STATE OF INDIANA

Mitchell E. Daniels Jr., Governor

OFFICE OF TECHNOLOGY
Karl B. Browning
Chief Information Officer

Indiana Government Center North
100 N. Senate Ave., Room N551
Indianapolis, IN 46204
(317) 232 - 3171

TO: Governor Daniels

CC: Neil Pickett

FROM: Karl B. Browning, Chief Information Officer

RE: Follow-up to December 31st Report Relating to Personal Information Systems

DATE: April 16, 2006

On December 31, 2005, in compliance with IC 4-1-6-7, I submitted a report identifying the State's systems that collect personal information. At the conclusion of that report, I committed to summarize the data collected and offer recommendations for going forward with this effort.

I. Findings & Recommendations

Finding 1: Agencies Did Not Comply with IC 4-1-6 Before this Administration

Recommendation 1: Amend IC 4-1-6 to Require the CIO to Report on Behalf of All Agencies

Though IC 4-1-6 was "on the books" since the late 1970s, agencies never complied with this statute. As detailed in my report on December 31st, it is important that they do because of the many benefits gained by knowing what information state government collects. The statute, however, requires each state agency, not the CIO, to report on these systems.

IC 4-1-6 should be amended to require the CIO to report on these systems on behalf of all state agencies. This will ensure that this important reporting requirement is complied with beyond my tenure; will demonstrate that this administration is committed to transparency and protection of personal information; and, will prevent duplication of efforts among agencies, inconsistent reporting formats, and multiple reports. Further, shifting this requirement to the CIO will meld well with IOT's efforts to ensure that each state IT system has adequate security and disaster recoverability.

Finding 2: State Police Is Not Required to Report, Yet the Inspector General Must Report

Recommendation 2: Amend IC 4-1-6 to Ensure that Any System that Is Part of a Law Enforcement Function Is Exempted

IC 4-1-6-1(d) expressly exempts the ISP. Though legislative history is not available, it is only logical that the drafters believed that law enforcement needed to collect personal information

without having to report on what they collect, as such reporting might hinder the effectiveness of law enforcement. Today, the State has additional agencies that perform law enforcement functions, such as the Attorney General's office and the OIG. Rather than attempt to identify every law enforcement agency, which will likely change over time anyway, IC 4-1-6 should define "law enforcement" and exempt reporting on systems that serve law enforcement.

Finding 3: The Schools for the Blind and Deaf Are Required to Report, though No Other Educational Institution Is So Required

Recommendation 3: Amend IC 4-1-6 to Exempt the Schools for the Blind and Deaf

IC 4-1-6-1(d) specifically exempts "the state-supported institutions of higher education." Further, though not specifically exempted, K-12 schools do not qualify as a part of *state* government; thus, the schools for the blind and deaf are the only educational institutions that fall within the purview of IC 4-1-6. These institutions operate as educational institutions, not traditional state agencies, and should probably be exempted.

Finding 4: The Separately Elected Officials Are Not Required to Report

Recommendation 4: Amend IC 4-1-6 to Include Separately Elected Officials

IC 4-1-6-1(d) specifically exempts the five separately elected officials. The offices/departments of these officials operate just like any other state agency and collect personal information. For example, the Auditor of State collects social security numbers in its payment systems. Moreover, many of the separately elected officials' systems share data with other state agencies' systems. There appears to be no reason to exempt these officials from the reporting requirement.

Finding 5: The Terms "Personal Information" and "Personal Information System" Are Too Broadly Defined in the Statute

Recommendation 5: Amend 4-1-6 to More Clearly Define these Terms

IC 4-1-6-1(a) defines "Personal information system" as "any recordkeeping process, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject." IC 4-1-6-1(b) defines "Personal information" as "any information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual including, but not limited to, his education, financial transactions, medical history, criminal or employment records, finger and voice prints, photographs, or his presence, registration, or membership in an organization or activity or admission to an institution."

These terms were obviously broadly defined in an attempt to not arbitrarily exclude a system that collects personal information. The problem, however, is that e-mail distribution lists, contacts in Microsoft Outlook, and telephone messages written on a piece of paper, for example, all fall within the definition. These definitions could be tightened up in a way to cover what is needed, but eliminate incidental processes/systems like the above examples.

Finding 6: IC 4-1-6 Does Not Require that There Be a Central Repository for the State's Personal Information Systems

Recommendation 6: Amend 4-1-6 to Require the CIO to Maintain the Database of Personal Information Systems, Available Upon Request

IC 4-1-6 includes detailed reporting requirements on those systems which were "added or eliminated since the last report with the governor on or before December 31" but does not require that any agency keep track of the systems actually maintained from year to year. Though there are new systems and systems eliminated each year, most systems simply evolve over time. To reinforce the importance of protecting privacy and upholding transparency in state government, IC 4-1-6 should be amended to require the CIO to maintain a database of personal information systems and that database should be available to the public in accord with the Access to Public Records Act.

Finding 7: Report to General Assembly Is Due Before Report to Governor

Recommendation 7: Amend IC 4-1-6 to Require Report to the General Assembly After the Report to the Governor

IC 4-1-6-9(a), in relevant part, provides: "Under the authority of the governor, a report shall be prepared, on or before December 1 annually, advising the general assembly of the personal information systems, or parts thereof, of agencies subject to this chapter, which are recommended to be maintained on a confidential basis by specific statutory authorization because their disclosure would constitute an invasion of personal privacy and there is no compelling, demonstrable and overriding public interest in disclosure."[1] This report is due before the report to the Governor, which addresses which systems are new or have been eliminated. It seems logical that the new systems should be identified before they should be recommended to the General Assembly for statutory protection.

Finding 8: Agencies Want to Keep Information Confidential, Sometimes without Adequate Legal or Policy Assistance

Recommendation 8: Build in Enough Time between the Two Reports to Allow for Review by Policymakers and the Public Access Counselor

Some agencies will ask to keep information confidential that, if considered by others, should probably not be so protected. Agencies' requests to keep information confidential should undergo a review by the Public Access Counselor prior to submission to the General Assembly, at least to eliminate requests that are plainly covered by other laws. Moreover, there are likely to be requests that warrant consideration by higher level policymakers. The reporting requirements should build in enough time to consider such issues and should also require that the Public Access Counselor assist the CIO in meeting the requirements of IC 4-1-6-9.

[1] Last year's report is available online at http://www.in.gov/legislative/igareports/agency/reports/IOT01.pdf.

II. Conclusion

Assuming you agree with this course, I will submit our draft to your office prior to the next legislative session and work with Neil Pickett and others in your office to find support for this in the General Assembly. Please contact me if you have any questions or concerns with this course of action.

Regardless of statutory change, over the next several months my staff will continue to work on an improved process to meet the two reporting requirements. We will ask agencies to review and update the data that they submitted last year, and we will specifically target those agencies that did not respond to our efforts last year.

One final note, included in the Appendix below is a summary of the personal information systems we have identified to date.

Appendix

After a more thorough analysis of the data collected, we have identified 724 systems from 51 agencies collecting personal information. Because of the wide variety of data collected and the many different reasons for collecting the data, we decided to more generally categorize systems into seven categories: "Personally Identifiable," "Educational," "Employment," "Financial," "Health," "Law Enforcement," and "Other." The following are examples of the types of data in each of the six specific categories.

- **Personally Identifiable:** Name, Address, E-mail, Phone, Photo, Date of Birth/Death, Organizational Affiliations, Familial Relationships, Place of Birth, Drivers License Number, and Social Security Number
- **Educational:** Student ID #s, University Name, Academic Status, Certification Status, Continuing Education Participation, FAFSA Application Information, and Scholarship Awards
- **Employment:** Salary Information, Payroll Information, Professional Credentials, Military Status, Resumes, Professional License Numbers, Grievances, Disciplinary Actions, Military/Vietnam Bonus, Certification Status, and Continuing Education Participation
- **Financial:** Income Information, Bank Account Information, Loan Application Information, Property Value, Tax Withholding Level, and Credit Card Numbers
- **Health:** Insurance Claim Info, Medicare Number, Lab Results, Clinical Status, Treatments, Referrals, Counseling, Pregnancies, Insurance, Co-Infections, Death Certificate Information, Partner Notifications, and Disabilities
- **Law Enforcement:** DOC Offender Number, Criminal Background Checks, Charges, Victim Information, and Traffic Violations/Driving Record

The 724 systems were categorized into one or more of the seven different categories. The following are the total number of systems in each category. (Of the 724 systems, 262 were categorized in more than one category; thus, the numbers below add to 986, not 724.)

- Systems collecting Personally Identifiable data 530
- Systems collecting Educational data 42
- Systems collecting Employment data 113
- Systems collecting Financial data 149
- Systems collecting Health data 117
- Systems collecting Law Enforcement data 28[2]
- Systems collecting "Other" data 7

We categorized where state agencies were obtaining the data for their personal information systems: (a) directly from individual; (b) from another governmental agency; or, (c) from other public/private entities. The import of this distinction is that if the information is received directly from the individual, the individual should know he or she is providing the information. If the information is drawn from another governmental agency, the individual may know he or she provided the information but not know that it would be used for a different purpose. Finally, if the information is drawn from another public/private source, the individual is likely not to know that the information is being used by government for any purpose.

Of the agencies that identified where their data originated, the State has the following number of systems in each category.

- Directly from Individual 313
- From Another Governmental Agency 281
- From Other Public/Private Entities 89

Of the systems for which agencies identified the level of access to the system's data, the State has the following number of personal information systems in each category. (Each access level represents the minimum level of access. For example, if a system is available to the public, it is also available to every access level below it in the list.)

- Available to the Public 43
- Available to the Other Government Agencies 159
- Available to the Internal Agency Only 87
- Available to the Internal Division Only 43
- Available to the Internal Program Group Only 15
- Available to the Classified 105

[2] Since Indiana State Police is exempted from the reporting requirements of IC 4-1-6-7, this total does not include any systems from the ISP.

Finally, of the systems for which agencies identified the number of the system's records, the State has personal information systems in the following ranges.

- 0-100 63
- 101-500 123
- 501-1000 68
- 1001-3000 57
- 3001-5000 39
- 5001-10,000 44
- 10,001-25,000 52
- 25,001-50,000 71
- 50,001-100,00 32
- 100,001-500,000 58
- 500,001-1,000,000 6
- 1,000,001-2,000,000 2
- 2,000,001-5,000,000 15
- 5,000,001-10,000,000 6
- >10,000,000 2