from federal, State, or local government records.

23 (Source: P.A. 97-483, eff. 1-1-12.)

24 (815 ILCS 530/10)

25 Sec. 10. Notice of Breach.

HB1260 Engrossed

- 4 -

LRB099 05116 JLS 25145 b

1 (a) Any data collector that owns or licenses personal
2 information concerning an Illinois resident shall notify the
3 resident at no charge that there has been a breach of the
4 security of the system data following discovery or notification
5 of the breach. The disclosure notification shall be made in the
6 most expedient time possible and without unreasonable delay,
7 consistent with any measures necessary to determine the scope
8 of the breach and restore the reasonable integrity, security,
9 and confidentiality of the data system. The disclosure
10 notification to an Illinois resident shall include, but need
11 not be limited to, information as follows:

12 (1) With respect to personal information as defined in
13 Section 5 in paragraph (1) of the definition of "personal
14 information":

15 (A) (i) the toll-free numbers and addresses for
16 consumer reporting agencies; 7

17 (B) (ii) the toll-free number, address, and
18 website address for the Federal Trade Commission; 7 and

19 (C) (iii) a statement that the individual can
20 obtain information from these sources about fraud
21 alerts and security freezes.

22 The notification shall not, however, include information
23 concerning the number of Illinois residents affected by the
24 breach.

25 (2) With respect to personal information defined in
26 Section 5 in paragraph (2) of the definition of "personal

HB1260 Engrossed

- 5 -

LRB099 05116 JLS 25145 b

1 information", notice may be provided in electronic or other
2 form directing the Illinois resident whose personal
3 information has been breached to promptly change his or her
4 user name or password and security question or answer, as

5 applicable, or to take other steps appropriate to protect
6 all online accounts for which the resident uses the same
7 user name or email address and password or security
8 question and answer.

9 (b) Any data collector that maintains or stores, but does
10 not own or license, computerized data that includes personal
11 information that the data collector does not own or license
12 shall notify the owner or licensee of the information of any
13 breach of the security of the data immediately following
14 discovery, if the personal information was, or is reasonably
15 believed to have been, acquired by an unauthorized person. In
16 addition to providing such notification to the owner or
17 licensee, the data collector shall cooperate with the owner or
18 licensee in matters relating to the breach. That cooperation
19 shall include, but need not be limited to, (i) informing the
20 owner or licensee of the breach, including giving notice of the
21 date or approximate date of the breach and the nature of the
22 breach, and (ii) informing the owner or licensee of any steps
23 the data collector has taken or plans to take relating to the
24 breach. The data collector's cooperation shall not, however, be
25 deemed to require either the disclosure of confidential
26 business information or trade secrets or the notification of an

1 Illinois resident who may have been affected by the breach.

2 (b-5) The notification to an Illinois resident required by
3 subsection (a) of this Section may be delayed if an appropriate
4 law enforcement agency determines that notification will
5 interfere with a criminal investigation and provides the data
6 collector with a written request for the delay. However, the
7 data collector must notify the Illinois resident as soon as
8 notification will no longer interfere with the investigation.

9 (c) For purposes of this Section, notice to consumers may
10 be provided by one of the following methods:

11 (1) written notice;

12 (2) electronic notice, if the notice provided is
13 consistent with the provisions regarding electronic
14 records and signatures for notices legally required to be
15 in writing as set forth in Section 7001 of Title 15 of the
16 United States Code; or

17 (3) substitute notice, if the data collector

18 demonstrates that the cost of providing notice would exceed
19 \$250,000 or that the affected class of subject persons to
20 be notified exceeds 500,000, or the data collector does not
21 have sufficient contact information. Substitute notice
22 shall consist of all of the following: (i) email notice if
23 the data collector has an email address for the subject
24 persons; (ii) conspicuous posting of the notice on the data
25 collector's web site page if the data collector maintains
26 one; and (iii) notification to major statewide media or, if

HB1260 Engrossed

- 7 -

LRB099 05116 JLS 25145 b

1 the breach impacts residents in one geographic area, to
2 prominent local media in areas where affected individuals
3 are likely to reside if such notice is reasonably
4 calculated to give actual notice to persons whom notice is
5 required.

6 (d) Notwithstanding any other subsection in this Section, a
7 data collector that maintains its own notification procedures
8 as part of an information security policy for the treatment of
9 personal information and is otherwise consistent with the
10 timing requirements of this Act, shall be deemed in compliance
11 with the notification requirements of this Section if the data
12 collector notifies subject persons in accordance with its
13 policies in the event of a breach of the security of the system
14 data.

15 (Source: P A. 97-483, eff. 1-1-12.)

16 (815 ILCS 530/12)

17 Sec. 12. Notice of breach; State agency.

18 (a) Any State agency that collects personal information
19 concerning an Illinois resident shall notify the resident at no
20 charge that there has been a breach of the security of the
21 system data or written material following discovery or
22 notification of the breach. The disclosure notification shall
23 be made in the most expedient time possible and without
24 unreasonable delay, consistent with any measures necessary to
25 determine the scope of the breach and restore the reasonable

HB1260 Engrossed

- 8 -

LRB099 05116 JLS 25145 b

1 integrity, security, and confidentiality of the data system.
2 The disclosure notification to an Illinois resident shall
3 include, but need not be limited to information as follows:

4 (1) With respect to personal information defined in
5 Section 5 in paragraph (1) of the definition of "personal
6 information": 7

7 (i) the toll-free numbers and addresses for
8 consumer reporting agencies; 7

9 (ii) the toll-free number, address, and website
10 address for the Federal Trade Commission; 7 and

11 (iii) a statement that the individual can obtain
12 information from these sources about fraud alerts and
13 security freezes.

14 (2) With respect to personal information as defined in
15 Section 5 in paragraph (2) of the definition of "personal
16 information", notice may be provided in electronic or other
17 form directing the Illinois resident whose personal
18 information has been breached to promptly change his or her
19 user name or password and security question or answer, as
20 applicable, or to take other steps appropriate to protect
21 all online accounts for which the resident uses the same
22 user name or email address and password or security
23 question and answer.

24 The notification shall not, however, include information
25 concerning the number of Illinois residents affected by the
26 breach.

1 (a-5) The notification to an Illinois resident required by
2 subsection (a) of this Section may be delayed if an appropriate
3 law enforcement agency determines that notification will
4 interfere with a criminal investigation and provides the State
5 agency with a written request for the delay. However, the State
6 agency must notify the Illinois resident as soon as
7 notification will no longer interfere with the investigation.

8 (b) For purposes of this Section, notice to residents may
9 be provided by one of the following methods:

10 (1) written notice;

11 (2) electronic notice, if the notice provided is
12 consistent with the provisions regarding electronic
13 records and signatures for notices legally required to be

14 in writing as set forth in Section 7001 of Title 15 of the
15 United States Code; or
16 (3) substitute notice, if the State agency
17 demonstrates that the cost of providing notice would exceed
18 \$250,000 or that the affected class of subject persons to
19 be notified exceeds 500,000, or the State agency does not
20 have sufficient contact information. Substitute notice
21 shall consist of all of the following: (i) email notice if
22 the State agency has an email address for the subject
23 persons; (ii) conspicuous posting of the notice on the
24 State agency's web site page if the State agency maintains
25 one; and (iii) notification to major statewide media.
26 (c) Notwithstanding subsection (b), a State agency that

HB1260 Engrossed

- 10 -

LRB099 05116 JLS 25145 b

1 maintains its own notification procedures as part of an
2 information security policy for the treatment of personal
3 information and is otherwise consistent with the timing
4 requirements of this Act shall be deemed in compliance with the
5 notification requirements of this Section if the State agency
6 notifies subject persons in accordance with its policies in the
7 event of a breach of the security of the system data or written
8 material.

9 (d) If a State agency is required to notify more than 1,000
10 persons of a breach of security pursuant to this Section, the
11 State agency shall also notify, without unreasonable delay, all
12 consumer reporting agencies that compile and maintain files on
13 consumers on a nationwide basis, as defined by 15 U.S.C.
14 Section 1681a(p), of the timing, distribution, and content of
15 the notices. Nothing in this subsection (d) shall be construed
16 to require the State agency to provide to the consumer
17 reporting agency the names or other personal identifying
18 information of breach notice recipients.

19 (e) Notice to Attorney General. Any State agency that
20 suffers a single breach of the security of the data concerning
21 the personal information of more than 250 Illinois residents
22 shall provide notice to the Attorney General of the breach,
23 including:

24 (A) The types of personal information compromised in
25 the breach.

26 (B) The number of Illinois residents affected by such

1 incident at the time of notification.

2 (C) Any steps the State agency has taken or plans to
3 take relating to notification of the breach to consumers.

4 (D) The date and timeframe of the breach, if known at
5 the time notification is provided.

6 Such notification must be made within 45 days of the State
7 agency's discovery of the security breach or when the State
8 agency provides any notice to consumers required by this
9 Section, whichever is sooner, unless the State agency has good
10 cause for reasonable delay to determine the scope of the breach
11 and restore the integrity, security, and confidentiality of the
12 data system, or when law enforcement requests in writing to
13 withhold disclosure of some or all of the information required
14 in the notification under this Section. If the date or
15 timeframe of the breach is unknown at the time the notice is
16 sent to the Attorney General, the State agency shall send the
17 Attorney General the date or timeframe of the breach as soon as
18 possible.

19 (Source: P.A. 97-483, eff. 1-1-12.)

20 (815 ILCS 530/45 new)

21 Sec. 45. Data security.

22 (a) A data collector that owns or licenses, or maintains or
23 stores but does not own or license, records that contain
24 personal information concerning an Illinois resident shall
25 implement and maintain reasonable security measures to protect

1 those records from unauthorized access, acquisition,
2 destruction, use, modification, or disclosure.

3 (b) A contract for the disclosure of personal information
4 concerning an Illinois resident that is maintained by a data
5 collector must include a provision requiring the person to whom
6 the information is disclosed to implement and maintain
7 reasonable security measures to protect those records from
8 unauthorized access, acquisition, destruction, use,
9 modification, or disclosure.

10 (c) If a state or federal law requires a data collector to
11 provide greater protection to records that contain personal
12 information concerning an Illinois resident that are
13 maintained by the data collector and the data collector is in
14 compliance with the provisions of that state or federal law,
15 the data collector shall be deemed to be in compliance with the
16 provisions of this Section.

17 (d) A data collector that is subject to and in compliance
18 with the standards established pursuant to Section 501(b) of
19 the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801,
20 shall be deemed to be in compliance with the provisions of this
21 Section.

22 (815 ILCS 530/50 new)

23 Sec. 50. Entities subject to the federal Health Insurance
24 Portability and Accountability Act of 1996. Any covered entity
25 or business associate that is subject to and in compliance with

HB1260 Engrossed

- 13 -

LRB099 05116 JLS 25145 b

1 the privacy and security standards for the protection of
2 electronic health information established pursuant to the
3 federal Health Insurance Portability and Accountability Act of
4 1996 and the Health Information Technology for Economic and
5 Clinical Health Act shall be deemed to be in compliance with
6 the provisions of this Act, provided that any covered entity or
7 business associate required to provide notification of a breach
8 to the Secretary of Health and Human Services pursuant to the
9 Health Information Technology for Economic and Clinical Health
10 Act also provides such notification to the Attorney General
11 within 5 business days of notifying the Secretary.

**APPENDIX D—ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES
ACT (815 ILCS 505/1 ET SEQ.) SECTIONS 2QQ & 2RR**

(815 ILCS 505/2QQ)

Sec. 2QQ. Insurance cards; social security number.

(a) As used in this Section, "insurance card" means a card that a person or entity provides to an individual so that the individual may present the card to establish the eligibility of the individual or his or her dependents to receive health, dental, optical, or accident insurance benefits, prescription drug benefits, or benefits under a managed care plan or a plan provided by a health maintenance organization, a health services plan corporation, or a similar entity.

(b) A person or entity may not print an individual's social security number on an insurance card. A person or entity that provides an insurance card must print on the card an identification number unique to the holder of the card in the format prescribed by Section 15 of the Uniform Prescription Drug Information Card Act.

(c) An insurance card issued to an individual before the effective date of this amendatory Act of the 93rd General Assembly that does not comply with subsection (b) must be replaced by January 1, 2006 with an insurance card that complies with subsection (b) if the individual's eligibility for benefits continues after the effective date of this amendatory Act of the 93rd General Assembly.

(d) A violation of this Section constitutes an unlawful practice within the meaning of this Act.

(Source: P.A. 95-331, eff. 8-21-07.)

(815 ILCS 505/2RR)

Sec. 2RR. Use of Social Security numbers.

(a) Except as otherwise provided in this Section, a person may not do any of the following:

(1) Publicly post or publicly display in any manner an individual's social security number. As used in this Section, "publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public.

(2) Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity, or on a wristband or on the outside of any file associated with the products or services provided by the person or entity; however, a person or entity that provides an insurance card must print on the card an identification number unique to the holder of the card in the format prescribed by Section 15 of the Uniform Prescription Drug Information Card Act.

(3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.

(4) Require an individual to use his or her social security number to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site.

(5) Print an individual's social security number on any materials that are mailed to the individual, unless State or federal law requires the social security number to be on the document to be mailed. Notwithstanding any provision in this Section to the contrary, social security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the social security number. A social security number that may permissibly be mailed under this Section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope or visible without the envelope having been opened.

(b) A person that used, before July 1, 2005, an individual's social security number in a manner inconsistent with subsection (a) may continue using that individual's social security number in the same manner on or after July 1, 2005 if all of the following conditions are met:

(1) The use of the social security number is continuous. If the use is stopped for any reason, subsection (a) shall apply.

(2) The individual is provided an annual disclosure that informs the individual that he or she has the right to stop the use of his or her social security number in a manner prohibited by subsection (a).

A written request by an individual to stop the use of his or her social security number in a manner prohibited by subsection (a) shall be implemented within 30 days of the receipt of the request. There shall be no fee or charge for implementing the request. A person shall not deny services to an individual because the individual makes such a written request.

(c) This Section does not apply to the collection, use, or release of a social security number as required by State or federal law or the use of a social security number for internal verification or administrative purposes. This Section does not apply to the collection, use, or release of a social security number by the State, a subdivision of the State, or an individual in the employ of the State or a subdivision of the State in connection with his or her official duties.

(d) This Section does not apply to documents that are recorded or required to be open to the public under State or federal law, applicable case law, Supreme Court Rule, or the Constitution of the State of Illinois.

(e) If a federal law takes effect requiring the United States Department of Health and Human Services to establish a

national unique patient health identifier program, any person who complies with the federal law shall be deemed to be in compliance with this Section.

(f) A person may not encode or embed a social security number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the social security number as required by this Section.

(g) Any person who violates this Section commits an unlawful practice within the meaning of this Act.
(Source: P.A. 97-139, eff. 1-1-12.)

APPENDIX E – MEDICARE ACCESS AND CHIP REAUTHORIZATION ACT OF 2015

TITLE V—MISCELLANEOUS Subtitle A—Protecting the Integrity of Medicare

SEC. 501. PROHIBITION OF INCLUSION OF SOCIAL SECURITY ACCOUNT NUMBERS ON MEDICARE CARDS.

(a) IN GENERAL.—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)) is amended—

(1) by moving clause (x), as added by section 1414(a)(2) of the Patient Protection and Affordable Care Act, 6 ems to the left;

(2) by redesignating clause (x), as added by section 2(a)(1) of the Social Security Number Protection Act of 2010, and clause (xi) as clauses (xi) and (xii), respectively; and

(3) by adding at the end the following new clause:

“(xiii) The Secretary of Health and Human Services, in consultation with the Commissioner of Social Security, shall establish costeffective procedures to ensure that a Social Security account number (or derivative thereof) is not displayed, coded, or embedded on the Medicare card issued to an individual who is entitled to benefits under part A of title XVIII or enrolled under part B of title XVIII and that any other identifier displayed on such card is not identifiable as a Social Security account number (or derivative thereof).”.

(b) IMPLEMENTATION.—In implementing clause (xiii) of section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)), as H. R. 2—78

added by subsection (a)(3), the Secretary of Health and Human Services shall do the following:

(1) IN GENERAL.—Establish a cost-effective process that involves the least amount of disruption to, as well as necessary assistance for, Medicare beneficiaries and health care providers, such as a process that provides such beneficiaries with access to assistance through a toll-free telephone number and provides outreach to providers.

(2) CONSIDERATION OF MEDICARE BENEFICIARY IDENTIFIED.—Consider implementing a process, similar to the process involving Railroad Retirement Board beneficiaries, under which a Medicare beneficiary identifier which is not a Social Security account number (or derivative thereof) is used external to the Department of Health and Human Services and is convertible over to a Social Security account number (or derivative thereof) for use internal to such Department and the Social Security Administration.

(c) FUNDING FOR IMPLEMENTATION.—For purposes of implementing

the provisions of and the amendments made by this section, the Secretary of Health and Human Services shall provide for the following transfers from the Federal Hospital Insurance Trust Fund under section 1817 of the Social Security Act (42 U.S.C. 1395i) and from the Federal Supplementary Medical Insurance Trust Fund established under section 1841 of such Act (42 U.S.C. 1395t), in such proportions as the Secretary determines appropriate:

(1) To the Centers for Medicare & Medicaid Program Management Account, transfers of the following amounts:

(A) For fiscal year 2015, \$65,000,000, to be made available through fiscal year 2018.

(B) For each of fiscal years 2016 and 2017, \$53,000,000, to be made available through fiscal year 2018.

(C) For fiscal year 2018, \$48,000,000, to be made available until expended.

(2) To the Social Security Administration Limitation on Administration Account, transfers of the following amounts:

(A) For fiscal year 2015, \$27,000,000, to be made available through fiscal year 2018.

(B) For each of fiscal years 2016 and 2017, \$22,000,000, to be made available through fiscal year 2018.

(C) For fiscal year 2018, \$27,000,000, to be made available until expended.

(3) To the Railroad Retirement Board Limitation on Administration Account, the following amount:

(A) For fiscal year 2015, \$3,000,000, to be made available until expended.

(d) EFFECTIVE DATE.—

(1) IN GENERAL.—Clause (xiii) of section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)), as added by subsection (a)(3), shall apply with respect to Medicare cards issued on and after an effective date specified by the Secretary of Health and Human Services, but in no case shall such effective date be later than the date that is four years after the date of the enactment of this Act.

(2) REISSUANCE.—The Secretary shall provide for the reissuance of Medicare cards that comply with the requirements of such clause not later than four years after the effective date specified by the Secretary under paragraph (1).

APPENDIX F – DEPARTMENT OF THE ARMY – PAMPHLET 600-8-14

**Headquarters
Department of the Army
Washington, DC
30 November 2015
UNCLASSIFIED**

SUMMARY

DA PAM 600-8-14

Army Identification Tags

This new pamphlet, dated 30 November 2015--

o Provides the procedures for the standardization of all Army identification

tags for the U.S. Army, Army National Guard, U.S. Army Reserve Soldiers,

Department of the Army civilians overseas, and other authorized civilian

personnel, in accordance with AR 600-8-14 (throughout).

o Discusses the issuance of, and specifications for, Army identification tags

for designated personnel (throughout).

**Headquarters
Department of the Army
Washington, DC
30 November 2015
Personnel-General
Army Identification Tags
Department of the Army
Pamphlet 600-8-14
History.**

This publication is a new Department of the Army pamphlet.

Summary. This pamphlet establishes the procedures for standardizing all Army identification tags throughout the Army.

Applicability. This pamphlet applies to the active Army, Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to Department

of the Army civilians overseas, and other authorized civilian personnel.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, *page 1*

Purpose • 1-1, *page 1*

References • 1-2, *page 1*

Explanation of abbreviations and terms • 1-3, *page 1*

Designated publishing roles • 1-4, *page 1*

Overview • 1-5, *page 1*

Chapter 2

Identification Tags, *page 1*

Identification tag issuance • 2-1, *page 1*

Specifications required for identification tags and embossing • 2-2, *page 1*

Chapter 3

Application Process, *page 2*

Rules for processing applications for identification tags • 3-1, *page 2*

Processing applications for identification tags • 3-2, *page 2*

Steps for ordering and issuing identification tags • 3-3, *page 2*

Rules for replacing identification tags • 3-4, *page 3*

DA PAM 600-8-14 • 30 November 2015 i

UNCLASSIFIED

Contents—Continued

Appendix A. References, *page 4*

Table List

Table 3-1: Steps for processing identification tag applications, *page 2*

Figure List

Figure 2-1: Sample identification tag with single last name line entry, *page 2*

Figure 2-2: Sample identification tag with extended last name entry, *page 2*

Glossary

ii DA PAM 600-8-14 • 30 November 2015

Chapter 1

Introduction

1-1. Purpose

This pamphlet prescribes procedural guidance for the issuance of identification (ID) tags to personnel of the United

States Army, Army National Guard, Army National Guard of the United States and United States Army Reserve

Soldier, Department of the Army (DA) civilians overseas, and other authorized civilian personnel.

1-2. References

See appendix A.

1-3. Explanation of abbreviations and terms

See glossary.

1-4. Designated publishing roles

a. The Deputy Chief of Staff, G-1, through the Commander, U.S. Army Human Resources Command provides

procedural guidance oversight for the management and issuance of Army ID tags.

b. Commanders at all levels—

(1) Process and ensure all requests for Army ID tags are in compliance with this pamphlet.

(2) Verify the accuracy of personnel data on the Army ID tags and enforce the wear of Army ID tags in accordance

with Army Regulation (AR) 670-1.

1-5. Overview

a. This pamphlet provides procedural guidance for the issuance of ID tags, in accordance with AR 600-8-14.

b. Operating instructions for issuing Army installation ID tag machines may vary by manufacturer; however, uniformity of the ID tags must be in compliance with this pamphlet and other regulatory guidance.

Chapter 2

Identification Tags

2-1. Identification tag issuance

a. Every Soldier will be issued two ID tags as soon as possible after entry on active duty, initial active duty for

training, or assignment to a Reserve Component unit.

b. Contracted Senior Reserve Officer Training Corps cadets are authorized issuance of two ID tags.

c. Two ID tags may be issued upon request to the following personnel under the jurisdiction of an overseas commander:

(1) DA civilians serving in an overseas location.

(2) Dependents of U.S. Army personnel. (Dependents who are not citizens may be furnished ID tags upon request.

The phrase “Depn of US Natl” will be shown on the ID tags.)

(3) Other U.S. Nationals.

d. The issuance of medical warning tags which serve as a means of rapid recognition of selection health problems is

covered under AR 40-66.

e. Identification tags are used for identification, casualty reporting, and graves-registration purposes. Each Soldier

must have two identification tags and the information contained on the tags must be current.

2-2. Specifications required for identification tags and embossing

a. All ID tags will be composed of Monel or other adopter metal, approximately two inches long by 1 1/8 inches

wide, and about 0.025 inch thick, the corners rounded and the edges smooth.

b. ID tags are limited to five lines of text and 18 characters per line for embossing.

c. All ID tags will have the following information embossed on them:

(1) *Line 1.* Name of the wearer: Enter last name, first name, middle initial. (If the full name cannot be embossed on

the first line, put the last name on line 1, place the first name and middle initial on line 2.

Subsequent entries shift

down one line each. If a U.S. National, the name will be the same as shown on passport or ID card.)

(2) *Line 2.* (Service Number) Department of Defense (DOD) ID number (10 digits, no hyphens) (The Social

Security number has been replaced by the DOD ID, in accordance with DODI 1000.30.)

(3) *Line 3.* Blood group and type. Record as "A", "B", "AB", or "O", followed by "POS" OR "NEG." Do not use

plus (+) or minus (-) signs to record the blood type. If the blood type is incorrect the Soldier must update the medical

system of record.

DA PAM 600-8-14 • 30 November 2015 1

(4) *Line 4.* Religious preference. Spell this out when possible (the example shown in figures 2-1 and 2-2 is used to

set forth a pattern for guidance). If the religious preference is incorrect, the Soldier must update the personnel system

of record.

Smith, John D.

000000000

A POS

Baptist

Figure 2-1. Sample identification tag with single last name line entry

Smith-Jones

John D.

000000000

A POS

Baptist

Figure 2-2. Sample identification tag with extended last name entry

Chapter 3

Application Process

3-1. Rules for processing applications for identification tags

a. Individuals may request ID tags through their brigade or battalion adjutant to the issuing office.

b. The issuing office must ensure that the applicant is an authorized recipient of the embossed ID tags.

3-2. Processing applications for identification tags

Processing request for ID tags will normally be completed within 10 workdays.

3-3. Steps for ordering and issuing identification tags

The steps for ordering and issuing ID tags are outlined in table 3-1, and embossing guidance is provided in paragraph

2-3c.

Table 3-1

Steps for processing identification tag applications

Step Work center Required action

1 Unit or individual Request ID tags

2 Unit Verify data accuracy

3 Issuing office Verify data accuracy (name spelling, DOD ID, blood type and religion) in the personnel system; emboss two ID tags

4 Individual Verify data accuracy on the embossed ID tags

2 DA PAM 600-8-14 • 30 November 2015

3-4. Rules for replacing identification tags

a. Identification tags currently in use will be changed only upon specific request by the individual wearing the ID

tags through their unit's adjutant. Reasons to replace ID tags include the following:

(1) Legal name changes.

(2) Incorrect information embossed on ID tags

(3) Lost ID tags.

b. Validation of changed marital status and legal name changes are the responsibility of the individual's unit adjutant.

DA PAM 600-8-14 • 30 November 2015 3

Appendix A

References

Section I

Required Publications

AR 40-66

Medical Record Administration and Health Care Documentation (Cited in para 2-1d.)

AR 600-8-14

Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible

Personnel (Cited in para 1-5a.)

AR 638-2

Army Mortuary Affairs Program (Cited in para 2-2b.)

AR 670-1

Wear and Appearance of Army Uniforms and Insignia (Cited in para 1-4b(2).)

DODI 1000.30

Reduction of Social Security Number Use Within DOD (Cited in para 2-2c(2).)

Section II

Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this

publication. Unless otherwise stated, all publications are available at <http://www.apd.army.mil/>.

AR 11-2

Managers Internal Control Program

AR 25-30

The Army Publishing Program

AR 25-50

Preparing and Managing Correspondence

AR 600-8-104

Army Military Human Resource Records Management

AR 638-8

Army Casualty Program

DA Pam 600-8

Military Human Resources Management Administrative Procedures

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA Forms are available on the Army Publishing Directorate (APD) Web site (<http://www.apd.army.mil/>).

DA Form 2028

Recommended Changes of Publications and Blank Forms
4 DA PAM 600-8-14 • 30 November 2015

Glossary

Section I

Abbreviations

AR

Army Regulation

DA

Department of the Army

DOD

Department of Defense

ID

identification

Section II

Terms

Department of Defense Identification Number

A 10 digit unique personnel identifier (also referred to as the Electronic Data Interchange Personal Identifier (EDI-PI)) created within the Defense Enrollment Eligibility Reporting System for each person who has a direct relationship with DOD.

Monel

A group of nickel alloys and copper, with small amounts of iron, manganese, carbon, and silicon. Monel alloys are resistant to corrosion by many agents, including rapidly flowing seawater.

Emboss

The process of imprinting personnel information onto metal tags, in order to produce the prescribed Army identification tags.

Section III

Special Abbreviations and Terms

This section contains no entries.

DA PAM 600-8-14 • 30 November 2015 5

UNCLASSIFIED PIN 105828-000